EVIDENCE INDEPENDENCE ASSESSMENT WORKSHEET

A copy of evidence is independent only if the attacker cannot exercise the same authority over both the original and the copy. Answer each question for one evidence source at a time.

01	Can the source system modify its own logs after the fact?	☐ YES	☐ NO
02	Does the evidence repository share authentication infrastructure with infrastructure with the source?	☐ YES	☐ NO
03	Can the same administrative authority modify both the source and the evidence repository?	☐ YES	☐ NO
04	Can telemetry be altered in transit, before collection completes?	☐ YES	☐ NO
05	Is there no independent evidence path outside the source's own authority chain?	☐ YES	☐ NO
06	Would incident responders be unable to validate this evidence against a separate authority domain?	☐ YES	☐ NO

SCORING

Count your YES answers.

Each YES marks a point where this source shares authority with the thing it's meant to be evidence of.

0 YES — genuine independence boundary.

1–2 YES — partial; find the shared authority path and separate it.

3+ YES — this is a copy, not independent evidence.