GRYPHON
SECURITY

NIST-Based Security Audit

Clear Risk Insight. Defensible Decisions.

A focused cybersecurity assessment designed for organizations where operational continuity, regulatory exposure, and reputational trust are non-negotiable.

Organizations across all sectors face increasingly complex cyber risk. They manage high-value sensitive data, rely on interconnected systems and cloud services, and are frequent targets for ransomware, credential theft, and data extortion. This service provides leadership with a clear, defensible understanding of their true security posture using a NIST-aligned methodology tailored to how modern organizations actually operate.

What We Do

We conduct a structured cybersecurity audit evaluating the administrative, technical, and physical safeguards that protect sensitive and regulated information.

The assessment is aligned with NIST SP 800-53 control families and scaled appropriately for the organization's size and complexity. Rather than applying generic enterprise checklists, we evaluate how controls function in real workflows—how users authenticate, how data is accessed and shared, how remote access is secured, how incidents would be detected, and how reliance on cloud and third-party providers affects actual risk.

The result is a practical, evidence-based evaluation of the organization's current security posture—not a theoretical maturity score.

Why This Matters

Cybersecurity failures create consequences beyond downtime or technical inconvenience. Control gaps can expose sensitive data, disrupt critical operations, and trigger regulatory, contractual, and reputational fallout.

These incidents place leadership decisions under scrutiny after the fact. This audit identifies where material risk truly exists, distinguishes high-impact exposures from low-value findings, and equips leadership with a defensible foundation for security decisions before an incident forces those decisions under pressure.

Our Assessment Approach

This service uses a NIST-aligned but non-bureaucratic methodology.

We apply nationally recognized security principles while deliberately avoiding compliance theater. The assessment is not a certification, attestation, or government audit. Instead, it is a risk-focused evaluation designed to answer one core question:

"If something goes wrong, will leadership be able to demonstrate that security decisions were informed, reasonable, and defensible?"

Findings are contextualized to the organization's size, staffing model, technology stack, and threat exposure so recommendations are achievable, prioritized, and relevant.

What's Evaluated

The audit focuses on control areas most relevant to modern organizational operations, including:

- **Access & Authentication**
  Identity management, multi-factor authentication, privileged access, and user lifecycle controls
- **Monitoring & Logging**
  Audit logging, alerting capability, and visibility into suspicious or unauthorized activity
- **Backup & Recovery**
  Backup scope, immutability, recovery testing, and ransomware resilience
- **Incident Readiness**
  Detection capability, response procedures, internal roles, and external coordination readiness
- **Data Protection**
  Encryption, data handling practices, and protection of privileged and sensitive information
- **Governance & Training**
  Policies, risk management practices, security awareness, and leadership oversight

Each area is evaluated against NIST expectations and translated into clear, operational risk language.

What You Receive

- Executive-level findings in plain English suitable for partners or boards
- Risk-rated gaps (High / Medium / Low) tied to realistic threat scenarios
- Evidence-based recommendations grounded in observed conditions
- A prioritized remediation roadmap supporting budgeting and accountability

Who This Service Is For

This service is designed for:

- Small-to-mid sized organizations
- Organizations handling sensitive, regulated, or high-value information
- Environments seeking an objective, defensible view of security posture

It is particularly valuable for organizations preparing for insurance renewal, responding to third-party security inquiries, formalizing governance, or seeking clarity before investing in new security tools.

This Service Is *Not* Designed For

- Organizations seeking a checkbox compliance audit
- Organizations looking for managed SOC services or tool resale
- Environments without leadership buy-in for remediation and risk ownership

Gryphon Security focuses on clarity, independence, and defensible outcomes.

Why Gryphon Security

- **Clear & Defensible:** Findings leadership can understand and stand behind
- **NIST-Based**: Grounded in nationally recognized standards
- **Independent & Vendor-Neutral**: No resale pressure, no product bias

Next Steps

An initial conversation is structured, confidential, and obligation-free.

We will:

- Confirm scope and environment
- Discuss key risk concerns
- Explain exactly what the assessment will and will not cover

We will not pressure you into tools, managed services, or long-term contracts.

Gryphon Security, LLC
Risk-Based Cybersecurity Assessments
info@gryphonsec.com | www.gryphonsec.com