

English for Ransomware Readiness Briefings

A training course for solutions architects

Final artifact: 5-minute ransomware readiness briefing to customer IT leadership

Level: B1 Business Operational | Format: 8 sessions × 60 min, online | Group: 3–5 learners

Task family: Pitch / proposal — recommending a course of action

The task

A solutions architect delivers a 5-minute ransomware readiness briefing to a customer's IT leadership. The briefing gives the CIO or CISO enough to act — either green-light a remediation, escalate budget, or close the engagement — without scheduling a follow-up to ask the same questions again.

Audience: customer CIO or CISO, sometimes joined by the head of infrastructure. Senior, time-poor, technically literate but not always in the data-protection weeds. Two to four people on the call.

Success: the customer makes a decision in the same meeting — approve the recommended action, escalate, or decline. The SA is not asked to come back with the same briefing.

Language outcomes

Solutions architects who complete this course will be able to:

- Open a briefing with a clear readiness verdict and one-line rationale, without preamble
- Describe what is in place using plain operational language, not product-feature language
- Name the single largest gap directly — without softening, hedging, or burying it in qualifiers
- Pair each risk scenario with the customer's current recovery position, so exposure is visible without exaggeration
- Switch register from technical (RPO, immutability, air-gap) to executive (downtime cost, board exposure) within the same briefing
- Close with a specific, named action request the customer can approve in the same meeting

Structure

Beat	Purpose	Time
Verdict & headline	State the readiness rating and your stance in one sentence	~30 sec
Readiness profile	What's already in place — protected workloads, recovery posture	~60 sec
Critical gap	The single largest exposure, named directly	~45 sec
Risk scenarios	2–3 attack scenarios paired with current recovery position	~90 sec
Recommendation	Specific action request with timeline	~45 sec

8-session schedule

#	Session	Artifact
1	Orientation & Baseline	Unassisted 5-min recording + L1

		score
2	Structure & core language	75-sec fragment: verdict + readiness profile
3	Partial simulation	2-min walkthrough of risk scenarios beat
4	Full simulation — Round 1	Full 5-min recording + diagnostic notes
5	Repair & upgrade	Re-recorded segment on main breakdown
6	Pressure variation	5-min briefing under one new variable
7	Final simulation	Unassisted 5-min recording + L7 score
8	Evaluation & Capstone	L1/L7 reveal + capstone on real upcoming customer + personal grade report

What each learner receives

- Personal portfolio of 8 recordings across the course
- Per-criterion scores at L1 and L7 (5 criteria, 0/1/2 each, /10 total)
- Individual grade band: Distinction / Pass with merit / Pass / Not yet passing
- Pass certificate on either performance ($L7 \geq 6/10$) or improvement ($L7 - L1 \geq 2$ points)

Portfolio

Save each recording to a shared folder. One folder per learner.

File naming: Veeam_[Region]_[LearnerID]_RansomwareBriefing_L[#]_YYYY-MM-DD

Three rules for the trainer

- 1. Follow the lesson order.** The sessions build on each other. Don't skip, don't swap.
- 2. Score the artifact at L1 and L7 using the full scorecard.** Other lessons need only a brief observation note. The L1 and L7 scores produce each learner's grade.
- 3. No language help and no language bank during L1 or L7.** These are the before-and-after measures. Hide all references. Observe and record only.