EFSP Auxiliary ESL Curriculum

Cybersecurity English

Instructor guide for advanced ESL learners working in cybersecurity

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.

Purpose and Course Logic

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

Core language challenge

Advanced learners do not only need vocabulary. They need the ability to ask which standard applies, who owns the decision, what evidence is sufficient, what risk is being accepted, and how to disagree without sounding vague, defensive, or reckless.

Each module trains a realistic workplace pressure point with role-specific terms, decision language, pushback practice, and a written output learners can adapt to their own work.

Course objectives

- Use cybersecurity terminology accurately in meetings, written updates, handoffs, escalations, reviews, and client or stakeholder conversations.
- Turn vague requests into specific questions about evidence, owner, deadline, constraint, risk, and decision rights.
- Push back on unsafe, unsupported, noncompliant, unrealistic, or poorly scoped proposals while preserving professional trust.
- Handle realistic dialogues from the field, including conflict, uncertainty, documentation gaps, customer or stakeholder pressure, and cross-functional disagreement.
- Produce concise workplace outputs: briefing notes, escalation updates, meeting scripts, risk memos, decision records, and follow-up messages.

Instructor Module Plans

Module 1. Security Triage and Alert Investigation (90 minutes)

Move from noisy alerts to risk-based investigation.

Learners should be able to

- Use these terms accurately: SIEM, alert, false positive, privileged account.
- Explain the workplace tension: Privilege, behavior, context, and evidence need review.
- Respond professionally when a stakeholder says: Close them as false positives because the user is senior.
- Draft a usable alert triage note with facts, caveats, owner, and next step.

Customized scenario

Workplace pressure

The SOC receives repeated alerts from a privileged account.

Close them as false positives because the user is senior.

Privilege, behavior, context, and evidence need review.

Classroom sequence

1. Terminology drill: define each term, then use it in one sentence from the learner's own role.
2. Risk map: identify the stakeholder, the decision, the evidence gap, the operating constraint, and the cost of being wrong.
3. Pushback ladder: move from clarifying question to evidence-based objection to consequence to decision request.

4. Output lab: draft and revise a alert triage note.

Module 2. Incident Response and Containment (90 minutes)

Communicate urgency without speculation.

Learners should be able to

- Use these terms accurately: incident, containment, ransomware, forensics.
- Explain the workplace tension: Scope, containment, evidence preservation, communications, and legal review matter.
- Respond professionally when a stakeholder says: Tell everyone the company is breached.
- Draft a usable incident bridge update with facts, caveats, owner, and next step.

Customized scenario

Workplace pressure

A ransomware note appears on a shared server.

Tell everyone the company is breached.

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

Classroom sequence

1. Terminology drill: define each term, then use it in one sentence from the learner's own role.
2. Risk map: identify the stakeholder, the decision, the evidence gap, the operating constraint, and the cost of being wrong.
3. Pushback ladder: move from clarifying question to evidence-based objection to consequence to decision request.
4. Output lab: draft and revise a incident bridge update.

Module 3. Vulnerability Management (90 minutes)

Prioritize vulnerabilities beyond CVSS alone.

Learners should be able to

- Use these terms accurately: CVE, CVSS, exploitability, compensating control.
- Explain the workplace tension: Exploitability, exposure, asset criticality, compensating controls, and downtime must be balanced.
- Respond professionally when a stakeholder says: Patch every system immediately.
- Draft a usable vulnerability prioritization memo with facts, caveats, owner, and next step.

Customized scenario

Workplace pressure

A critical CVE affects an internet-facing system.

Patch every system immediately.

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

Classroom sequence

1. Terminology drill: define each term, then use it in one sentence from the learner's own role.
2. Risk map: identify the stakeholder, the decision, the evidence gap, the operating constraint, and the cost of being wrong.

3. Pushback ladder: move from clarifying question to evidence-based objection to consequence to decision request.
4. Output lab: draft and revise a vulnerability prioritization memo.

Module 4. Identity, Access, and Least Privilege (90 minutes)

Push back on excessive access requests.

Learners should be able to

- Use these terms accurately: IAM, least privilege, MFA, RBAC.
- Explain the workplace tension: Least privilege, approval, logging, and time-bound access are required.
- Respond professionally when a stakeholder says: Grant temporary admin access.
- Draft a usable access request response with facts, caveats, owner, and next step.

Customized scenario

Workplace pressure

A contractor asks for admin rights to troubleshoot faster.

Grant temporary admin access.

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

Classroom sequence

1. Terminology drill: define each term, then use it in one sentence from the learner's own role.
2. Risk map: identify the stakeholder, the decision, the evidence gap, the operating constraint, and the cost of being wrong.
3. Pushback ladder: move from clarifying question to evidence-based objection to consequence to decision request.
4. Output lab: draft and revise a access request response.

