COMPLIANCE

HIPAA | PCI DSS | PENETRATION TESTING | REMEDIATION VERIFICATION

Regulatory Compliance Services

HALOCK continues to lead the information security community in understanding the role of risk management in regulatory compliance and security. Regulations, such as the HIPAA Security Rule, Gramm-Leach-Bliley Safeguards Rule, Massachusetts 201 CMR 17.00, 23 NYCRR Part 500 (NYDFS), and many other regulations require reasonable security safeguards to achieve compliance.

HALOCK prepares our clients for risk management by developing their unique criteria for assessing risk and accepting risk. HALOCK then conducts a risk assessment for the client by considering how effective foreseeable threats would be in their environment, and estimating the likelihood and impacts of those threats. When risks evaluate as too high, HALOCK then recommends safeguards that evaluate as “reasonable” in the client environment, given their mission, their objectives, and their obligations.

HALOCK®

Compliance Services

HIPAA Security Rule

The HIPAA Security Rule provides a set of "specifications" that should be met in order to demonstrate compliance with the regulation. Risk assessments help establish reasonableness for addressable specifications, and identify risks to PHI that are associated with the specifications and foreseeable threats.

State Regulations

State regulations such as 23 NYCRR Part 500 (New York DFS) and 21 CMR 17.00 (Massachusetts) are also based on risk, requiring that risk analysis help determine when risks and safeguards reasonably protect personal and financial information.

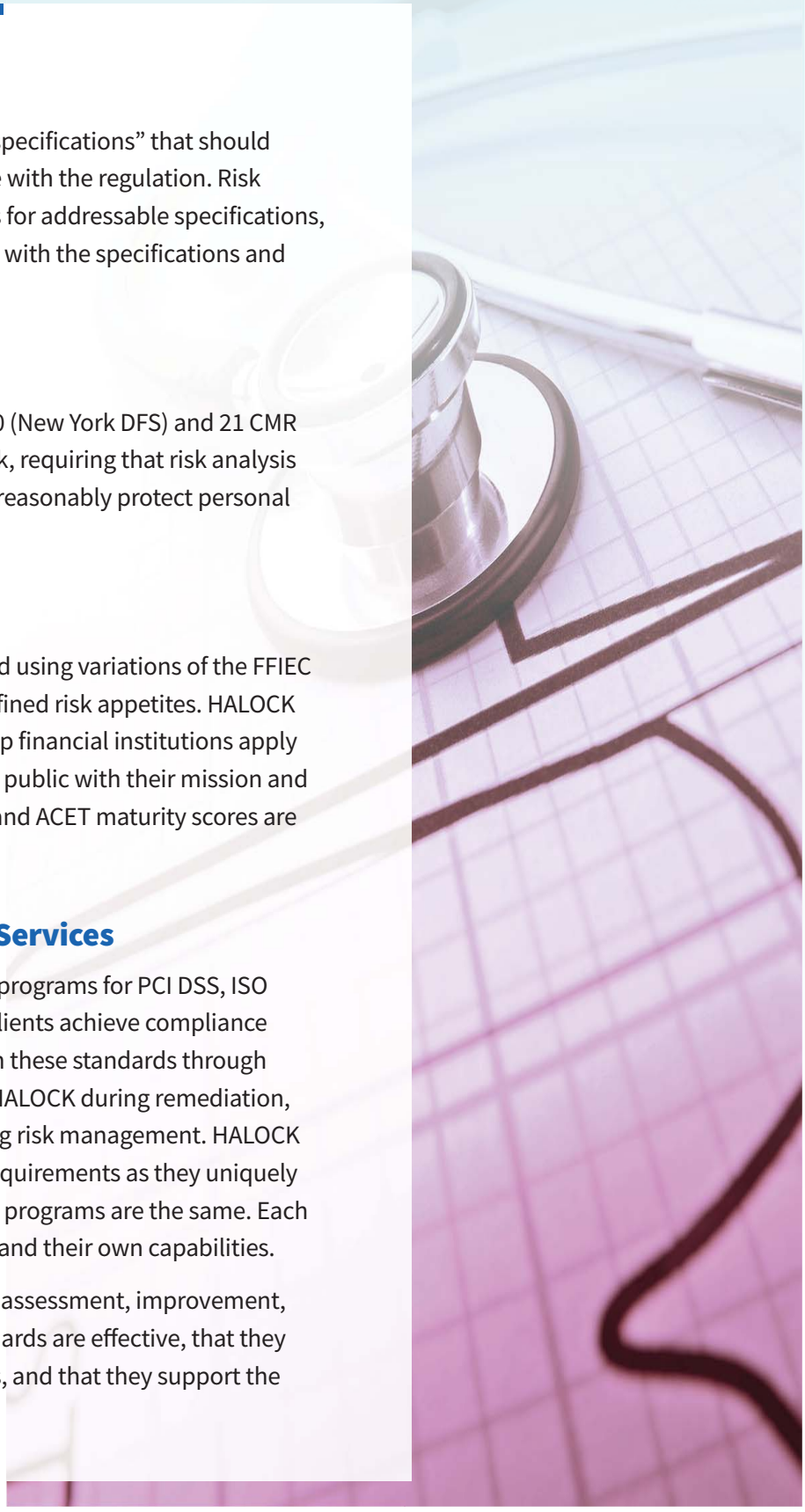
Financial Regulations

Retail banks and credit unions are examined using variations of the FFIEC CAT which require risk assessments and defined risk appetites. HALOCK is able to conduct risk assessments that help financial institutions apply safeguards that balance the interests of the public with their mission and objectives, and to determine whether CAT and ACET maturity scores are acceptable.

