All Covered

IT SERVICES FROM KONICA MINOLTA / **FINANCE**

Information Security Officer Advisory Service

Information Security, Risk Management and Compliance

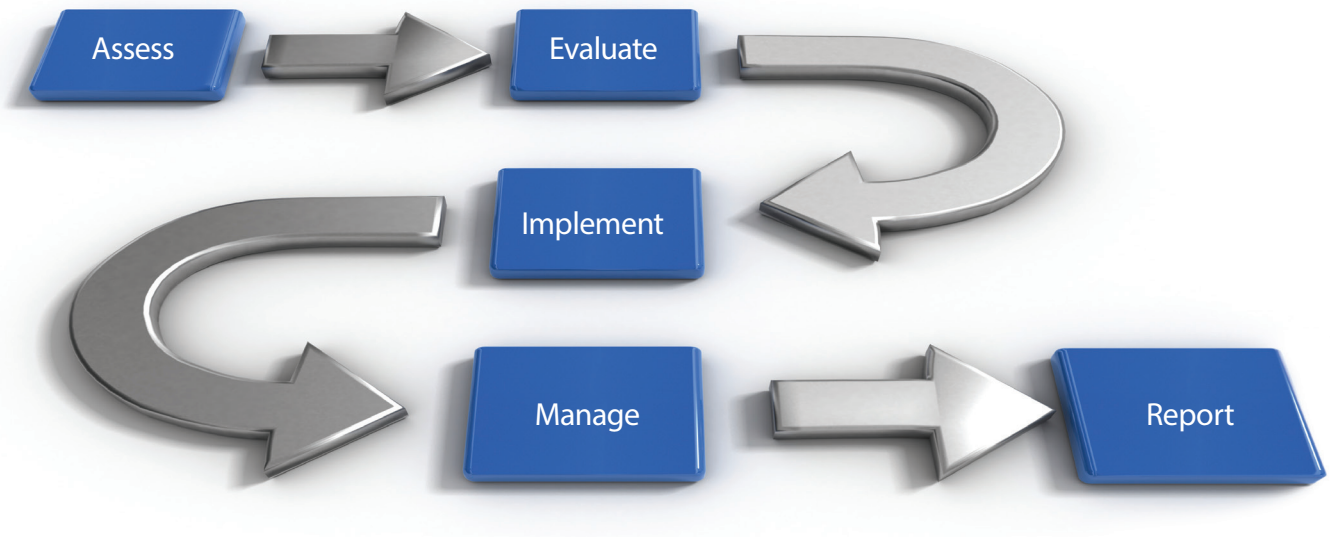
With issues as complex as regulatory compliance, oversight and cybersecurity, financial institutions cannot afford to take half measures. IT security issues represent a continuous threat to the integrity of an institution's data, while the amount of information examiners demand regarding policies, procedures and safeguards continues to grow. Recent regulatory guidance is requiring Financial Institutions to address the role of an Information Security Officer (ISO). A well-structured approach will allow your bank to implement an ISO without overburdening existing staff. All Covered's ISO Advisory Service enables your Institution to stay ahead of cyber threats and meet regulations.

Certified IT Security and Compliance Professionals

Our ISO Advisory Service allows your organization to utilize our pool of certified experts to perform most tasks typically assigned to your ISO. Working both on-site and remotely, our experts will help your Institution achieve its goals with greater levels of efficiency. All Covered provides independent and unbiased advice to address all applicable information security requirements driven by regulatory and compliance objectives, senior management direction and accepted information security best practices.

All Covered's ISO Advisory Services are:

- Provided by First Class Certified IT Security and Compliance Professionals
- Delivered Using Security & Governance Best Practices
- Audit Tested
- Regulatory Compliant



Information Security Officer Advisory Service

Features	Benefits
Initial IT Security Assessment	Perform onsite Compliance & Information Security Assessment, General IT & Security Assessment, and Gap Analysis. Presentation of findings.
IT Security Assessment Remediation Planning	Review security features of new systems to ensure that they meet the security requirements of existing policies.
IT Security Remediation Recommendations	Recommend appropriate changes to policies and standards based on evolution of risk.
IT Security Program	Establish a risk-based IT Security Program that is customized to the environment, revised annually to incorporate changes in the threat landscape (cyber attack, incident response strategies, etc.) and regulatory demands. Includes policies and customizable procedure guidance that meets FFIEC requirements.
Annual GLBA IT Risk Assessment	Identify and assess GLBA assets for potential vulnerabilities and risk impacts. Engage all necessary functional areas, design, train and assist with the creation of a best practice assessment of risk as outlined by the FFIEC. Align with ERM strategies.
Business Continuity Assessment and Planning	Perform a customized Business Impact Analysis to determine critical business functional areas and dependencies. Create specific Business Continuity Plans including Pandemic Planning. Evaluate always-on strategies including migration to cloud based offerings that are easy to update and always available.
IT Audit Support	Engage with Banking clients to prepare for audit and exams - from survey completion to full service audit reporting. Provide IT Audit support for both internal and external IT Audits and Regulatory Exams. Collaborate with Banking and Financial clients to interpret reports from core and critical vendor services. Information prepared and organized specifically in support of a Financial Industry Audit.
Vulnerability Assessment and Remediation	Implement ongoing vulnerability assessments, remediation and reporting to reduce risk and address IT compliance.
3rd Party PenTest & Social Engineering Management	Procure, coordinate and assess 3rd Party PenTest & Social Engineering. Provide remediation management and documentation.
Log Management and Security Incident Event Management	24x7 real time network security supporting system logging, security incident response and compliance requirements. Suspicious activity is detected and corrective action is taken to mitigate the activity.
IT Security Training	Work with your IT team and the bank to ensure adequate technical and procedural security is designed around new systems. Ensuring information security and GLBA related training is provided to bank employees as needed. Relevant and timely, the IT Security training addresses concepts geared to Executive Management and employee understanding (phishing, social engineering) as well administrator level discussions and incorporates concepts of cyber-attack and incident response.
IT Steering Committee Meeting Attendance	Active participation in the planning of IT initiatives. Ensure resources and capital are best utilized to meet the strategic goals of the organization.
Compliance/Risk Management Committee Participation	Investigate and reporting information security issues to the Compliance and Risk Management Committee or other levels of management as appropriate.
Board Training & Reporting	Assist in preparing reports to the Board of Directors on the effectiveness of Bank's Information Security.
Board Meeting Participation	Twice annual Board Meeting participation delivering reports and providing training.

KONICA MINOLTA

All Covered