Perimity™ Cyber Evidence Framework

FRAMEWORK

Translating Operational Security Controls into Financially Defensible Proof for Healthcare Organizations

THE STRUCTURAL GAP

Cybersecurity implementation and cyber insurance interpretation operate under different definitions.

Healthcare organizations often maintain appropriate controls, yet struggle to demonstrate them in underwriting-aligned form.

This gap creates renewal friction, policy ambiguity, and potential claim negotiation risk.

THE FRAMEWORK MODEL

The Perimity Cyber Evidence Framework™ establishes a structured approach built on four pillars:

I. Underwriting Alignment
Align controls to insurer evaluation criteria.

II. Control Validation Domains
Prioritize high-impact areas influencing underwriting and claims.

III. Evidence Integrity
Standardize documentation to reduce interpretation ambiguity.

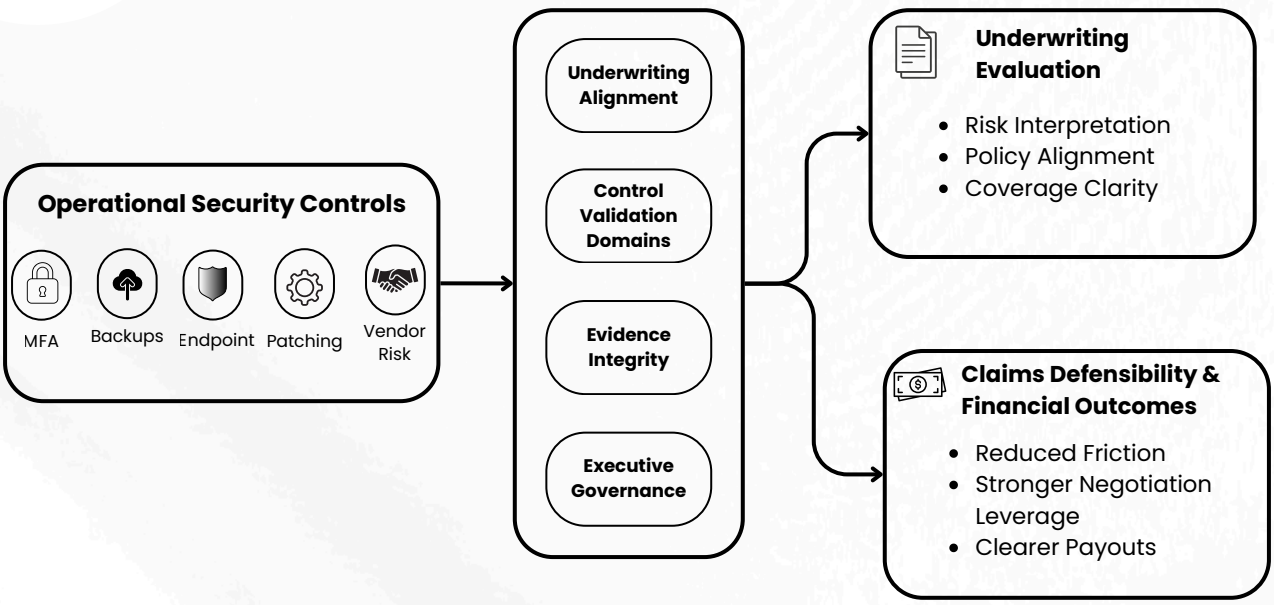
IV. Executive Governance
Establish ownership and continuous validation processes.

FRAMEWORK STRUCTURE

By aligning operational controls with insurance interpretation, organizations improve underwriting clarity and strengthen claim defensibility before incidents occur.

cjacobs@perimity.io
(813) 609-0976

Perimity™ Cyber Evidence Framework



PILLAR FUNCTIONS

Pillar I — Underwriting Alignment
Clarifies insurer interpretation of operational controls.

Pillar II — Control Validation Domains
Focuses validation on areas driving underwriting decisions.

Pillar III — Evidence Integrity
Ensures defensible documentation across review and claims.

Pillar IV — Executive Governance
Establishes accountability for continuous readiness.

OUTCOMES

- Reduced renewal friction
- Greater underwriting clarity
- Improved policy alignment
- Stronger claim defensibility
- Clear translation between technical and insurance language

cjacobs@perimity.io
(813) 609-0976