INSTRUCTOR ANSWER KEY

CONFIDENTIAL

The 5 C's Framework • The Fact Sheet • Writing Audit Findings

QUICK ANSWER SUMMARY

Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10
B	B	B	C	B	B	C	B	C	C

Each answer block shows: **(1) the correct answer highlighted in green** **(2) the explanation in gold** (3) why each incorrect option fails in grey.

Q1

[Module 3A — Criteria] **When writing the Criteria span, which best describes a strong Criteria statement?**

CORRECT ANSWER: B

✓ **B. A citation of a specific policy section that the organization has formally adopted, stating the exact requirement.**

Why

Strong Criteria must be specific, cited, and relevant. Naming the policy document, section number, and exact requirement gives management nothing to dispute — they approved and adopted that standard. This is the benchmark against which the Condition is measured.

Other options

A. Too vague — 'properly controlled' cannot be measured and gives management grounds to dispute whether a gap exists at all.

C. Citing a framework the organization has not formally adopted creates the 'orphaned standard' trap — management can legitimately argue the standard does not apply to them.

D. Auditor opinion is not a Criteria. The standard must be documented and agreed — not based on what the auditor believes best practice should be.

Q2

[Module 3A — Condition] **An auditor writes: 'Several user accounts lacked management authorization.' What is the primary weakness?**

CORRECT ANSWER: B

✓ **B. It uses the vague superlative 'several' instead of a specific number and percentage.**

Why

Condition statements must replace all superlatives with specific numbers. 'Several' cannot be verified, cannot be measured against a population, and gives management room to argue about what 'several' means. '54 of 200 accounts (27%)' leaves no room for that argument.

Other options

A. Policy citation belongs in the Criteria, not the Condition. The Condition records what was observed — the Criteria establishes the standard.

C. Cause is a separate element. The Condition should only report facts — mixing in explanation of why the gap exists weakens the factual credibility of the observation.

D. Length is not the issue. A Condition statement can be one sentence if it contains specific, evidence-based numbers. More words do not make it stronger.

Q3	*[Module 3A — Cause]* **The Cause is written as: 'IT staff failed to remove accounts when employees left.' Why is this weak?**	CORRECT ANSWER: **B**
✓	**B. It identifies a people failure rather than the underlying process or system failure.**	
Why	Cause should identify process failures, not people failures. 'IT staff failed to act' points to individuals, which leads to a recommendation of retraining — a solution that wears off. The real cause is structural: no automated integration between HR termination notifications and Active Directory deprovisioning. That structural cause leads to a structural recommendation that permanently fixes the problem.	
Other options	**A.** The number of accounts belongs in the Condition, not the Cause. Cause explains why the gap exists, not how many instances were found. **C.** Cause is correctly a separate element from Condition. The Condition describes what was found; the Cause explains the root reason it occurred. **D.** Cause should be specific — general Causes lead to general Corrections that do not fix the root problem. Specificity is a strength, not a weakness.	

Q4	*[Module 3A — Consequence]* **Which is the strongest Consequence statement for terminated employee accounts remaining active?**	CORRECT ANSWER: **C**
✓	**C. 23 former employees currently retain active system access, creating immediate risk of data exfiltration, a PIPEDA compliance gap with penalties up to $100,000 per violation, and potential reputational damage if a breach occurs.**	
Why	Strong Consequence uses the Consequence Multiplier: it names what specifically could go wrong, identifies a current (not theoretical) risk (23 accounts active right now), cites the specific regulation and penalty, and covers multiple impact categories — financial, regulatory, and reputational. The executive reading this cannot argue that the risk is theoretical.	
Other options	**A.** Generic and interchangeable — this sentence could appear in any finding for any control weakness in any organization. It creates no urgency. **B.** Better than A but still vague. 'Possible' signals theoretical risk. No financial figure, no regulation, no current condition. Executives respond to specificity, not possibility. **D.** The severity rating is a label, not a Consequence. Repeating the risk rating in the Consequence section adds no information and makes the auditor appear to be relying on the label rather than making the argument.	

Q5	*[Module 3A — Correction]* **Three root causes identified. The auditor recommends: 'Management should improve access controls and retrain IT staff.' What is wrong?**	CORRECT ANSWER: **B**
✓	**B. The recommendation addresses the symptom and fails to map to any of the three identified root causes.**	
Why	The alignment test for Correction: if this recommendation is fully implemented, does each root cause go away? Here — no automated provisioning control, no HR-IT integration, no periodic access review — none of these structural weaknesses is addressed by 'improve controls and retrain staff.' The recommendation treats the symptom (staff behaviour) rather than the system and process failures that make the problem inevitable regardless of staff behaviour.	
Other options	**A.** Length is not the issue. A weak recommendation can be long or short. What matters is that it addresses the root causes, not how many words it uses. **C.** Retraining is appropriate when inadequate training is the root cause. When the root cause is a missing technical control or integration gap, retraining does not fix the problem. **D.** Corrections are developed collaboratively with management and the auditee during the Fact Sheet meeting — but the auditor is responsible for ensuring the recommendations address the root causes identified.	

