Investigative Pacing

Timing and Decision Points (KA-MOD-022)

Mastering the shift between **rapid response** and **deliberate analysis** to maximize evidence preservation and investigative integrity.

1. The Dual Modes of Investigation

⚡ Rapid Response (Speed)

Prioritizes immediate action to mitigate ongoing harm or loss of critical evidence (volatile data).

Goal: Containment and Preservation.

- **Actions:** Isolate systems, suspend access, capture volatile memory (RAM), take initial snapshots.
- **Timing:** Minutes to hours.

🔬 Deliberate Analysis (Accuracy)

Prioritizes thoroughness, cross-referencing, and synthesis to build a defensible narrative.

Goal: Synthesis, Conflict Resolution, and Reporting.

- **Actions:** Deep-dive forensics, data modeling, interviewing, legal review, report drafting.
- **Timing:** Days to weeks.

↕

2. The Critical Shift: When to Change Pacing

⬇️ Shift DOWN: Speed to Accuracy

When you must slow down to prevent error.

- All volatile data is secured.
- Incident is fully contained.
- A major conflict in evidence is found (requires KA-MOD-021).

TIMING JUDGEMENT

The Investigator's core responsibility is defining the appropriate mode.

Risk of Loss vs. **Risk of Error**

⬆️ Shift UP: Accuracy to Speed

When a new finding necessitates immediate action.

- A new, active threat is discovered.
- New evidence is about to be wiped (e.g., auto-deletion policy timer).
- Required stakeholder notification timeline is immediate.

3. The High-Cost Error: Rushing Synthesis

⚠️

The Critical Mistake: Premature Conclusion

The largest pacing error is moving from the Rapid phase to reporting without sufficient **Deliberate Analysis**.

A rushed conclusion risks overlooking contradictory evidence, leading to an **unreliable or indefensible final finding**.

KA-MOD-022 | Good investigative timing is not about being fast, but about being **deliberately paced** to ensure both evidence integrity and report accuracy.