ReguLight Logic & Algorithms Guide

This guide provides a comprehensive overview of the ReguLight logic, focusing on the mathematical frameworks that translate operational health into risk intelligence.

Control Effectiveness: From Static to Dynamic

ReguLight differentiates between a control's design and its execution. While the **Control Risk Reduction Factor (CRRF)** defines the theoretical maximum effectiveness (0–100%) under perfect conditions, the system calculates the **Current Effectiveness** to reflect real-world degradation.

The Worst-Case Logic Algorithm

ReguLight adopts a pessimistic, safety-first approach. The algorithm assumes that the most severe failure defines the control's limit, preventing the system from masking critical vulnerabilities with minor successes.

The Calculation Process

1. **Baseline Initialization:** The process begins with a perfect operational health factor of 1.0.
2. **Multi-Source Evaluation:** The system scans four distinct "Degradation Sources":
    - **Incidents:** Identifies catastrophic failures where the control failed to prevent or detect a threat.
    - **Issues:** Proactive findings (e.g., from audits) that signal potential future failures.
    - **Overdue Tasks:** Signals operational decay when maintenance or standard operations are neglected.
    - **Overdue Document Reviews:** Identifies "documentation drift," where procedures may no longer match current technical realities.
3. **Factor Selection:** Every issue is assigned a decimal factor. The system ignores averages and selects the **Minimum (Worst) Factor**.
4. **Final Computation:** The Current Effectiveness is the product of the Baseline CRRF and the Worst Factor.

Severity and Impact Reference Table

The following factors are applied based on the severity of the findings:

Source	Category / Level	Factor	System Meaning
Incidents	Critical / High	0.0	Control is completely ineffective
	Medium / Low	0.5	Control operates at 50% capacity
Issues	4 (Critical)	0.5	50% effectiveness reduction
	3 (High)	0.7	30% effectiveness reduction
	2 (Medium)	0.8	20% effectiveness reduction
	1 (Low)	0.9	10% effectiveness reduction
Tasks	Any Overdue	0.8	Signals operational blind spots
Documents	Any Overdue	0.8	Signals procedural obsolescence

Residual Risk: The Layered Defense Algorithm

Residual risk is the quantified threat remaining after controls are applied to the **Inherent Risk** (the risk score before any mitigation).

Dimension Separation

ReguLight calculates Likelihood and Impact independently because different control types serve different functions:

- **Likelihood Controls:** Preventive, Organizational, and Technical controls designed to stop a threat from occurring.
- **Impact Controls:** Detective, Corrective, and Technical controls designed to minimize damage once a threat occurs.

The 8-Step Calculation Workflow

The system uses the following method for both dimensions:

1. **Decimal Conversion:** Control effectiveness percentages (e.g., 85%) are converted to decimals (0.85).
2. **Averaging Effectiveness:** The system calculates the average effectiveness of all controls in the set. This ensures that one poorly performing control is visible and pulls down the overall score.
3. **Redundancy Multiplier:** To reward "Defense in Depth," ReguLight applies a multiplier: 1.0 + (0.5 x number of extra controls).
4. **Multiplier Cap:** The multiplier is **capped at 2.0**. This accounts for diminishing returns where overlapping controls provide no additional unique benefit.
5. **Reduction Factor:** The Average Effectiveness is multiplied by the Multiplier to determine the raw reduction.
6. **90% Safety Cap:** No matter how many controls exist, the reduction is capped at **0.90 (90%)**. This accounts for "Black Swan" events, zero-day exploits, and unknown vulnerabilities.
7. **Real-World Dampening:** A constant factor of **0.85 (85%)** is applied to the capped reduction to account for implementation gaps, configuration drift, and human error.
8. **Final Scaling:** The result is applied to the inherent risk score and rounded to the nearest integer on a 1–4 scale.

Algorithmic Principles

- **Anti-Aggregation:** Multiple issues do not multiply (e.g., 0.5 x 0.8). This prevents "double-counting" and ensures the calculation remains simple yet conservative.
- **Visibility of Failure:** Even if a risk score remains "Low" due to redundancy, a failed control is immediately apparent because it drops the average effectiveness metric.
- **Recovery Prioritization:** The system identifies a clear "Recovery Path". Resolving the "Worst Factor" (e.g., a Critical Incident) provides the most immediate improvement to the score.
- **Dynamic Response:** As operational data changes (e.g., a task becomes overdue or an incident is closed), the residual risk score updates automatically, providing a living risk posture.