Security Standard Compliance Services

HALOCK helps our clients manage security programs for PCI DSS, ISO 27001, and the NIST Risk Framework. Our clients achieve compliance – and certification where appropriate – with these standards through initial security assessments, working with HALOCK during remediation, validating compliance, and through ongoing risk management. HALOCK helps our clients understand compliance requirements as they uniquely apply to them. No two information security programs are the same. Each organization operates with their own risks, and their own capabilities.

HALOCK guides each of our clients through assessment, improvement, and validation to ensure that security standards are effective, that they meet requirements set by standards bodies, and that they support the environments that they protect.



PCI DSS

HALOCK assesses cardholder data environments to understand both how well the organization addresses the PCI DSS requirements, and to recommend the clients best strategy toward compliance. Some organizations can greatly reduce their PCI DSS compliance obligations through segmentation of networks and processes, or by completely isolating card transactions from the organization. Our initial priority is to be sure that clients are not doing more than what is necessary to achieve and maintain both compliance and security.

HALOCK's Qualified Security Advisors (QSAs) conduct consultative compliance assessments to be sure that we understand the nature of each client's business, and to identify practical methods for resolving sometimes complex security and compliance challenges.

HALOCK's PCI DSS validations help clients gather the required documentation and evidence they need to demonstrate compliance, and will both evaluate and analyze this evidence to produce a Report on Compliance (ROC). HALOCK also offers integration with our penetration testers and risk assessors to verify network segmentation, and to uncover other security concerns that should be addressed to maintain compliance.

ISO 27001

ISO 27001 is commonly misunderstood as a security controls standard. ISO 27002 is a set of controls and best practices. However, ISO 27001 certification verifies that an organization operates an Information Security Management System (ISMS); a risk-based management program that measurably reduces risk to meet specific objectives.

HALOCK helps our clients identify parts of their organization and technical environment that can best align information security programs with measurable outcomes, and begins the planning phase with a comprehensive risk assessment. The risk assessment will shape a security plan for achieving business goals using reasonable security goals. HALOCK then helps design and implement security processes, management oversight methods, and security controls that provide evidence of continuous improvement; a key objective for ISO 27001 certification.

CIS Controls, NIST SP 800-53, Cyber Security Framework and Others

Some organizations have a need to demonstrate compliance with security frameworks that are not supported with a certification program. CIS Controls, NIST SP 800-53, the NIST Cybersecurity Framework, and others provide a controls framework, a risk analysis framework, and specific standards for configuring systems in known-secure ways. But similar to compliance and other standards-based frameworks, these can only be successfully maintained over time with a supportive, risk-based management program.

As with our other compliance offerings, HALOCK helps our clients establish the foundations for these other frameworks by defining their unique risk assessment and acceptance criteria, conducting a risk assessment for a strategically important scope of business, and developing a security plan based on the assessment's results.

Why HALOCK?

HALOCK continues to lead the information security community by evolving and improving risk-based management methods, either toward certification or for compliance and continual improvement. Contact us to see how our strategic approach to information security management can help you demonstrate compliance to these frameworks and others.

As principal authors of **CIS Risk Assessment Method (RAM)** and board members of The **Duty of Care Risk Analysis (DoCRA)** Council, HALOCK offers the unique insight to help organizations define their acceptable level of risk and establish "duty of care" for cybersecurity. Through this risk assessment method, businesses can evaluate cyber risk that is clear to legal authorities, regulators, executives, lay people, and security practitioners.

HALOCK's service philosophy, **Purpose Driven Security®**, can best be summarized as reasonable and appropriate risk management:

Security controls implemented should encompass the necessary **balance of compliance and business goals.** Not all security controls should be implemented, and those that are should be implemented only to a certain degree depending on the calculated risk being treated.

Organizations have an obligation to **perform proactive due care to reduce liability for shareholders, clients, partners, employees and the greater good** as appropriate. Thus, businesses need to take into consideration on cyber threats that are foreseeable, which HALOCK can help identify.

This comprehensive approach enables organizations effectively support a security budget and maximize protection of critical information assets.

HALOCK®

HALOCK Security Labs
1834 Walden Office Square, Suite 200
Schaumburg, IL 60173
847-221-0200

Incident Response Hotline: 800-925-0559

halock.com

About HALOCK

Founded in 1996, HALOCK Security Labs is a thought-leading information security firm, that combines strengths in strategic management consulting with deep technical expertise. HALOCK's service philosophy is to apply just the right amount of security to protect critical assets, satisfy compliance requirements and achieve corporate goals. HALOCK's services include: Security and Risk Management, Compliance Validation, Penetration Testing, Incident Response Readiness, Security Organization Development, and Security Engineering.