CBCA-AB TABLETOP EXERCISE

Scoring Sheets (Self-Assessment)

Purpose:
Enable organizations to objectively assess whether their current governance, recovery, and security posture can survive **real operational pressure** without silently degrading confidentiality.

This scoring is intended for **internal use only**.

HOW TO USE THESE SHEETS

- Complete **during or immediately after** the tabletop exercise
- Scores must reflect **observed behavior**, not intent
- Any **red-line failure** results in overall **FAIL**, regardless of numeric score
- Partial credit is allowed only where explicitly stated

SCORECARD 1 — Governance Integrity

Measures whether security policy holds under pressure.

Item	Observation	Score
Fail-closed behavior upheld throughout exercise	☐ Yes ☐ No	0 / 5
Any bypass proposed (verbal or implied)	☐ Yes ☐ No	**AUTO-FAIL**
Any undocumented process invented	☐ Yes ☐ No	**AUTO-FAIL**
Policy followed exactly as written	☐ Yes ☐ Partial ☐ No	0 / 3 / 5
Policy ownership was clear and respected	☐ Yes ☐ No	0 / 5

Max Score: 15
Red Line: Any bypass or undocumented process = FAIL

SCORECARD 2 — Operational Discipline

Measures whether operations followed governance instead of improvisation.

Item	Observation	Score
Correct escalation path used	☐ Yes ☐ Partial ☐ No	0 / 3 / 5
Recovery actions executed in correct sequence	☐ Yes ☐ No	0 / 5
Denied operations accepted without workaround	☐ Yes ☐ No	0 / 5
Recovery mode explicitly entered and exited	☐ Yes ☐ No	0 / 5

Max Score: 20
Interpretation: Scores below 15 indicate reliance on informal hero operations.

SCORECARD 3 — Leadership Resolve

Measures executive behavior under availability pressure.

Item	Observation	Score
Leadership explicitly supported fail-closed decisions	☐ Yes ☐ No	0 / 5
“Just this once” language used	☐ Yes ☐ No	**AUTO-FAIL**
Security framed as protection (not outage)	☐ Yes ☐ Partial ☐ No	0 / 3 / 5
Risk acceptance documented, not implicit	☐ Yes ☐ No	0 / 5

Max Score: 15
Red Line: Any informal override or exception = FAIL

SCORECARD 4 — Recovery Hygiene

Measures whether recovery increases risk or resets it.

Item	Observation	Score
Recovery authorization explicitly activated	☐ Yes ☐ No	0 / 5
Recovery access time-bounded	☐ Yes ☐ No	0 / 5

Item	Observation	Score
All recovery grants invalidated after use	☐ Yes ☐ No	**REQUIRED**
Key rotation completed post-recovery	☐ Yes ☐ No	0 / 5
Recovery artifacts re-secured	☐ Yes ☐ No	0 / 5

Max Score: 20
Red Line: Failure to invalidate grants = FAIL

SCORECARD 5 — Cultural Signals (Observer-Only)

Completed by auditor / observer. Not self-scored.

Signal Observed	Yes / No
Operators expressed frustration with controls	☐ Yes ☐ No
Pressure to prioritize speed over integrity	☐ Yes ☐ No
Informal side conversations about bypasses	☐ Yes ☐ No
Clear understanding of *why* controls exist	☐ Yes ☐ No

Interpretation:
Multiple “Yes” responses indicate latent bypass risk even if formal scores are high.

OVERALL RESULT

☐ **PASS** — Governance and controls held under pressure
☐ **FAIL** — One or more red-line failures observed

Note:
A FAIL does not indicate technical weakness.
It indicates **organizational incompatibility with fail-closed security**.

INTERPRETATION GUIDE (FOR PARTICIPANTS)

- **High scores + PASS:**
  Organization is structurally capable of enforcing long-term confidentiality.

- **High scores + FAIL:**
  Cultural or leadership gaps undermine technical controls.
- **Low scores + PASS:**
  Controls exist but are fragile; high risk of future degradation.
- **Low scores + FAIL:**
  Architecture likely collapses under real incident conditions.

If this exercise feels uncomfortable, it is working.

Security that only functions when everything is calm is not security.

What Your Score Means

This exercise is intentionally uncomfortable. That does not mean it failed — it means it worked.

PASS with high scores
Indicates your organization can sustain fail-closed behavior under pressure. Security controls are likely to remain intact during real incidents.

PASS with low scores
Controls exist, but are fragile. Operational or leadership pressure could weaken them during a prolonged or high-stakes event.

FAIL due to bypass or informal overrides
This does not indicate a technical failure. It indicates **organizational incompatibility with fail-closed security models**.

Repeated FAIL outcomes
Suggest that long-term confidentiality risk is being managed implicitly through hero operations, informal exceptions, or post-incident cleanup — not through enforceable controls.

This framework is intended to help teams understand *where* they stand today, not to assign blame.