Q6	*[Module 3A — 5 C's Framework]* **On the draft Fact Sheet sent to the auditee, Cause and Correction are deliberately left blank while Criteria, Condition, and Consequence are already filled in. Why?**	**CORRECT ANSWER: B**
✓	**B. Criteria, Condition, and Consequence can be determined by the auditor independently from evidence, while Cause and Correction must be developed together with the auditee and management before they are agreed.**	
Why	Criteria comes from the policy or standard, Condition comes from testing, and Consequence follows from the risk implications of the gap — all three can be documented by the auditor from evidence alone, which is why they go out fast, within one to two business days of completing testing. Cause and Correction are different. The easiest explanation for a control gap is often not the real root cause, and only the auditee and management have the operational knowledge to identify what is actually happening. Correction must align with Cause, so Correction cannot be developed until Cause has been discussed and agreed. Leaving both blank on the draft signals that these two elements are built through conversation, not announced by the auditor.	
Other options	**A.** Cause and Correction are not confidential — they are openly discussed with the auditee and management during the Fact Sheet meeting. They are blank on the draft only because they have not yet been developed at that point, not because they are restricted information. **C.** Cause and Correction are required for every finding regardless of severity. Severity is assigned afterward, in the auditor-only section, once Cause and Correction have already been agreed. **D.** Whether a finding is included in the report is a separate decision from whether Cause has been developed. A finding can be fully resolved through the Fact Sheet process and still warrant inclusion in the final report.	

Q7	*[Module 3B — Fact Sheet Philosophy]* **What is the primary purpose of issuing a Fact Sheet to management during fieldwork?**	**CORRECT ANSWER: C**
✓	**C. To share findings as they are identified, allowing management to confirm facts, provide context, and contribute to recommendations — eliminating most report-level disputes.**	
Why	The Fact Sheet shifts management from audience to partner. By engaging with each finding during fieldwork — before the report is finalized — management has already seen, discussed, and responded to every element. The result is a submission meeting with no surprises, management responses already in place, and findings that have survived scrutiny at the fieldwork stage rather than being contested at the report stage.	
Other options	**A.** Management cannot veto findings. If they dispute an element and cannot provide substantive new information, the finding stands and the disagreement is documented. The Fact Sheet is not a veto mechanism. **B.** The purpose is collaboration, not preparation for argument. Giving management advance notice to prepare counter-arguments would be the opposite of the Fact Sheet philosophy. **D.** While the Fact Sheet does create valuable audit documentation, methodology compliance is not its primary purpose. Its purpose is to transform management from adversary to partner.	

Q8	*[Module 3B — Fact Sheet Structure]* **What does the 'Enforced Y/N' checkbox in the Criteria section capture that 'Accepted Y/N' alone does not?**	**CORRECT ANSWER: B**
✓	**B. Whether management acknowledges that the policy is actively being enforced — not just that it exists on paper.**	
Why	A policy that exists but is not enforced is itself a finding — and it completely changes the Cause and the Correction. If management checks Accepted Y but Enforced N, the auditor has discovered that the control failure is not about compliance with an enforced standard but about the absence of any enforcement mechanism. That is a fundamentally different problem requiring a different recommendation.	
Other options	**A.** Whether the policy is strong enough is the auditor's professional judgment — it is not captured by a checkbox and is not management's determination to make. **C.** Policy currency is important but is not what the Enforced checkbox measures. Currency relates to whether the policy has been reviewed and updated; enforcement relates to whether it is being applied. **D.** Auditee presence at the meeting is a logistical matter captured in the header fields, not the purpose of the Enforced checkbox.	

Q9	*[Module 3B — Pushback Scenarios]* **Management says: 'We already fixed that issue last month.' What is the best course of action?**	**CORRECT ANSWER: C**
✓	**C. Request documentation, verify and test the remediation through working papers, modify the finding if confirmed — but still include it in the report with credit given to management for proactive correction.**	
Why	Including the finding with a credit note serves two purposes: it preserves the integrity of the audit record (the gap existed during the audit period) and it changes management's incentive in future audits — they learn that proactive remediation earns acknowledgement rather than just removing a finding. This builds the trusted advisor relationship that makes future audits more productive.	
Other options	**A.** Accepting verbal assurances without verification violates basic audit standards. Remediation must be verified and tested through working papers before any modification to the finding. **B.** The Fact Sheet process exists precisely so management responses can be incorporated before the final report. Ignoring a significant management response defeats the purpose of collaborative fieldwork. **D.** A new Fact Sheet is appropriate when new testing reveals the original finding was incorrect or when an expanded sample confirms a disputed finding — not when management claims prior remediation.	

Q10	*[Module 3B — Audit Report Framing]* **Which approach best reflects the audit function as a trusted advisor rather than an adversary?**	**CORRECT ANSWER: C**
✓	**C. Frame the report to show both what is working well and what needs improvement — using visual indicators where helpful — so management sees a complete picture, not just a list of problems.**	
Why	An auditor who only documents problems is perceived as an adversary. An auditor who acknowledges strengths alongside weaknesses is a trusted advisor. A visual overview — green indicators for effective controls, red for areas needing improvement — gives management a balanced scorecard. When eight of ten controls are shown in green, management's posture toward the two red areas changes from defensiveness to problem-solving. The findings are the same; the frame changes everything.	
Other options	**A.** Limiting findings to only the most critical may miss important medium-risk items and creates an incomplete picture. The goal is completeness with appropriate prioritization, not brevity at the expense of coverage. **B.** Management responses do not compromise independence — they improve the report. A report that includes management responses is more credible and actionable than one that does not. **D.** Removing disputed findings without substantive new evidence compromises audit integrity. Disagreements are documented and both positions presented — the finding stands.	

