IMAGEQUEST℠

BANKING SERVICES

Advisory Services for Information Security, Compliance and Operations

Ever need a helping hand?

- An examiner is asking to see your IT Security documentation.
- You do not have the time – or the expertise — to know where to start.
- You want an IT and Cybersecurity expert at the table during your next regulatory examination.
- Security and compliance requirements are changing faster than you can manage.

ImageQuest's Information Security, Compliance, and Operations Advisory Services for banks provide you with the support you need. You can depend on our expertise to assist with time-consuming regulatory requirements, freeing you to focus more on business initiatives.

This service is perfect for community banks that need additional expertise and services but cannot fill a position to take on these responsibilities.

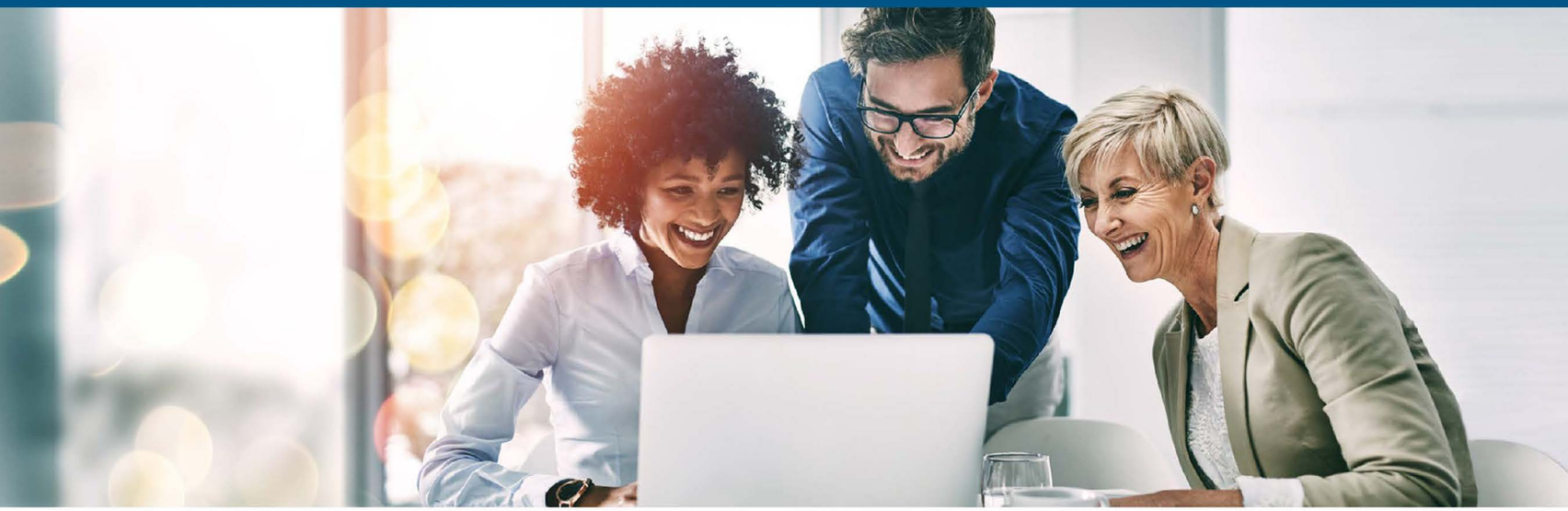
Our knowledgeable advisors fulfill these responsibilities to help you meet the IT compliance and regulatory standards your bank faces.

IMAGEQUEST.COM | INFO@IMAGEQUEST.COM | 888.979.2679

THE IMAGEQUEST℠ APPROACH

FOR YOUR SECURITY & COMPLIANCE

Our expert team is ready to serve you



Hire ImageQuest to:

- Develop, implement, and monitor your Information Security Program.
- Participate in IT strategic planning development.
- Develop an AI strategy for your bank.
- Serve as designated Chief Information Security Officer (CISO) or Information Security Officer (ISO).
- Take an active role in your Vendor Management Program, including coordinating relevant annual reviews and risk assessments for all critical and other designated vendors.
- Oversee all written Information Security (IS) policies.
- Evaluate vulnerabilities and ensure risks are appropriately categorized and scheduled for remediation.
- Coordinate response when an actual incident occurs using your Incident Response Plan.
- Oversee the completion of the Business Impact Analysis or disaster recovery testing of critical functions.
- Coordinate ongoing Information Security (IS) training, including overseeing social engineering testing and reporting.
- Prepare an annual report to your Board/Committee as required by a regulatory authority.
- Be the Subject Matter Experts for Common Vulnerabilities and Exposures (CVEs) and their severity and interoperability within the environment.
- Conduct annual IS or operational risk assessments and maintain risk assessment calendar.
- Maintain all written Information Security (IS) policies, including Business Continuity/Disaster Recovery, Incident Response, and Vendor Management Plans.
- Serve as the liaison for internal audit and exam processes.
- Assist in selecting external auditors.
- Provide Penetration Testing.