Fast-Track Compliance Readiness Checklist

NET-TECH CONSULTING
Real People, Real Protection, Right Now

Use this checklist to evaluate your organization's readiness for a rapid compliance remediation engagement. Each item represents a critical element auditors, insurers, and clients frequently request as part of due diligence, breach response, or contract renewal processes. Addressing these areas quickly can dramatically reduce exposure and increase your operational credibility.

✓ **Do you have a documented Written Information Security Policy (WISP)?**

A WISP outlines your organization's overarching security objectives, procedures, and responsibilities. It serves as the foundational document that maps back to frameworks like NIST or HIPAA.

✓ **Have you formally segmented your vendors by access level and criticality?**

Vendor segmentation ensures that third parties are categorized by risk level, enabling tailored controls and more effective risk mitigation. It's a requirement in many regulatory frameworks and procurement policies.

✓ **Can you produce access logs and evidence of MFA enforcement?**

Auditors and incident responders will request access logs and MFA configuration evidence to verify your enforcement of identity controls. Having these easily accessible demonstrates maturity and readiness.

✓ **Do you have a current Incident Response Plan (IRP) and tabletop test documentation?**

A documented and tested IRP proves your team is prepared to handle breaches. Tabletop exercises validate that your plan is understood and executable under pressure.

✓ **Is your data classification policy up to date and mapped to systems?**

Data classification policies define how sensitive information is labeled, protected, and monitored. Mapping this policy to your actual systems helps ensure the right controls are applied consistently.

✓ **Are policy sign-offs, training logs, and audit evidence collected and versioned?**

Signed acknowledgments and audit trails are essential for demonstrating control enforcement and meeting internal and external compliance requirements.

✓ **Can you show closure documentation to clients or insurers within 24–48 hours?**

Closure documentation includes consolidated evidence packages showing how issues were resolved—critical for passing audits, renewing cyber insurance, or maintaining client trust.

If you answered 'No' or 'Not sure' to any of the above, our 60-day Fast-Track Compliance Remediation Package is built for you. We provide the tools, templates, and hands-on remediation to help you close these gaps fast—with minimal disruption and fixed-fee predictability.