Periodic Cybersecurity AUDIT CHECKLIST

Version 1.0

rule4

INTRODUCTION

Checklists aren't everything.

At Rule4, we have an anti-checklist mentality. We've seen enough environments and solved enough problems to know that every IT program should be customized and constantly evolving, and that checklists sometimes get in the way of that.

It's not enough to have a basic list and go through the same motions quarter after quarter, year after year — to be effective tools, audit checklists should be evolving documents, and audits should include critical analysis beyond checking the box.

We've provided this audit program checklist as a resource and jumping off point. Think of it as the foundation of the house; you'll need to add the walls, the roof, and all the finishing touches.

ADDITIONAL RESOURCES

There are a lot of regulatory standards and compliance frameworks out there today. Even if your organization isn't required to comply with any of them, they can provide an excellent resource and basis by which to measure and build your cybersecurity program.

We recommend the **National Institute of Standards and Technology's Cybersecurity Framework**, version 1.1, as a valuable and comprehensive template against which to gauge cybersecurity effectivenes.

PERIODIC CYBERSECURITY AUDIT Checklist

Paths of Attack

	Activity	*Minimum Frequency*
☐	Perform external vulnerability scan	Quarterly
☐	Perform external application penetration test	Annually
☐	Review DMZ service/servers	Annually

Software Patch-Level & Use Compliance

	Activity	*Minimum Frequency*
☐	Perform Software inventory and patch comparison	Quarterly

Network Security Architecture

	Activity	*Minimum Frequency*
☐	Review firewall configuration (including ALL rules)	Annually
☐	Evaluate internal network partitioning	Annually

User Administrative Policy & Compliance

	Activity	*Minimum Frequency*
☐	Perform a social engineering study	Annually

Encryption Usage & Key Handling

	Activity	*Minimum Frequency*
☐	Review encryption policy compliance	Annually

Trust-Level Dependencies & Management

	Activity	*Minimum Frequency*
☐	Review vendor and trusted partner access	Annually

Antivirus/Anti-Malware

	Activity	*Minimum Frequency*
☐	Confirm server and workstation virus signature updates	Quarterly

Role/Function Segmentation & Access Management

	Activity	*Minimum Frequency*
☐	Review termination list vs. access removed, new hires vs. access granted	Annually
☐	Review elevated privilege accounts	Quarterly

Remote Access

	Activity	*Minimum Frequency*
☐	Validate remote access is only via approved methods	Annually

Organizational & Security Measures

	Activity	*Minimum Frequency*
☐	Validate change and configuration maangement process compliance	Annually
☐	Inventory eDiscovery support tools	Annually
☐	Review IT security policy	Annually
☐	Review integration of IT security criteria with organization's purchasing process	Annually

Physical Network & System Infrastructure

	Activity	*Minimum Frequency*
☐	Review media and retired equipment disposal practices	Annually

Levels & Methods of Ongoing Vigilance

	Activity	*Minimum Frequency*
☐	Conduct incident response drill	Annually
☐	Review intrusion detection/prevention system effectiveness (event detection/reporting)	Quarterly

Regulatory Compliance

	Activity	*Minimum Frequency*
☐	Conduct formal review of organization's compliance with applicable regulatory standards (e.g., HIPAA, PCI DSS, ISO/IEC 27001)	Annually*

** Some standards, such as PCI DSS, may require more frequent review.*

3002 Bluff Street, Suite 100
Boulder, CO 80301
www.rule4.com | 888-4THEFOX