REGULATORY COMPLIANCE

REGULATORY COMPLIANCE
SERVICES

CSI

Dynamic Solutions. Superior Results.

PERSONALIZED HELP THAT RELIEVES THE BURDEN OF MANAGING COMPLIANCE

The burden of managing risk and compliance is hefty, and it continues to grow and evolve. Estimates indicate that compliance with the Dodd-Frank Act (DFA) alone consumes 24 million banker hours per year. CSI Regulatory Compliance understands today's challenging regulatory landscape and delivers personalized services to help your financial institution manage compliance with a wide variety of regulations, without the need to take on the expense of additional full-time compliance staff.

CSI REGULATORY COMPLIANCE SERVICES PROVIDE
COMPREHENSIVE ASSESSMENTS, TESTING & SUPPORT
FOR ALL YOUR REGULATORY COMPLIANCE NEEDS.

CSI Regulatory Compliance offers the following services for your financial institution:

- Offensive Security Services
- Risk Management & Compliance Services
- Compliance Training
- ComplianceNet

OFFENSIVE SECURITY SERVICES

CSI's Offensive Security Services provide a proactive and adversarial approach to protecting your organization against areas of opportunity for cybercriminals and social engineers.

External Penetration Testing

CSI provides superior external penetration testing that's performed by our GIAC- and CISSP-certified consultants who adopt a real-world attacker's methodology of reconnaissance, scanning and exploitation.

Internal Penetration Testing

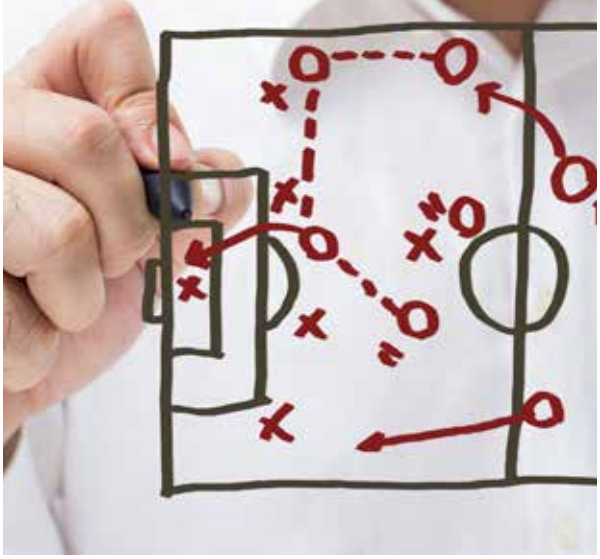
Information security program guidelines instruct financial institutions to conduct annual internal network and application-layer penetration testing to ensure the security of customer information and assets. CSI helps identify vulnerabilities without interruption to services through hands-on manual testing and research.

Wireless Network Audit

As an additional option for Internal Penetration Testing, the Wireless Network Audit analyzes limited encryption and authentication methods in use on your wireless networks.

Social Engineering Testing

Social engineering is one of the most sinister methods attackers use to gain access to customer information, because it manipulates those closest to the target—your employees. Using multiple methods, including email, telephone and personal discussion, our information security team conducts undercover interactive tests with employees to determine the amount of information a potential intruder could gain to penetrate systems.



iScan Vulnerability Assessment

Configured per GLBA guidelines, CSI's iScan tool provides the latest information security scanning techniques and is shipped to your organization. After you follow a few simple instructions to plug iScan into your network, the assessment is performed, and you return iScan using CSI prepaid shipping. CSI's certified consultants, who are trained in GLBA compliance, analyze the data and prepare a detailed report with recommendations for securing your network.

Password Audit

One weak, predictable or repeatedly used password is all cybercriminals need to gain access to your network. Using a sophisticated password-decrypting process, CSI identifies password vulnerabilities by auditing the stored versions of your organization's encrypted passwords to uncover patterns and other weaknesses. Then, CSI provides a comprehensive report so you can train end-users toward greater security.

Web Application Testing

Web applications are crucial to business efficiency, but if not managed adequately, they could cause a costly security breach. CSI's Web Application Testing service analyzes the security of any Web application (in-house, third-party proprietary or off-the-shelf) to detect vulnerabilities, including those identified by the Open Web Application Security Project (OWASP). Then, CSI provides detailed reports complete with mitigation tactics.

RISK MANAGEMENT AND COMPLIANCE SERVICES

CSI's regulatory compliance experts work with your organization to significantly lower your risk, prepare your institution to meet regulatory mandates and pass your next exam with flying colors.

