SAMPLE

Sample Security Readiness Findings Report

FICTIONAL EXAMPLE • HARBORLINE CLOUD SERVICES

DECISION SUMMARY

Harborline should address access review evidence and incident response testing before scheduling its first SOC 2 Type II examination. Its current policies provide a useful starting point, but several recurring controls need a named owner and retained operating evidence.

Scope and method

Illustrative scope: the fictional Harborline customer portal and supporting cloud environment. Example review: 10 control areas aligned to the SOC 2 security criteria, two owner interviews, and 11 supplied artifacts. This limited advisory sample does not establish audit readiness or predict an auditor opinion.

Illustrative findings

Priority	Observation and example evidence	Recommended action
High	Access reviews lack completion evidence. The access procedure calls for quarterly reviews. Two sample quarters had exported user lists but no dated owner sign-off or documented disposition of exceptions.	Assign a review owner; record review date, population, decisions, follow-up, and closure. Retain each completed review.
High	Incident response exercise has not been evidenced. A response plan exists, but no tabletop record, participant list, or lessons learned was provided for the sample period.	Run a scenario exercise; record roles, timeline, decisions, gaps, owners, and retest dates.
Medium	Vendor review cadence is unclear. The vendor inventory identifies critical suppliers, but renewal dates and reassessment results are incomplete for two sampled suppliers.	Define review frequency by risk; track due dates, review outcomes, exceptions, and acceptance decisions.

Suggested 60-day sequence

When	Action	Evidence of completion
Days 1-15	Confirm owners and control procedures.	Approved ownership and evidence checklist.
Days 16-30	Complete access review and response exercise.	Signed review record and exercise report.
Days 31-60	Close exceptions and validate recurring evidence.	Closure records and reviewed evidence samples.

Evidence and limitations

All company names, observations, artifacts, priorities, and recommendations above are fictional. A real engagement would validate facts with control owners, distinguish missing evidence from a control failure, and tailor the criteria and findings to the agreed scope. No SOC 2 report or assurance opinion is issued by this review.

Prepared by Larry McCauley | Security readiness advisory