Insider Threat Scenario Weighting

Domain	Sub-metric	Weight (w_i)	Justification (Scenario-specific criticality)
Procedural Alignment	Escalation path followed	4	Critical to ensure insider risk is escalated promptly, especially if legal/compliance risk is involved.
	IRP referenced during incident	4	The IRP must cover insider threats and legal handling procedures.
	Deviations justified	3	IRP deviations might occur due to sensitivity of HR/legal issues but must be well documented.
Operational Execution	Containment-action timing	4	Prompt account suspension or device isolation can prevent further leakage.
	Task coverage	4	Exfiltration vectors (USB, cloud sync, email) must all be assessed and contained.
	Execution accuracy	5	Mistakes (e.g., misidentifying a user or missing a channel) can lead to irreversible data loss.
Infrastructure Integration	Tool-usage effectiveness	5	Data Loss Prevention (DLP), audit logs, and endpoint monitoring are critical for insider threat detection.
	Tool alignment to IRP	4	Tools need to align with insider threat response protocols to avoid delays or mishandling.
	Inter-tool visibility	4	Visibility between EDR, DLP, and file system logging tools is vital for tracing activity.
Coordination & Communication	Role clarity	3	Important to know who has authority to lock accounts or notify legal/HR.
	Decision flow	4	Timely and precise decision-making (especially across IT–HR–legal) is essential.
	Communication logging	4	Logging all actions is crucial for audit and legal review.
Post-incident Follow-through	Root-cause analysis	5	Necessary to assess intent (negligent or malicious) and system vulnerabilities.
	Lessons learned	4	Helps improve access controls, monitoring policies, and HR processes.
	IRP updated post-simulation	3	IRP updates ensure insider handling policies are more effective post-incident.

Weighted Total = 60