Annex A — Governance & Recovery Stress Exercise (Self-Assessment Template)

CBCA-AB TABLETOP EXERCISE: "Organizations are encouraged to reuse, modify, and run this exercise internally."

This annex provides a reusable tabletop exercise and scoring framework intended to help organizations evaluate how their existing security controls, governance processes, and leadership decisions behave under real operational pressure.

The exercise is designed to be run without tools, vendors, or architecture changes. Its purpose is not to validate a specific product or solution, but to surface where:

- **fail-closed intent erodes under availability pressure**
- **informal bypasses emerge**
- **recovery workflows expand risk instead of reducing it**

Organizations are encouraged to reuse, adapt, and run this exercise internally using their current controls. Results are for internal assessment only.

The goal is not to "pass," but to reveal where gaps exist — so informed decisions can be made about governance, architecture, and risk tolerance.

Recovery & Rotation Under Fire (90-Minute Decision Simulation)

Objective:
Test whether **governance, discipline, and leadership resolve** hold under pressure — *without touching production systems*.

This exercise evaluates humans, not cryptography.

---

0. Rules of Engagement

1. **The architecture is immutable.**
   CBCA-AB is frozen. No "what if we changed X."
2. **Fail-closed is non-negotiable.**
   If policy does not allow an action, the answer is **NO**.
3. **No imaginary capabilities.**
   Participants may only take actions explicitly allowed by policy.
4. **All decisions are logged.**
   Proposed actions, approvals, hesitations, and bypass suggestions are recorded.

5. **Silence equals denial.**
   If no decision is made, the system denies access.

This is not a discussion.
It is a **decision simulation**.

---

1. Roles (Assign Before Starting)

Each role must be played by a real person.

- **Authority Owner (A)**
  Owns policy, KMS/HSM, grant issuance
- **Inline Enforcement Owner (B)**
  Owns transport enforcement, downgrade prevention
- **Operations Lead**
  Owns restores, uptime, customer/mission pressure
- **Security Lead**
  Owns threat assessment, incident framing
- **Executive Decision Authority**
  Final arbiter of risk acceptance (cannot change policy)
- **Observer / Auditor** *(silent)*
  Records decisions, pressure points, failures

No one may hold more than one role.

---

2. Starting State (T+0)

- Crown-jewel backup restore is **scheduled but not yet started**
- CBCA-AB policies active:
  - CJ-ROOT
  - CJ-RECOVERY (inactive)
- Authority (A) and Inline Enforcement (B) are healthy
- No known breach yet

---

3. Timeline & Injects

🔹 **Inject 1 — T+5 minutes**

Event:
Security monitoring reports *possible historical data exposure*.
No confirmation yet.

Question to group:

- Do you activate CJ-RECOVERY?
- Who authorizes?
- What justification is logged?

Correct Behavior:

- No action yet OR controlled activation with justification
- No policy changes

Failure Signal:

- Early relaxation “just in case”

🔹 **Inject 2 — T+10 minutes**

Event:
Authority (A) latency spikes to 5× normal.

Restore request arrives for crown-jewel dataset.

System Behavior:

- Some unwrap requests denied due to timeout

Questions:

- Do you retry?
- Do you change grant lifetimes?
- Do you cache grants?

Correct Behavior:

- Accept denial
- Escalate, do not bypass

Failure Signal:

- “Temporary” grant extension
- Caching proposals

🔹 **Inject 3 — T+15 minutes**

Event:
Inline Enforcement (B) drops 20% of sessions.

Exec asks:

“Can we bypass the inline box just for recovery?”

Questions:

- Who answers?
- What is the answer?
- How is it logged?

Correct Answer:

- **No**
- Denial framed as protection

Failure Signal:

- Any workaround suggested

🔹 **Inject 4 — T+25 minutes**

Event:
Media / mission pressure injected.

Statement delivered to Exec:

“If restore doesn’t complete in 30 minutes, there will be visible impact.”

Questions:

- Does leadership hold fail-closed?
- Does Ops propose shortcuts?

Correct Behavior:

- Accept delay
- Communicate risk transparently

Failure Signal:

- Informal override
- “One-time exception” language

🔹 **Inject 5 — T+35 minutes**

Event:
Security confirms **no active exfiltration**, but **keys may be exposed** historically.

Recovery now required.

Action Required:

- Activate CJ-RECOVERY

Checklist (must be verbalized):

- Multi-party authorization
- Logged activation
- Scope limitation
- Time-bounded grants

Failure Signal:

- Broad or vague authorization
- Missing documentation

🔹 Inject 6 — T+50 minutes

Event:
During recovery, Authority (A) denies multiple requests due to rate limits.

Ops Lead says:

"We're doing everything right — the system is blocking us."

Questions:

- Do you change rate limits?
- Do you pause recovery?
- Do you escalate?

Correct Behavior:

- Escalate
- Accept pause
- Do not weaken policy

Failure Signal:

- "Raise limits just for now"

🔹 Inject 7 — T+70 minutes

Event:
Recovery completes **partially**.

Remaining steps require:

- Re-wrapping data
- Grant invalidation
- Deactivation of CJ-RECOVERY

Questions:

- Are all grants invalidated?
- Is recovery mode exited?

- Is post-incident review scheduled?

Failure Signal:

- Leaving recovery mode active
- Reusing grants

---

4. End State (T+90 minutes)

Exercise ends regardless of outcome.

---

5. Scoring (Binary, Not Feelings)

PASS if:

- No bypasses proposed or implemented
- Fail-closed accepted under pressure
- Escalation followed governance
- All denials logged and justified
- Recovery completed or aborted cleanly

FAIL if:

- Any bypass suggested
- Any “temporary” weakening proposed
- Any undocumented action taken
- Any cached or extended grants
- Leadership overrode policy

One failure = exercise failure.

---

6. Debrief Questions (Mandatory)

1. Where was pressure highest?
2. Who felt tempted to bypass?

3. Was denial clearly understood as protection?
4. Did escalation paths work?
5. Would this hold at 3am during a real outage?

No blame. Only truth.

---

7. Why This Matters

“If we fail here, we would absolutely fail in production.”

This exercise determines **organizational compatibility**, not technical validity.