Parameters for Orgo Customization

Based on your feedback, I have refined the parameters, making them more nuanced and versatile for diverse organizations. The goal is to create a system that is not only intuitive but also flexible enough to handle varying workflows, risks, and organizational goals.

---

1. Reactivity Time

Definition: How quickly unresolved issues escalate to higher levels or trigger responses.

Improved Levels:

1 (Relaxed): Escalation happens after days or weeks (e.g., book clubs).

2 (Moderate): Escalation occurs within 24–72 hours (e.g., retail organizations).

3 (Responsive): Escalation happens within 12–24 hours (e.g., advocacy groups, environmental collectives).

4 (Urgent): Escalation occurs within hours (e.g., hospitals, construction sites).

5 (Immediate): Escalation happens within minutes (e.g., military, crisis management teams).

New Feature: Custom Reactivity Profiles.

Set separate reactivity times for different categories (e.g., Safety: Immediate; Routine: Relaxed).

---

2. Transparency vs. Privacy

Definition: Controls the visibility of information across the organization.

Refined Levels:

1 (Highly Private): Information is visible only to direct recipients unless explicitly escalated (e.g., military).

2 (Moderately Private): Visible to a small, predefined group (e.g., faith-based organizations).

3 (Balanced): Distributed to relevant teams and stakeholders (e.g., retail, hospitals).

4 (Moderately Transparent): Shared with most organizational members (e.g., advocacy groups, environmental organizations).

5 (Fully Transparent): Visible to the entire organization by default (e.g., cultural preservation associations).

New Feature: Dynamic Transparency Levels.

Adjust visibility based on the severity or category of the information (e.g., Safety issues: Transparent; HR complaints: Private).

---

3. Escalation Granularity

Definition: Determines the specificity and number of steps in the escalation process.

Enhanced Levels:

1 (Broad Escalation): Skips intermediate levels, escalating directly to higher authorities.

2 (Accelerated Escalation): Escalates faster, bypassing some intermediate levels.

3 (Moderate Escalation): Follows key escalation steps (e.g., staff → manager → VP).

4 (Detailed Escalation): Escalates through every intermediate level methodically.

5 (Granular Escalation): Requires approvals or responses at every level before moving upward.

New Feature: Escalation Paths by Role.

Customize escalation paths for specific roles or departments.

---

4. Review Frequency

Definition: How often periodic reviews are conducted to identify patterns or assess unresolved issues.

Improved Levels:

1 (Rare): Annually or on an ad-hoc basis (e.g., small social clubs).

2 (Occasional): Quarterly reviews (e.g., regional retail chains).

3 (Moderate): Monthly reviews (e.g., faith-based organizations, advocacy groups).

4 (Frequent): Weekly reviews (e.g., hospitals, medium-sized corporations).

5 (Continuous): Daily or even real-time reviews (e.g., military, high-risk industries).

New Feature: Adaptive Review Scheduling.

Frequency adjusts dynamically based on the volume or severity of cases logged.

---

5. Notification Scope

Definition: Determines the scope of people notified about specific messages or updates.

Refined Levels:

1 (Individual): Notifies only the recipient.

2 (Small Team): Notifies immediate stakeholders.

3 (Department): Notifies the entire department or functional group.

4 (Organization-Wide): Notifies all relevant roles in the organization.

5 (Public): Notifies external stakeholders or the general public (e.g., advocacy campaigns).

New Feature: Granular Notification Rules.

Customize notification scope based on the category or urgency of the information.

---

6. Pattern Sensitivity

Definition: How quickly repeated similar incidents are flagged as a pattern and escalated.

Refined Levels:

1 (Low Sensitivity): Patterns are detected only after extended periods or high repetition.

2 (Moderate Sensitivity): Patterns are flagged after moderate repetition (e.g., 5 cases in 6 months).

3 (Balanced): Balanced detection of patterns within weeks or months.

4 (High Sensitivity): Patterns are flagged after a few similar incidents (e.g., 3 cases in 1 month).

5 (Immediate Sensitivity): Patterns are flagged after just 1–2 similar incidents (e.g., safety-critical areas like hospitals).

New Feature: Custom Pattern Rules.

Sensitivity levels can vary for different categories (e.g., high for Safety, low for Routine).

---

7. Severity Escalation Threshold

Definition: The level of severity required for immediate escalation.

Enhanced Levels:

1 (Very High Threshold): Only severe, life-threatening issues escalate immediately.

2 (High Threshold): Severe and moderately critical issues escalate.

3 (Balanced Threshold): Both moderate and minor issues can escalate depending on context.

4 (Low Threshold): Even minor issues escalate quickly.

5 (No Threshold): All reports escalate immediately (e.g., crisis management).

New Feature: Severity Tagging System.

Automatically classify issues with severity tags (e.g., Critical, Major, Minor) based on content.

---

8. Logging and Traceability

Definition: The level of detail and depth recorded for actions and decisions.

Improved Levels:

1 (Minimal): Logs only high-level actions (e.g., case opened, case closed).

2 (Moderate): Logs key actions and updates.

3 (Detailed): Logs all actions, decisions, and communications.

4 (Audit-Ready): Includes compliance tags and timestamps for every action.

5 (Full Traceability): Logs everything, including metadata (e.g., IP addresses, user activity).

New Feature: Custom Logging Depth.

Adjust logging depth for different categories (e.g., detailed for Compliance, minimal for Routine).

---

9. Automation Level

Definition: Determines how much of the workflow is automated.

Refined Levels:

1 (Manual): Most actions require human input.

2 (Low Automation): Automates basic tasks like notifications and case logging.

3 (Moderate Automation): Automates routing, periodic reviews, and reporting.

4 (High Automation): Includes automated escalation and pattern recognition.

5 (Fully Automated): End-to-end automation, including decision-making and predictive analytics.

New Feature: Automation Profiles.

Apply different automation levels to categories (e.g., Safety: Fully Automated; HR: Manual).

---

10. Data Retention Policy

Definition: How long records and logs are stored in the system.

Improved Levels:

1 (Short-Term): Retain for 3–6 months (e.g., small clubs, short-term projects).

2 (Moderate): Retain for 1–5 years (e.g., retail, medium organizations).

3 (Long-Term): Retain for up to 10 years (e.g., healthcare, compliance-heavy industries).

4 (Indefinite): Retain until manually deleted (e.g., military, government agencies).

5 (Regulated): Adjusts automatically to comply with laws (e.g., GDPR, HIPAA).

New Feature: Category-Specific Retention Rules.

Set different retention periods for categories (e.g., Compliance: 10 years; Routine: 1 year).

---