Module 5. Threat Modeling and Secure Design (90 minutes)

Discuss security risk early in design.

Learners should be able to

- Use these terms accurately: threat model, attack surface, trust boundary, abuse case.
- Explain the workplace tension: Abuse cases, data flows, trust boundaries, and mitigations need design-time attention.
- Respond professionally when a stakeholder says: Do a quick review after launch.
- Draft a usable threat model findings with facts, caveats, owner, and next step.

Customized scenario

Workplace pressure

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

Do a quick review after launch.

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

Classroom sequence

1. Terminology drill: define each term, then use it in one sentence from the learner's own role.
2. Risk map: identify the stakeholder, the decision, the evidence gap, the operating constraint, and the cost of being wrong.

3. Pushback ladder: move from clarifying question to evidence-based objection to consequence to decision request.
4. Output lab: draft and revise a threat model findings.

Module 6. Governance, Risk, and Compliance (90 minutes)

Translate control gaps into business risk.

Learners should be able to

- Use these terms accurately: control, audit evidence, risk acceptance, remediation.
- Explain the workplace tension: Control design, evidence, ownership, remediation, and risk acceptance need clarity.
- Respond professionally when a stakeholder says: Say the control is mostly working.
- Draft a usable GRC remediation plan with facts, caveats, owner, and next step.

Customized scenario

Workplace pressure

Audit finds incomplete access reviews.

Say the control is mostly working.

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

Classroom sequence

1. Terminology drill: define each term, then use it in one sentence from the learner's own role.
2. Risk map: identify the stakeholder, the decision, the evidence gap, the operating constraint, and the cost of being wrong.
3. Pushback ladder: move from clarifying question to evidence-based objection to consequence to decision request.
4. Output lab: draft and revise a GRC remediation plan.

Module 7. Security Awareness and Phishing (90 minutes)

Coach users without shaming them.

Learners should be able to

- Use these terms accurately: phishing, social engineering, reporting culture, security awareness.
- Explain the workplace tension: Behavior, training, reporting culture, and technical controls all matter.
- Respond professionally when a stakeholder says: Send a public warning.
- Draft a usable awareness coaching script with facts, caveats, owner, and next step.

Customized scenario

Workplace pressure

An executive clicks a phishing simulation link.

Send a public warning.

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

Classroom sequence

1. Terminology drill: define each term, then use it in one sentence from the learner's own role.
2. Risk map: identify the stakeholder, the decision, the evidence gap, the operating constraint, and the cost of being wrong.

3. Pushback ladder: move from clarifying question to evidence-based objection to consequence to decision request.
4. Output lab: draft and revise a awareness coaching script.

Module 8. Executive Risk Briefings (90 minutes)

Explain cyber risk in decision language.

Learners should be able to

- Use these terms accurately: residual risk, threat actor, maturity, investment ask.
- Explain the workplace tension: Residual risk, threat landscape, controls, investment, and response readiness require nuance.
- Respond professionally when a stakeholder says: Give a yes-or-no answer.
- Draft a usable board cyber-risk update with facts, caveats, owner, and next step.

Customized scenario

Workplace pressure

The board asks whether the organization is safe from attacks.

Give a yes-or-no answer.

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

Classroom sequence

1. Terminology drill: define each term, then use it in one sentence from the learner's own role.
2. Risk map: identify the stakeholder, the decision, the evidence gap, the operating constraint, and the cost of being wrong.
3. Pushback ladder: move from clarifying question to evidence-based objection to consequence to decision request.
4. Output lab: draft and revise a board cyber-risk update.

Nomenclature and Jargon

These are classroom working definitions. Learners should adapt wording to their organization's policies, systems, and local regulatory environment.

Security Triage and Alert Investigation

Term	Working meaning
SIEM	Working cybersecurity term used in security triage and alert investigation; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.
alert	Working cybersecurity term used in security triage and alert investigation; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.
false positive	Working cybersecurity term used in security triage and alert investigation; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.
privileged account	Working cybersecurity term used in security triage and alert investigation; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.

Incident Response and Containment

Term	Working meaning
incident	Unplanned event that disrupts service, safety, quality, security, operations, or expected performance.
containment	Working cybersecurity term used in incident response and containment; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.
ransomware	Working cybersecurity term used in incident response and containment; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.
forensics	Working cybersecurity term used in incident response and containment; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.

Vulnerability Management

Term	Working meaning
CVE	Working cybersecurity term used in vulnerability management; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.
CVSS	Working cybersecurity term used in vulnerability management; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.
exploitability	Working cybersecurity term used in vulnerability management; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.
compensating control	Working cybersecurity term used in vulnerability management; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.

