anunta

Who Owns Risk?

A Guide to Building Shared Accountability in Security

anunta

Mini Guide

Market Headwinds, Cross Functional Alignment, and a Conversation Guide

In today's hybrid and fast-moving environments, risk isn't isolated—and neither is responsibility. While IT teams are held accountable for uptime and security, many of the systems, behaviors, and decisions that influence risk live outside their control. This guide helps IT leaders surface shared accountability, align stakeholders, and drive visibility and resilience across the business.

What the Market Is Saying

As responsibilities for digital systems spread across departments, the lines of accountability are increasingly blurry. The market is responding with new expectations for shared responsibility and transparency.

Identity-first security and Zero Trust architecture becoming the new baseline

Gartner notes it's moving from a buzzword into foundational infrastructure practice (Gartner).

Real-time observability is now core to operational resilience

IDC emphasizes that real-time monitoring and AI-driven observability are critical for incident detection and prevention (Cisco).

Consistent policies across environments remain a major pain point

Numerous analysts highlight ongoing struggles to unify security controls across cloud and hybrid deployments (Cisco).

Executives expect measurable business outcomes from security

Observability is increasingly seen as a strategic capability—beyond uptime, towards informed business resilience (WOCU-Monitoring).

Who You Should Be Talking To (And Why)

Securing and observing infrastructure effectively requires collaboration across functionally diverse teams:

FUNCTION	WHY THEY MATTER
Security/Compliance Team	Defines acceptable risk levels, regulatory requirements, and enforcement policies
Infrastructure/Cloud Team	Manages placement of controls and ensures visibility across environments
App Owners/Product Teams	Understand critical dependencies—they know what needs to remain up & performant
Executives (CIO, CFO)	Need to see ROI and risk exposure in business terms, not just technical metrics

Conversation Guide

4 Questions to Break the Silos

1. Security team

"Which user or device access scenarios keep you up at night—and how are we currently mitigating them?"

2. Infrastructure/Cloud team

"Do we truly have full observability into our hybrid environment today? Where might we have blind spots?"

3. App/Product teams

"What would an unexpected outage or data breach cost your team in terms of work delay or user impact?"

4. Executive leadership

"Which operational or security risks are most threatening to our business goals? How should we quantify and address them?"

How to Use This Guide

Use this guide along with your checklist to surface high-impact gaps and foster a more resilient, unified infrastructure strategy—one that delivers both trust and visibility. Because risk isn't just an IT problem—it's an organizational one.

anunta

Get a second opinion on your current approach.

Because risk isn’t just an IT problem, it’s an organizational one.

Contact Us