Scenario Weighting Guide: Credential Leakage

Domain	Sub-Metric	Weight (w_i)	Justification
Procedural Alignment	Escalation path followed	4	Leaked credentials often require escalation to security and identity governance teams, especially when privileged accounts are involved.
Procedural Alignment	IRP referenced during incident	4	IRP should include credential exposure response steps (account disablement, re-auth policy, MFA reset).
Procedural Alignment	Deviations justified	3	Variance from IRP may occur if real-time conditions change; these must be rationalised and documented to retain defensibility.
Operational Execution	Containment-action timing	5	Time is critical—any lag in account disablement or session invalidation can result in deeper compromise.
Operational Execution	Task coverage	5	Password reset alone is insufficient. Session tokens, OAuth keys, and federated identities must also be revoked.
Operational Execution	Execution accuracy	5	Mistakes in user disablement or token revocation may escalate the breach or affect production systems.
Infrastructure Integration	Tool-usage effectiveness	5	Effectiveness of IAM, SIEM, or IDP tools (e.g., Azure AD, Okta, CrowdStrike) is central to timely containment.
Infrastructure Integration	Tool alignment to IRP	4	Pre-configured tooling helps streamline triage and reduces delay in remediation.
Infrastructure Integration	Inter-tool visibility	4	Visibility into which systems a credential accessed (Cloud, VPN, SaaS) is essential for scoping.
Coordination & Communication	Role clarity	4	Clarity on who controls identity systems is crucial; often delays stem from HR, IT, or vendors not knowing who owns response.
Coordination & Communication	Decision flow	4	Must support fast revocation and system lockout decisions. Waiting on consensus can cost breach depth.
Coordination & Communication	Communication logging	3	Logs should reflect who disabled the user, who approved it, and any investigative notes for future audit.
Post-Incident Follow-through	Root-cause analysis	5	Knowing how the credentials leaked (phishing, repo leak, MFA bypass) is fundamental for recovery and prevention.
Post-Incident Follow-through	Lessons learned	4	SMEs may not fix bad credential hygiene (e.g., hard-coded keys) without structured post-event reflection.
Post-Incident Follow-through	IRP updated post-simulation	3	If the IRP lacked credential leakage response steps, updating it ensures preparedness for repeat events.

Weighted Total = 62