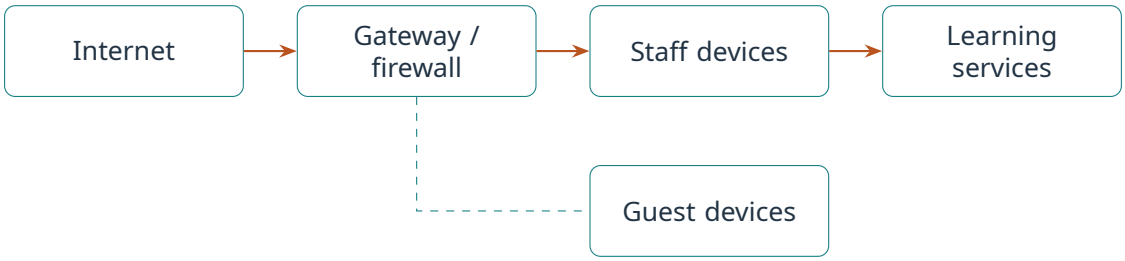
A GUIDED CLASSROOM EXERCISE

Network security & risk review

For advanced students, educators and small-institution IT discussions. A learning worksheet, not an ISO/IEC 27001 certification audit, compliance guarantee or penetration test.

Use only an authorised lab or paper scenario. This exercise does not require scanning, exploiting or changing a real network. Record “not tested” when you do not have evidence.

1 / Follow the services and trust boundaries



An illustrative map, not a recommended topology. Decide which paths should be permitted and which data needs protection. Segmentation helps only when the rules and management access are configured and checked.

Scenario

A small learning centre has staff laptops, a guest Wi-Fi network, a shared file service and cloud accounts. A single administrator manages updates. Backups exist, but nobody has recorded a recent restore test.

Asset	Why it matters	Evidence to request
Cloud accounts	Access to teaching files and communication.	MFA coverage, roles, recovery ownership.
File service	Availability and integrity of shared work.	Access review and a documented restore test.
Guest network	Untrusted devices share connectivity.	A reviewed separation policy and authorised checks.

2 / Define your scope

Services / data included:

Owner approving the review / date:

RISK / CONTROL / EVIDENCE

Review controls with a purpose

3 / Start with the risk

Risk	Candidate control	What would support confidence?
Account takeover	MFA and least privilege.	Coverage report, role review and tested recovery procedure.
Unpatched software	Asset inventory and patch ownership.	Version records and a maintained update schedule.
Loss of teaching files	Backups separated from the working copy.	Dated restore test with the result recorded.
Unwanted access from guests	Segmentation and explicit firewall rules.	Reviewed policy and authorised connectivity checks.

Controls reduce particular risks; no single control makes a system secure. Encryption, for example, does not repair an overly broad access permission.

4 / Worked risk-register entry

Finding: backup jobs report success but restoration has not been tested.
Possible impact: files may be unavailable when recovery is needed.
Uncertainty: the review has not shown that the backups are unusable.
Action: the authorised administrator restores a non-sensitive sample to an isolated location, checks its integrity and records the outcome.
Owner / review date: assign a responsible role and an achievable date.

Likelihood and impact ratings should use an agreed scale. A simple low/medium/high classroom rating supports discussion; it is not an objective measurement of risk.

My register entry

Finding and evidence:

Likely consequence / uncertainty:

Action / owner / review date:

RECORD THE RESULT

Security review worksheet

For each item, write Y (evidence supports it), N (gap found), or NT (not tested). A tick is not enough: record what you inspected.

Review item	Status	Evidence / next action
Asset and service owners are identified.		
Privileged access is limited and reviewed.		
MFA and account recovery have clear ownership.		
Update responsibilities and exceptions are recorded.		
Guest / staff separation has a reviewed purpose.		
Backup restoration has documented evidence.		
Logs are useful, access-controlled and retained appropriately.		
Incident reporting and escalation are understood.		

5 / Reflect

Question: Why does a successful backup job not prove recovery will work?
Suggested explanation: the job may have copied incomplete or unusable data, or the restore process may fail. A controlled restore test gives more direct evidence while still having a limited scope.

Further reading

NIST Cybersecurity Framework: nist.gov/cyberframework. The Govern, Identify, Protect, Detect, Respond and Recover functions provide a useful discussion structure.
ISO/IEC 27001 overview: iso.org/standard/27001. Formal requirements require the actual standard and appropriate expertise.
This supplementary guide is not a complete Cambridge course or an operational security approval. No real credentials or sensitive incident evidence should be written in it.