SHAZAM®

Expertise that **gives you an edge.**

SHAZAMSecure

SHAZAMSecure® offers information security analysis and risk mitigation services. We specialize in risk, regulatory, ACH and IT exams; cybersecurity and technical security; and social engineering.

Strengthening Financial Institutions

Expertise

Tap into years of industry and real-world expertise and bring this knowledge to your institution. Our own internal auditors, risk consultants and network security analysts — the very best in the business — will keep your institution safe.

Value

Keeping up with the complex and ever-changing world of information technology (IT) security, risk and compliance strains your staff. Let SHAZAM provide these unique skill sets to your institution at a reasonable price.

Guidance

Advice and support are available before, during and after your assessments, exams and courses. Easy-to-follow reports help you develop a plan to correct deficiencies and implement recommendations.

Risk, Regulatory and **IT Exams**

As new technologies and compliance demands increase, so does the need to better understand your risk exposure and ensure conformity with regulatory guidelines.

ACH Exam

As one of only 10 ACH payment associations, SHAZAM is uniquely qualified to review your ACH operations, policies and procedures. Our accredited ACH professional (AAP) will evaluate your ACH processes and ensure compliance with Nacha® Rules and other electronic payment regulations.

BSA Exam

Money laundering costs financial institutions billions of dollars every year. Failure to maintain BSA/AML compliance may result in civil and criminal penalties as well as reputational risk. Our risk-based approach follows the Federal Financial Institutions Examination Council's (FFIEC) BSA/AML manual and reviews your OFAC program, customer identification program, due diligence of deposit accounts, independent transactional testing and other key areas.

IT Exam

A full evaluation of your information security and IT policies, procedures and controls will determine the adequacy of your security and risk management efforts. Our IT exam identifies areas where you're most at risk and provides a detailed review of your environment to confirm compliance with FFIEC guidelines. Recommended actions are provided as a roadmap to ensure your institution has a well-secured and compliant IT environment.

Cybersecurity and **Technical Security**

Cyberattacks and technical attacks are evolving at the speed of light. It's important to understand where weaknesses within your network may exist to help protect your reputational risk and the likelihood of being hacked.

External Vulnerability Assessment

Using leading-edge software scanning tools and manual techniques, our external security assessment looks for areas that may be exposed to malicious attack through your firewall.

Internal Vulnerability Assessment

Our internal vulnerability assessment performs a thorough scan of all your internal IP addresses to help you better understand weaknesses that may exist on your network. Findings are prioritized by risk level, so you can focus on correcting the most important items first.

Wireless Vulnerability Assessment

Gain a better understanding of the potential vulnerabilities on your WI-FI network. Our assessment looks at your WLAN configurations, operational security controls and operational policies and procedures to determine what risks may exist. We also include a heat map to show you a visual of your current WI-FI signal coverage and strength.

VPN Vulnerability Assessment

Risks and vulnerabilities can be found anywhere, including your virtual private network (VPN). We will assess all critical components of your VPN which involves four main areas: authentication, technology, privacy and security. Findings and recommendations will be provided to help strengthen the security of your VPN.

Web Application Assessment

Your website can be a portal for hackers to launch an attack on your network. Our web application assessment reviews critical security issues within web applications and conducts tests to identify threats and evaluate the overall risk of your website.

Penetration Testing

A penetration test exploits the vulnerabilities found in the internal and external security assessments through proof-of-concept attacks. These tests help you better understand the extent to which an attacker can exploit vulnerabilities through destruction of systems, denial of service, theft of data and other malicious actions.

Additional **Services**

Managed Firewall

Your firewall is the first line of defense against external threats. Managing this critical security element is a full-time commitment. Let our professional staff provide 24/7 intrusion detection/prevention monitoring and response service. Customized monthly reports demonstrate the quality and value of this service to your executive management and board of directors.

Safe Act Examination

The examination will address the Secure and Fair Enforcement Licensing Act of 2008. We will focus on verifying your compliance with nationwide licensing and registration for mortgage loan originators. Findings and recommendations will be discussed with staff at the conclusion of the engagement.

IT, Risk and Compliance Consulting

As a leader in the field of IT, risk and compliance, our SHAZAM Secure team can serve in a consultative role and equip your organization with the latest emerging technologies and risk mitigation practices. These include information security, risk assessments, business continuity planning, vendor management, TR-39 exams, consumer compliance and operations.

Microsoft 365 Assessment

A Microsoft 365 Assessment is designed to assist organizations in establishing the foundation level of security for anyone adopting Microsoft 365. Our assessment uses the Center for Internet Security's (CIS) Microsoft 365 Foundations Benchmark to determine the adequacy of your current security settings as well as to ensure recommended controls are in place for specific sections found in the benchmark.

Social **Engineering**

Social engineering is the fastest, easiest and most common method hackers use to gain access to networks all across the world. SHAZAM provides two ways to test your employees' awareness and understanding of these fraudulent electronic and physical attempts so you can create a stronger defense to protect your institution, staff and accountholders' information from being compromised.

Social Engineering Assessment

As your employees gather online information and unintentionally download viruses and malware, your entire network could be compromised with the click of a button. We test your employees' responses to a simulated attack and provide feedback on leading practices to better secure your organization against social engineering threats.

Phishing

Phishing is the act of intentionally creating a fake email with the hope of deceiving a recipient to perform an action that could compromise your network, such as clicking on a link, downloading a file, or entering sensitive information. Our services can assess the likelihood of your staff falling for one of these attacks, which can then be used as a learning experience to help prevent future attacks from being successful.

Vishing

Much like phishing, vishing looks to accomplish the same goal, only this method is done by phone. Hackers look for their targets to divulge sensitive information, such as passwords and usernames, which can then be used to gain access to your network or other areas where sensitive information may be held. Our team of professionals will test your employees to determine how likely they are to fall prey to a real-life vishing attack and provide valuable feedback on the results of our test.

The innovation and service you need for the **edge you want**.

SHAZAM®

800-537-5427 | SHAZAM.net