

Lesson 4 — Full Simulation (Round 1)

Session 4 of 8 | Duration: 60 min | Artifact: Full 5-min recording + diagnostic notes

Purpose

First full briefing under realistic conditions. Trainer uses the failure-pattern checklist to identify breakdowns for L5.

Phases

Time	Phase	Trainer does
0:00–0:05	Frame the session	State this is the first full run. Realistic conditions. No help.
0:05–0:20	Read the full profile	Silent reading of the full customer profile (below). Language bank visible but no teaching.
0:20–0:30	Silent prep	Learners plan their briefing. Notes allowed, scripts not.
0:30–0:55	Full briefings	Each learner records 5 min. No interruptions. Others on camera as the customer panel. Trainer ticks the failure-pattern checklist (below) during each recording.
0:55–1:00	Close	Brief observation on what held together. Save recordings and the marked checklist.

Scripted teacher language

“This is the first full run. Five minutes. No restarts — if something breaks, keep going.”

“Notes yes, scripts no. If you read a script, the customer will hear it.”

“I’m not coaching during the briefing. If you get stuck on a word, use a simpler one.”

Customer — full profile

Customer: Aurum Manufacturing — global manufacturer of precision components

Profile. 14,000 employees across 8 countries. Annual revenue €2.8B. Two HQ datacenters (Germany, Singapore) plus 12 manufacturing plants. The CISO requested this readiness review three weeks after a publicly-disclosed competitor breach. The customer’s board is asking the same question.

Estate. Roughly 60% on-prem VMware (manufacturing execution systems, SAP ECC, MES integrations); 25% Hyper-V across the two regional datacenters; 15% AWS for analytics and data warehousing. Approximately 4 PB total protected. Active Directory has two forests, one per region, with no recovery testing on either in the last 18 months.

Backup posture. Backups go to two separate on-site repositories — one per HQ datacenter. Neither is immutable. There is a tape rotation in Germany that goes off-site weekly, but no validated restore from

tape in 14 months. Edge plants back up locally with 7-day retention; no replication to HQ. Cloud workloads are protected with AWS Backup, no cross-account replication.

Recovery posture. Documented RTO is 8 hours for tier-1 systems; last DR test was 11 months ago and only covered SAP ECC partial restore (took 27 hours, was abandoned). No runbooks for ransomware-specific scenarios. No clean room. AD recovery has never been tested.

Risks. Single point of failure on the backup repositories — both reachable from the production AD domain. No immutability anywhere. AD recovery is the dominant blast-radius scenario. Edge plant data is unprotected against a 7+ day undetected encryption.

The briefing: Deliver a 5-minute readiness briefing to the customer's IT leadership.

Failure-pattern checklist

Tick the dominant patterns observed across the cohort. The top 1–2 ticks become the focus of L5.

- ☐ Verdict buried — readiness rating appears after the analysis, not in the headline
- ☐ Readiness profile reads like a feature list (“they have product X, version Y”) instead of operational reality (“they can recover the SAP cluster within 8 hours, they cannot recover AD”)
- ☐ Critical gap softened — hedged with “it might be worth considering” instead of named directly
- ☐ Risk scenarios named without recovery position (“there’s a risk of encryption” left hanging)
- ☐ Risk scenarios over-run and eat the action request
- ☐ Recommendation is vague (“I think we should improve immutability”) rather than specific (“I’m recommending we add immutable repositories at both HQ datacenters within 30 days”)
- ☐ Tense slippage when describing the customer’s environment (mixes past and present in one sentence)
- ☐ Vague verbs (“do”, “have”, “make”) where data-protection-precise verbs exist (replicate, immutable, isolate, restore, fail over)

Between-session work

No homework. Trainer prepares the L5 repair from the marked checklist.

Artifact

Full 5-min recording per learner + completed failure-pattern checklist (one per cohort, not per learner). Save as Veeam_[Region]_[LearnerID]_RansomwareBriefing_L4_YYYY-MM-DD.