CROWNSTONE
STRATEGY GROUP

Five Questions Your Security Program Can't Answer

A Practitioner's Framework for Human-Centered Security Assessment

Olutobi Oyinlade, PhD
Crownstone Strategy Group | The Cybersecurist
NEXUS Conference 2026 | University of North Texas

THE PROBLEM

Your Security Program Passes Every Audit. That's the Problem.

50+

assessments revealing the same pattern

$2M+

in hidden risk exposure despite passing audits

> *"If you learned tomorrow that you were breached 6 months ago, where would you say you were lucky rather than good?"*

The gap wasn't in their tools. It was in the questions nobody was asking.

THE GAP

What Standard Frameworks Were Never Designed to Find

Standard Frameworks	The Cybersecurist Lens™
Check if controls exist	Ask if controls work given human reality
Prescriptive — tells you what to build	Diagnostic — reveals how it actually operates
Point-in-time compliance snapshot	Identifies drift, decay, and compounding failure
Measure against an external standard	Measure against the system's own assumptions
Tool-agnostic, human-agnostic	Human-centered — built around behavior
Pass / Fail	Where are you lucky rather than good?

These aren't better answers to the same questions. They're entirely different questions.

THE FRAMEWORK

The Cybersecurist Lens™

A sequential diagnostic built on systems thinking, not checklists



01 What is this system optimizing for?



02 Where does it rely on perfect human behavior?



03 Which assumptions are no longer true?



04 How does failure emerge quietly over time?



05 Where does clarity reduce risk more than control?

Sequential and compound — each question builds on the last

01 QUESTION ONE

What is this system optimizing for?

HOW THE LENS ANSWERS THIS

Map stated objectives
vs. where resources actually flow

Trace budget, time, and attention
to reveal the hidden objective function

Identify optimization drift
— was it always optimizing for this,
or did priorities shift unnoticed?

CASE EXAMPLE

A healthcare org listed 'patient data protection' as priority #1. The Lens mapped where their security budget actually went:

60% → audit preparation
Patient protection was 4th — behind compliance reporting, vendor assessments, and policy docs.

The system had drifted from protecting patients to passing audits. Nobody noticed because the audits kept passing.

Why frameworks miss this: NIST and ISO confirm controls exist — they don't ask whether the program is oriented toward the right outcomes. The Lens maps the gap between stated priorities and actual resource allocation.

02 QUESTION TWO

Where does it rely on perfect human behavior?

Must Always Do

Procedures requiring consistent execution without automation

Must Never Do

Security that fails if someone takes a shortcut or errs

Must Correctly Judge

Decisions requiring expertise that may not be present

Case: A financial services firm had a 47-step IR plan requiring 6 correct judgment calls in the first 15 minutes — including whether to wake the CISO. The Lens mapped every point of human dependency. **The plan had never been tested with a junior analyst on a holiday weekend.**

Why frameworks miss this: Compliance asks 'does an IR plan exist?' The Lens asks 'can a real human execute this plan under real conditions?' It maps every single point where a human error creates a security event.

03 QUESTION THREE

Which assumptions are no longer true?

WHEN IT WAS BUILT

- The network perimeter matters
- All employees are in-office
- Data lives in one cloud
- Security team has 12 people

WHAT'S TRUE NOW

- Zero trust, identity is the perimeter
- 70% remote or hybrid
- Multi-cloud + SaaS sprawl
- Team has 6 people + contractors

Lens methodology: Systematically surface technical, organizational, environmental, and temporal assumptions — then test which ones still hold.

Why frameworks miss this: Frameworks measure against a fixed standard. The Lens measures the system against its own original assumptions — and checks if the world has moved on.

04 QUESTION FOUR

How does failure emerge quietly over time?

Accumulating Debt

Technical debt deferred. Exceptions becoming the norm. Documentation falling behind reality.

Eroding Margins

Safety buffers consumed. Redundancies bypassed. Response times slowly lengthening.

Normalizing Deviance

Workarounds become standard. Warnings routinely ignored. "That's just how we do it."

Broken Feedback

Metrics no longer reflect reality. Reports unread. Alerts tuned out. Reviews without changes.

Case: Firewall exception list: **340 total → 280 older than 6 months → 12 reviewed in the last year.** Those weren't exceptions anymore. They were the actual policy.

05 QUESTION FIVE

Where does clarity reduce risk more than control?

ADDING CONTROL

Controls layered on controls. Approvals that don't add value. Restrictions that create workarounds. Compliance activities disconnected from actual risk.

ADDING CLARITY

People understand WHY controls exist. Ownership is unambiguous. Risk is visible to decision-makers. Good judgment is enabled, not constrained.

Lens diagnostic: Ask 3 people on the same team who owns incident response at 2 AM on a Saturday. **If you get 3 different answers, you've found a clarity gap no amount of tooling will fix.**

Why frameworks miss this: Standard frameworks prescribe controls. The Lens identifies where controls create an illusion of security — and where clarity would reduce more actual risk than another layer of restriction.

THE METHODOLOGY

What Makes the Lens Different

Diagnostic, Not Prescriptive	Reveals how the system actually operates — doesn't just check boxes against an external standard
Human-Centered by Design	Built around how people actually behave under real conditions, not how policies assume they will
Sequential & Compound	Each question builds on the last — the compound picture reveals what no single question can
Systems Thinking, Not Checklists	Draws from organizational sociology, failure analysis, and complex systems — not just security engineering
Measures Resilience, Not Compliance	Asks 'where are you lucky rather than good?' instead of 'did you check this box?'

Built through 50+ real-world assessments. Refined through practice, not theory.

THE INTERSECTION

What Practitioners and Social Scientists Can Learn From Each Other

What Practitioners Bring

- Operational reality of failure modes
- Scale and urgency of organizational risk
- Case data that researchers can't access
- The 'what happens next' when theory meets practice

What Social Scientists Bring

- Frameworks for organizational behavior
- Rigor in studying human systems
- Theory explaining why the same failures recur
- Methods to study what we can't 'pen-test'

The real vulnerability isn't in the code. It's in the system — and that's a human problem.

CROWNSTONE

The Five Questions

01 What is this system optimizing for?

02 Where does it rely on perfect human behavior?

03 Which assumptions are no longer true?

04 How does failure emerge quietly over time?

05 Where does clarity reduce risk more than control?

Dr. Olutobi Oyinlade
Crownstone Strategy Group | The Cybersecurist
crownstone.io

Questions?