Evaluator Scoring Rubric: Public-Cloud Misconfiguration

Domain	Sub-Metric	Score = 0	Score = 1	Score = 3	Score = 4	Score = 5
Procedural Alignment	Escalation path followed	No escalation occurred	Escalation too late or unclear	Escalated but misrouted or incomplete	Mostly followed with minor delay	Escalated promptly and correctly
	IRP referenced during incident	IRP not consulted	Referenced only after incident escalation	Consulted intermittently	Mostly referenced with some gaps	Used proactively throughout
	Deviations justified	Deviations undocumented	Justified but not documented	Partially justified post-facto	Mostly justified in action logs	All deviations well justified and recorded
Operational Execution	Containment-action timing	No containment or excessive delay	Containment after exposure confirmed	Containment in 2 to 30 mins	Actioned in 10 to 20 mins	Prompt containment within 10 mins
	Task coverage	Only one misconfiguration addressed	Multiple errors missed or partially corrected	Most configurations fixed	Nearly all fixed, one minor missed	All misconfigurations addressed
	Execution accuracy	Changes caused further misconfiguration	Frequent errors or misapplied controls	Mostly correct with minor mistakes	Accurate with minor issues	All tasks completed correctly
Infrastructure Integration	Tool-usage effectiveness	No tooling used for misconfig analysis	Basic cloud tools used reactively	Manual and tool-based detection combined	Tooling used effectively, small gaps	Automated tools used proactively
	Tool alignment to IRP	No tooling aligned to IRP	Used unapproved or untracked tooling	Partially aligned tools	Mostly aligned with IRP guidance	All tools aligned with IRP procedures
	Inter-tool visibility	No telemetry or cloud logs collected	Logs fragmented across platforms	Partial log correlation	Logs aligned with gaps	Full visibility across systems
Coordination & Communication	Role clarity	Team unsure who owns cloud remediation	Cloud roles confused with on-prem roles	Mostly clear, some overlap	Roles followed with one confusion point	All cloud roles clearly followed
	Decision flow	Cloud response decisions blocked or delayed	Ad hoc or unclear decisions	Mostly informed decisions with some delay	Timely with minor misalignment	Quick, structured decisions on changes
	Communication logging	No communication documented	Partial documentation, some gaps	Major actions logged manually	Most actions logged, minor gaps	Fully documented, accessible logs
Post-Incident Follow-through	Root-cause analysis	No RCA or misdiagnosis of cloud issues	Surface-level config issue documented	Clear config root cause but no process link	RCA included root + access flaws	Full RCA covering config, access, policy
	Lessons learned	No reflection on config practices	Verbal discussion only	Written observations, no formal follow-up	Formal lessons noted, not yet implemented	Lessons documented and controls updated
	IRP updated post-simulation	No update	Noted verbally, no draft	Draft changes underway	Revised but not ratified	IRP updated, tested, and versioned