Grading a Nonconformity

A quick-reference guide · ISO/IEC 27001:2022 Lead Auditor Session

Every finding an auditor raises gets one of three grades. Getting the grade right is what makes a finding defensible — too harsh and management pushes back and stalls certification; too soft and a real risk goes unaddressed until the next visit.

Grade	What it means
Major NC	A requirement is not met at all, or the failure is systemic — it affects the ISMS's ability to achieve its intended outcome, or a cluster of minor issues points to a breakdown in a whole clause or control area.
Minor NC	A single lapse or isolated instance — the requirement is largely met, but one instance, one record, or one control application falls short.
OFI	The requirement is met — this is a suggestion for improvement, not a nonconformity. No corrective action is required.

Four questions to tell them apart

- 1. Is the requirement met at all, or only partially?
- 2. Is this one instance, or a pattern across the sample?
- 3. Does it affect the ISMS's ability to achieve its intended outcome?
- 4. Would a reasonable auditor expect this to put certification at risk?

Writing the finding

A defensible finding states three things, in this order: the requirement (what the clause or control demands), the evidence (what you actually observed, sampled, or were shown), and the gap (the specific difference between the two). A finding that skips straight to "the gap" without stating the requirement and evidence is the most common reason a finding gets successfully challenged in the closing meeting.

Weak vs. strong: the same finding, written two ways

Weak — gets challenged	Strong — holds up
"Access reviews aren't being done properly."	*"A.5.18 requires periodic review of access rights. The access review log shows no review was completed for Q2. Requirement not met for one of four quarters sampled — Minor NC."*

The left version names no clause, no evidence, and no scope — management can (and will) push back with "says who, and how often?" The right version is closed to challenge: it names the control, the specific record, the specific gap, and the sample it was drawn from.

Common grading mistakes

- Grading up to "Major" because the topic feels serious (e.g. access control), rather than because the failure is systemic or a requirement is entirely unmet.
- Grading down to "Minor" to avoid a difficult conversation with management — the grade should follow the evidence, not the room.
- Writing an OFI when the requirement is genuinely not met — an OFI carries no obligation to act, so this quietly waives a real gap.
- Combining two unrelated gaps into one finding — grade and correct each root cause separately, even if they surfaced in the same interview.

After the grade: closing the loop

A grade isn't the end of the audit trail. The closing meeting presents the finding and its grade to management, who can challenge it with additional evidence before it's finalised. From there, the auditee proposes a root cause and corrective action, and the auditor's job shifts to verification: confirming the action was actually implemented and that it addresses the root cause — not just the symptom that was observed on the day.

This is the exact call you'll practise live in Module 03 of the ISO 27001 Lead Auditor session — bring a real finding from your own ISMS if you have one.