Information Security Review

CSI combines technical and regulatory expertise to provide you with the most comprehensive GLBA compliance review and report in the industry. CSI's security experts conduct a full on-site information security assessment and provide an extensive evaluation of your information security systems and procedures, as well as a comprehensive network vulnerability scan and a risk-based summary of observations with recommendations designed to help you comply.

Red Flags Review Service

Since the addition of the Red Flags Rule to the Fair and Accurate Credit Transactions Act (FACTA) of 2003, financial institutions have been required to implement identity theft prevention programs. CSI performs a review of your program and provides a customized report with feedback of our findings, including actionable recommendations for strengthening your program.

IT Audit

CSI's IT Audit provides you with a qualitative, comprehensive review and analysis of all the major information technology areas recommended by the FFIEC's IT Examination Handbook, in order to ensure you have a thorough picture of your entire network. CSI identifies the current and foreseeable risks threatening your systems and the consumer data housed on them, and provides recommendations for mitigating those risks.

IT Risk Assessment

CSI assesses your institution to determine an IT risk baseline, including risks to the confidentiality, integrity and availability of your systems. Our experts then help you develop a solid framework and process for your institution to perform ongoing IT risk assessments.

Cybersecurity Risk Assessment

CSI's Cybersecurity Risk Assessment helps organizations gauge the level of risk associated with their cyber presence, identify and evaluate existing cybersecurity controls and determine the need for additional security measures. The risk assessment will assist with meeting the expectations of the guidance issued by the FFIEC.

BSA/AML Audit

CSI's BSA/AML Audit is a comprehensive evaluation, focused on risk-based testing as well as the review of related documents, that provides reasonable assurance of compliance with government mandates. An objective report of any violations, findings or areas of weakness and corrective action will be provided to assist you with strengthening and enhancing your overall BSA compliance program.

Risk Management Services

CSI SmartRisk IQ, our industry-leading ERM software solution, includes on-site help from our risk and compliance experts. Our ERM team assists in your initial risk assessments, and develops customized Key Risk Indicators (KRIs) for your institution. You also gain ongoing support from our ERM team through quarterly check-ins that answer your risk management questions.

High-Risk Vendor Evaluation

CSI provides a thorough review of control documentation provided by your high-risk vendors. This review offers a sharper picture of the controls in place and the level of risk associated with them.

Red Flags Identity Theft Risk Assessment

This assessment evaluates your daily operations to expose identity theft risks to covered account holders, and is the cornerstone of an effective identity theft prevention program. Following the guidelines set forth under FACTA, CSI assesses the methods utilized to open and access covered accounts in conjunction with the 26 red flags identified by financial regulators. Then we provide a detailed report that effectively portrays the identity theft risk level of each covered account type.

COMPLIANCE TRAINING

Developed by information security professionals, the following seminars are designed to strengthen your institution's information security program or fulfill your BSA/AML training requirement.

- **CSI's Information Security Training** provides your employees with a better awareness of the current dangers faced by your institution, giving them a richer understanding of the critical role they play in protecting it.
- **CSI's Social Engineering Training** gives your employees the ability to recognize and thwart social engineering tactics before they endanger your institution.
- **CSI's Bank Secrecy Act Training** focuses your employees' attention on identifying and preventing money laundering risks. It also covers policies and procedures for CIP/SAR, including required reporting and record-keeping training, to support your institution's specific BSA/AML compliance priorities and issues.
- **CSI's Cybersecurity Awareness Training** is designed specifically to educate bank board members and ensure they have access to accurate, timely and relevant industry information in the areas of cybersecurity and IT governance. Whether you prefer virtual or in-person training, our experts will conduct an interactive exercise to educate your board on the FFIEC's five general awareness topics related to cybersecurity preparedness. The training is tailored to your board and financial institution, and provides a hands-on opportunity for facilitating cybersecurity-related discussion and questions.

COMPLIANCENET

With ComplianceNet, CSI Regulatory Compliance puts its entire panel of regulatory experts at your disposal. Whether specific to your institution or regarding the industry in general, this subscription service allows your overburdened staff to email CSI with their compliance questions related to:

- BSA/OFAC
- Deposits & Operations
- Dodd-Frank Requirements
- Information Security
- Loans

Save your institution time and money by capitalizing on our experts' extensive
knowledge and research capabilities. It's
simple. You ask the questions. We provide the solution. ComplianceNet delivers high-quality answers with exceptional service:

- Experts with more than 100 years of combined regulatory experience are on call Monday through Friday during regular business hours to receive your emailed questions and respond with actionable feedback within three business days or less
- Email up to 48 submissions per year (some restrictions apply), including requests for compliance reviews of drafted advertisements and standard-length policy documents