eSureITy

CYBER INSURANCE READINESS SERVICES

Turn underwriting scrutiny into a strategy advantage

Cyber insurance is no longer a paperwork exercise

Underwriters now treat your environment like a live security audit, not a simple questionnaire. If you can't prove control maturity, continuous monitoring, and tested incident response, you don't just pay more. You risk exclusions, reduced limits, or outright denial of coverage after an incident.

Most organizations still assume:

- "Our broker will handle it."
- "Our MSP will jump in if something happens."
- "If we have a policy, we're covered."

That gap between assumptions and what carriers actually require is where claims die and executives get surprised.

eSureITy exists to close that gap.

We don't sell or place insurance.

We make your cyber program "insurance-ready" and defensible.

Protecting MSPs and IT providers from insurance whiplash

MSPs and IT providers sit in the blast radius of almost every cyber incident. Underwriters now structure policies so that unauthorized actions can become your problem.

eSureITy helps MSPs and IT providers:

- Clarify where their responsibility ends and the client's policy begins
- Document incident response protocols that require carrier authorization before action
- Avoid "good intention" responses that trigger subrogation or coverage disputes
- Align their own E&O and cyber liability policies with client expectations

Result: fewer post-incident surprises, less finger-pointing, and a clearer professional risk profile.

The problem most buyers don't see coming

1. Coverage that looks solid—until the first claim

Carriers are raising the bar for security maturity. Without documented controls, ongoing testing, and monitoring, claims can be delayed, limited, or denied altogether.

2. MSPs and IT providers with their hands tied

Many policies require carrier authorization before incident response. If your MSP acts without approval—no matter how good their intentions—coverage can be voided or you can face subrogation exposure.

3. Misaligned policies between you and your providers

When you and your MSP, cloud provider, or critical vendors carry cyber coverage from different insurers, liability disputes and finger-pointing are common. Everyone assumed someone else's policy would pick up the tab.

4. "Shared coverage" myths

Executives often think their MSP's insurance somehow covers them. It doesn't. Each party needs their own cyber liability policy. The only real protection is alignment of controls, roles, and response playbooks.

Contact Us

info@eSureITy.com

www.eSureITy.com

eSureITy Cyber Insurance Readiness Services

✓ Proactive risk and control assessment
Review pen tests, risk assessments, and findings through an underwriting lens, turning technical reports into clear evidence of proactive risk management.

✓ Monitoring and response readiness check
Validate that your SOC/MDR/EDR stack, logging, and escalation paths meet carrier expectations and can be described in precise, defensible language.

✓ Framework and control mapping
Map your tools, processes, and policies to NIST CSF, CIS, ISO 27001 and similar frameworks, closing gaps most likely to trigger underwriting concern.

✓ Human-layer and training validation
Evaluate phishing simulations, LMS content, cadence, and metrics so your awareness program counts as a measurable control—not a checkbox.

✓ IR and BC/DR insurance alignment
Tighten incident response and business continuity plans, tabletops, and runbooks so they reflect policy conditions, carrier notification requirements, and real-world decision paths during an event.

Engagement model

Phase 1 – Readiness Baseline

- Review existing policies, applications, renewals, and carrier questionnaires
- Inventory controls: MFA, EDR, SOC/MDR, vulnerability management, IR, BC/DR, training, frameworks

Phase 2 – Gap and Evidence Mapping

- Identify high-impact gaps from an underwriting and claims-handling standpoint
- Map controls and documentation to carrier expectations and preferred frameworks

Phase 3 – Control and Documentation Uplift

- Prioritize fixes that reduce both cyber risk and insurance friction
- Standardize control descriptions, runbooks, and metrics for re-use across carriers

Phase 4 – Renewal and Incident Support (Advisory)

- Prepare for renewals with updated artifacts and narratives
- Advise during incidents on coordination with carriers and adherence to policy conditions
- Continually refine your program as carrier expectations evolve

Who benefits

- CFOs and Risk Officers seeking predictable renewals and fewer exclusions
- CIOs and CISOs needing a control narrative that stands up to underwriting scrutiny
- MSPs and IT providers trying to avoid subrogation and misaligned expectations

Brokers who want better-prepared clients and cleaner submissions

eSureITy's role: your cyber–insurance translation layer

eSureITy is a cyber insurance readiness and risk advisory firm. We do not sell insurance or manage a SOC.

We help you:

- Translate underwriting requirements into concrete technical and procedural controls
- Validate that your existing controls match what carriers expect
- Align MSP, internal IT, security vendors, and brokers around one coordinated story
- Build evidence packs so your security posture is easy to underwrite and defend

You keep your existing security partners and brokers.

We make the entire ecosystem easier to insure and less likely to fight you at claim time.

What "insurance-ready" looks like

Carriers are increasingly converging on the same core security requirements:

- Multi-Factor Authentication (MFA) on all critical systems
- Endpoint Detection & Response (EDR)
- 24×7 threat monitoring via a SOC or MDR service
- Regular penetration testing and vulnerability assessments
- Documented Incident Response and Business Continuity plans
- Ongoing employee security awareness training
- Alignment with frameworks like NIST CSF, CIS Controls, or ISO 27001

eSureITy's Cyber Insurance Readiness Services are designed to build and prove strength in exactly these areas.

Why eSureITy

- Singular focus on cyber risk and insurance readiness
- Independence from carriers—no conflicts of interest, no policy sales
- Deep understanding of both security controls and underwriting language
- Ability to coordinate MSPs, internal teams, and brokers into one coherent risk story

Establish your Cyber Insurance Readiness Baseline with eSureITy

Use your next renewal, policy increase, or carrier change as a forcing function to upgrade your security program, your documentation, and your negotiating position—not just your premium.