2026 CYBER INSURANCE TECHNICAL AUDIT

5 Compliance Markers Your Carrier is Checking For Agencies with 5–19 Employees



INTRODUCTION

Cyber insurance carriers are increasing their requirements for small agencies. Missing these markers could put your E&O policy or coverage at risk. Use this checklist to verify that your agency is compliant.

THE 5 COMPLIANCE MARKERS

1. MFA (Multi-Factor Authentication)
   Must be enabled on all email, remote access, and administrative accounts.
2. Immutable Backups
   Backups must be air-gapped or protected from ransomware and accidental deletion.
3. EDR/MDR (Endpoint Detection & Response / Managed Detection & Response)
   Advanced endpoint protection beyond basic antivirus.
4. Security Awareness Training
   Staff must be trained regularly on phishing, social engineering, and cyber hygiene.
5. Vulnerability Scanning
   Regular internal network scans to ensure all systems are patched.

NEXT STEPS / CALL TO ACTION

If you’re unsure whether your agency has implemented any of these 5 markers, or if you need help verifying your cyber insurance compliance, please call or email us using the contact information below. We can walk you through the audit and ensure your agency is protected.

Thank you for taking proactive steps to protect your agency!

Paul Drewek / JIT Systems, LLC / 317-689-9251 / info@jitsystems.biz