BREAKWATER ASOC / RESPONSE EVALUATION

Evaluate the reasoning. Test the authority to act.

Response orchestrates the Agentic AI SOC investigation. Evaluate the Council's reasoning, digital rehearsal and human control against one reproducible operational case.

ILLUSTRATIVE STARTING QUESTION / SUSPICIOUS WORKSTATION ACTIVITY

Is containment justified, and what would make it safe to authorize?

An engineering workstation behaves unusually after maintenance. Examine intrusion and legitimate change before choosing an intervention.

Observations → Council & rehearsal → Authorized proposal

01

Establish the case

Agree observations, time window and known alternatives. Record your current investigation and approval baseline.

Retain: A reproducible case, owners and success criteria.

02

Challenge the reasoning

Review Council explanations, citations, dissent and evidence gaps. Record the AI mode and actual model outputs.

Retain: An investigation record and corrected assertions.

03

Rehearse the proposal

Compare interventions in the agreed model or lab. Review targets, impact, recovery and verification.

Retain: A scenario comparison and bounded response proposal.

04

Test the control gates

Test approvals, changed targets and dry-run failures. Check outcomes and recovery on the supported test path.

Retain: Expected versus observed gate and outcome results.

Record whether AI is scripted or live. Agree the backend, adapters and test environment; authorize production changes separately.

ACCEPTANCE CRITERIA / REASONING, AUTHORITY & OUTCOMES

A useful answer. A controlled operational decision.

Compare the same case and proposed action with your baseline. Agree reasoning measures and mandatory gates before testing; record failures and successful runs.

EVALUATION SCORECARD / AGREE TARGETS WITH YOUR TEAM

What to assess	Evidence to retain	Measures to agree
Investigation quality	Hypotheses, cited observations, dissent and open questions.	Supported conclusions, unsupported assertions and time to review.
Rehearsal usefulness	Scenario inputs, intervention options and assumptions.	Differences explained; impact and recovery reviewed by operations.
Authorization integrity	Approval scope, expiry, evidence and target checks.	Expired or changed approvals blocked; fresh authorization required.
Execution boundaries	Dry-run results and supported adapter/target scope.	Mismatches and failed dry runs block the tested action.
Verification & recovery	Service checks, compensation results and intervention record.	Outcome verified; recovery failures escalated with an assigned owner.

Exercise failure cases in a controlled test environment.

Test expired approval, changed target, dry-run mismatch and failed health checks. Check supported compensation and escalation. Name security, operations and recovery owners before execution.

YOUR EVALUATION DELIVERABLE / DECISION BRIEF

Case & AI configuration

Inputs, baseline and scripted/live mode.

Reasoning & proposal

Evidence, alternatives and human decision.

Control test results

Expected blocks and observed outcomes.

Operational decision

Fit, remaining gaps and accountable owners.

Bring a case your team must decide on.

Request a Response demo