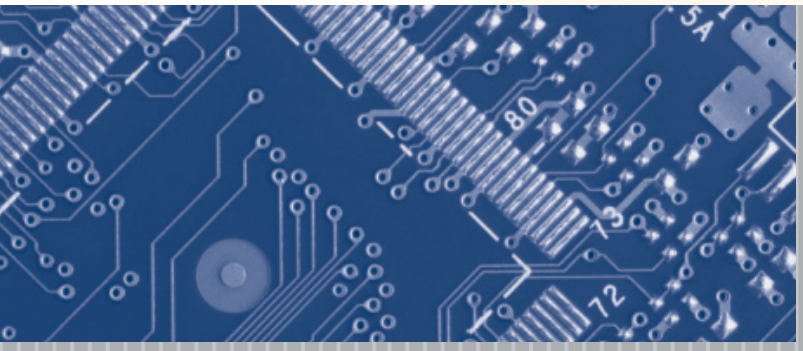
RLR
MANAGEMENT CONSULTING, INC.

www.rlrmgmt.com
1-888-757-7330



Information Technology & Compliance

IT Audits

RLR has completed over 100 IT audits for our clients. Our Certified Information Systems Auditor (CISA) takes a positive approach with our clients through reviews of existing Information Technology (IT) operations, policies, procedures and controls. IT Audits are conducted in strict accordance with the Federal Financial Institutions Examination Council (FFIEC) Information Systems Examination Handbook and other applicable financial institution requirements and guidelines. The scope of the audit includes reviews of the following areas:

- Status of Findings from Previous Examinations
- IT Organization Structure and Board/Management Oversight
- Network and End-User Computing
- IT Risk Management
- Information Security Program (includes GLBA 501b related requirements)
- Electronic Banking and Website
- Disaster Recovery and Business Continuity Planning

Information Technology Policies & Procedures

RLR has worked with numerous clients assisting them with the development of their policies and procedures for all areas of Information Technology, including the Information Security Risk Assessment and Information Security Program. IT policies and procedures are customized specifically for each client's unique environment and comply with all FFIEC regulatory requirements, covering all required topics.

Information Security Programs

RLR has developed numerous Information Security Programs for our clients. In accordance with FFIEC and GLBA requirements, the Information Security Program is a set of policies and procedures that describe the bank's management responsibilities, security measures and controls. An Information Security Risk Assessment is first conducted to determine the security and control measures needed to adequately protect all bank and customer confidential information.

Information Security Risk Assessment

RLR has worked with many clients to assist with the development of their Information Security Risk Assessment to comply with FFIEC and GLBA requirements. The Information Security Risk Assessment is a documented process to identify the client's information and technology assets, threats to those assets, vulnerabilities, existing security controls and processes, and the current security standards and requirements. The Information Security Risk Assessment also analyzes the probability and impact associated with the known threats and vulnerabilities to the assets, and prioritizes the risks present due to threats and vulnerabilities to determine the appropriate level of training, controls, and assurance necessary for effective mitigation.

Vendor Due Diligence Review

RLR has defined a framework to develop and document the vendor due diligence required for our client's critical Technology Service Providers. Vendor due diligence includes a documented review of the following areas:

- Information Technology & Compliance
- Financial Condition
- Information Security (including Security Assessment Review and Vendor Information Security Program)
- Internal Controls (SAS 70 or similar Independent Auditor's Report)
- Business Continuity/Disaster Recovery Plan and Test Results
- Contract Review
- Client References
- Insurance