Scenario Weighting Guide: *Public-Cloud Misconfiguration*

Domain	**Sub-Metric**	**Weight (w_i)**	**Justification**
Procedural Alignment	Escalation path followed	**4**	Cloud exposure incidents may go unnoticed without escalation. Timely involvement of appropriate roles (e.g., cloud security lead, legal) is crucial for containment and breach notification.
Procedural Alignment	IRP referenced during incident	**4**	Most SMEs lack cloud-specific playbooks. Referencing a prepared IRP reduces error and delays in high-stakes misconfigurations.
Procedural Alignment	Deviations justified	**3**	If deviations from the IRP occur (e.g., due to third-party misconfig tools), they must be documented to maintain auditability and compliance posture.
Operational Execution	Containment-action timing	**5**	Exposure windows can lead to PII disclosure. Delayed containment (e.g., closing public S3 buckets) directly increases regulatory and reputational risk.
Operational Execution	Task coverage	**5**	Cloud misconfigs often involve multiple interlinked permissions or storage classes. All affected services must be addressed to prevent recurrence.
Operational Execution	Execution accuracy	**5**	A misstep (e.g., applying the wrong IAM role or mis-scoping a policy) can reintroduce risk or break production systems.
Infrastructure Integration	Tool-usage effectiveness	**5**	SMEs often lack automated CSPM or DLP tools. Effectiveness in using available tools (e.g., AWS Config, Azure Policy, logs) defines success in these scenarios.
Infrastructure Integration	Tool alignment to IRP	**4**	Pre-authorised tooling (defined in IRP) ensures cloud diagnostics and remediation can proceed without delay or missteps.
Infrastructure Integration	Inter-tool visibility	**4**	Many cloud tools are siloed. Visibility across identity, storage, and networking layers is essential to track access and change events.
Coordination & Communication	Role clarity	**4**	Public cloud roles (DevOps, Cloud Admin, Security) must be well defined. Delays often arise from ambiguity in who is responsible.
Coordination & Communication	Decision flow	**4**	Cloud misconfigs may require urgent decisions (e.g., disabling a pipeline or revoking access). Decision flow must be clear and fast.
Coordination & Communication	Communication logging	**3**	While not always critical during active response, full comms logs are essential for forensic review and regulator interaction post-incident.
Post-Incident Follow-through	Root-cause analysis	**5**	Must identify not just the misconfigured setting, but *why* it happened — e.g., poor CI/CD validation, IAM sprawl, third-party misconfiguration.
Post-Incident Follow-through	Lessons learned	**4**	Misconfigurations often stem from repeatable process issues. Capturing learnings and updating pipelines and guardrails is essential.
Post-Incident Follow-through	IRP updated post-simulation	**3**	IRP may not have covered cloud-specific scenarios; post-update ensures preparedness for similar future events.

Weighted total = 62