DOCUMENT 01 / 05 · THE FRAMEWORK

The Four Pillars.

A modular operating system for resilient, insurable, security-by-default operations.

IR 1.0 was reactive — alert fatigue, 3 a.m. panic, security bolted on as an afterthought. IR 2.0 reframes incident response as an operating system built on four load-bearing pillars: Governance, Architecture, Technology, and Culture. This document defines each pillar, the Calm Loop that ties them together, and the first principles that govern the whole.

SERIES	DOCUMENT	VERSION	LICENSE
IR 2.0	01 of 05	1.3 · 2025	CC BY 4.0

PREMISE

Most incident response programs are built to survive a fire. Few are built to prevent one.

IR 2.0 is a deliberate replacement for a model that was always temporary. We treat resilience as engineering — composable, evidence-based, insurable — not heroics.

— IR 1.0 · The way it was	— IR 2.0 · The way forward
REACTIVE FIREFIGHTING	**PROACTIVE, SYSTEMATIC RESILIENCE**
Alert fatigue, unclear roles	Security by default architecture
Security bolted on as an afterthought	Automated, reversibility-gated response
3 a.m. panic, improvised responses	Insurable, auditable, evidence-based
Audit-driven, not outcome-driven	Outcome-driven, modular, testable

> *Resilience is not a department. It is a property of the system itself.*

THE FRAMEWORK

Four pillars. One system.

Each pillar answers a different question. Together, they form a load-bearing structure — strong enough to fail safely, simple enough to adopt incrementally.

01 Governance

The Why & The Proof

- Risk & governance posture
- IR plan & playbooks
- Tabletop drills
- KPIs & metrics
- Insurability evidence

02 Architecture

The How — Foundation

- Security by default
- IAM & Zero Trust
- Network segmentation
- Immutable backups
- Cloud-native ready

03 Technology

The What — Tools

- EDR / XDR detection
- SIEM visibility
- SOAR automation
- AI-assisted triage
- The Calm Loop

04 Culture

The Who — Brain

- Blameless post-mortems
- Threat intelligence
- Continuous learning
- Team sustainability
- Future-proofing

THE CALM LOOP

Automated response, in four moves.

The Calm Loop is the operational heartbeat of IR 2.0 — a closed cycle that turns alerts into action, and action into learning. Each step has explicit inputs, outputs, and a reversibility gate.

01 ↓

Sense

DETECT & ENRICH

Signals from EDR, SIEM, identity, and email gateways are normalized and enriched with threat context before reaching a human.

→

02 ↓

Decide

APPLY RS GATES

Each candidate action is scored on Reversibility. RS-1/2 auto-execute; RS-3+ require approval. Decisions are logged as evidence.

→

03 ↓

Act

EXECUTE PLAYBOOK

The matching playbook runs end-to-end: contain, revoke, notify. Every step emits a structured artifact for downstream review.

→

04 ↺

Learn

IMPROVE & EVOLVE

A blameless post-mortem feeds back into playbooks, automation, and training. The loop gets faster every time it runs.

↺

WHAT THE LOOP GUARANTEES

Three properties make the Calm Loop different from traditional SOAR. *First*, every action carries a reversibility score, so automation is never riskier than its rollback path. *Second*, every step writes evidence — the artifact *is* the audit. *Third*, the learning step is a first-class node, not a checkbox; the loop is designed to improve itself.

The result is a response system that scales without scaling the team. Calm comes from the certainty that the system has already handled the easy work, leaving humans for the calls only humans can make.

≤15m

AUTO-CONTAIN TARGET — RUN PHASE

RS-2

DEFAULT AUTO-EXECUTE CEILING

100%

ACTIONS CAPTURED AS EVIDENCE

FIRST PRINCIPLES

Six rules. Every decision flows from them.

P · 01

Security by default

Built in, not bolted on. The default configuration is the safe configuration; opt-out, not opt-in.

P · 02

Modular by construction

Adopt what you need, when you need it. Every component stands alone and composes without rewrites.

P · 03

One control, many checkboxes

A single control evidences against multiple frameworks. Compliance is a side effect of doing the work.

P · 04

Evidence as data

Tickets, logs, tests, and artifacts *are* the proof. If it isn't queryable, it didn't happen.

P · 05

Reversibility-gated automation

Automation may move only as fast as its undo path. RS classification governs every action.

P · 06

Insurance as North Star

Insurer applications are the field's most honest gap assessment. Treat them as your free roadmap.

WHERE TO GO NEXT

Read *02 — Crawl, Walk, Run* to map your current posture to a phased adoption path. *03 — The Insurability Cheat Code* is the gap assessment that tells you what to fix first.

GET THE FRAMEWORK

deretti.com/ir2