Identity, Access, and Least Privilege

Term	Working meaning
IAM	Working cybersecurity term used in identity, access, and least privilege; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.
least privilege	Working cybersecurity term used in identity, access, and least privilege; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.
MFA	Working cybersecurity term used in identity, access, and least privilege; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.
RBAC	Working cybersecurity term used in identity, access, and least privilege; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.

Threat Modeling and Secure Design

Term	Working meaning
threat model	Working cybersecurity term used in threat modeling and secure design; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.
attack surface	Working cybersecurity term used in threat modeling and secure design; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.
trust boundary	Working cybersecurity term used in threat modeling and secure design; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.
abuse case	Working cybersecurity term used in threat modeling and secure design; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.

Governance, Risk, and Compliance

Term	Working meaning
control	A process, approval, check, or technical safeguard designed to reduce risk.
audit evidence	Working cybersecurity term used in governance, risk, and compliance; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.
risk acceptance	Working cybersecurity term used in governance, risk, and compliance; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.
remediation	Working cybersecurity term used in governance, risk, and compliance; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.

Security Awareness and Phishing

Term	Working meaning
phishing	Working cybersecurity term used in security awareness and phishing; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.
social engineering	Working cybersecurity term used in security awareness and phishing; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.
reporting culture	Working cybersecurity term used in security awareness and phishing; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.
security awareness	Working cybersecurity term used in security awareness and phishing; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.

Executive Risk Briefings

Term	Working meaning
residual risk	Working cybersecurity term used in executive risk briefings; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.
threat actor	Working cybersecurity term used in executive risk briefings; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.
maturity	Working cybersecurity term used in executive risk briefings; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.
investment ask	Working cybersecurity term used in executive risk briefings; define the owner, evidence source, governing document, risk, and decision impact before using it in a meeting.

Industry-Specific Meeting Moves

Situation	Useful language
Security Triage and Alert Investigation	Before we commit, I want to confirm SIEM, alert, the owner, and the evidence behind the decision. If privilege, behavior, context, and evidence need review., I recommend we document the risk and agree on the next step.
Incident Response and Containment	Before we commit, I want to confirm incident, containment, the owner, and the evidence behind the decision. If scope, containment, evidence preservation, communications, and legal review matter., I recommend we document the risk and agree on the next step.
Vulnerability Management	Before we commit, I want to confirm CVE, CVSS, the owner, and the evidence behind the decision. If exploitability, exposure, asset criticality, compensating controls, and downtime must be balanced., I recommend we document the risk and agree on the next step.

Situation	Useful language
Identity, Access, and Least Privilege	Before we commit, I want to confirm IAM, least privilege, the owner, and the evidence behind the decision. If least privilege, approval, logging, and time-bound access are required., I recommend we document the risk and agree on the next step.
Threat Modeling and Secure Design	Before we commit, I want to confirm threat model, attack surface, the owner, and the evidence behind the decision. If abuse cases, data flows, trust boundaries, and mitigations need design-time attention., I recommend we document the risk and agree on the next step.
Governance, Risk, and Compliance	Before we commit, I want to confirm control, audit evidence, the owner, and the evidence behind the decision. If control design, evidence, ownership, remediation, and risk acceptance need clarity., I recommend we document the risk and agree on the next step.
Security Awareness and Phishing	Before we commit, I want to confirm phishing, social engineering, the owner, and the evidence behind the decision. If behavior, training, reporting culture, and technical controls all matter., I recommend we document the risk and agree on the next step.
Executive Risk Briefings	Before we commit, I want to confirm residual risk, threat actor, the owner, and the evidence behind the decision. If residual risk, threat landscape, controls, investment, and response readiness require nuance., I recommend we document the risk and agree on the next step.

High-pressure pushback frames

- I understand the urgency. The risk is that we move faster than the evidence or process supports.
- I am not blocking the goal. I am naming the condition we need before the decision is safe and credible.
- If we accept this risk, we should name the owner, document the assumption, and define the trigger for escalation.
- That may be possible, but not under the current scope, timeline, or approval path.
- Let's separate what we know, what we assume, and what still needs confirmation.

Assessment and Coaching

Performance rubric

Skill	Developing	Proficient	Strong
Terminology	Recognizes terms but uses them loosely.	Uses field terms accurately in context.	Defines terms, connects them to evidence, and explains decision impact.
Pushback	Disagrees vaguely or avoids disagreement.	Names concern with evidence and next step.	Balances urgency, relationship, risk, owner, and decision rights.
Scenario judgment	Focuses on one stakeholder's preference.	Identifies constraint, risk, and process.	Guides the group toward a documented, realistic decision.
Written output	Writes general summaries.	Produces clear notes with facts and owner.	Creates concise, decision-ready workplace communication.

Source orientation

- NIST, CISA, and relevant security frameworks.
- Company incident-response and access-control policies.
- Legal, privacy, and communications guidance for incidents.
- The learner's own company policies, SOPs, contracts, systems, templates, and approved communication standards.