

Strategic Technology Consulting

Information Security and Technology solutions designed to fulfill your credit union's compliance needs.



Information security has never been more challenging than it is today. Current trends such as a mobile workforce, BYOD, and cloud computing mean that more of your staff and clients are accessing sensitive business information from more places and in more ways than ever before.

For the credit union, the challenge is to protect this information from loss, from theft, and from increasingly sophisticated threats, while at the same time addressing privacy, compliance, and risk management mandates. Keeping up with the continuous changes, whether to the threat environment you operate in or the new technologies and strategies developed to remain competitive, requires a depth of expertise and experience that most organizations do not possess internally.

The professional information security consultants at AdvantageCIO have been helping credit unions and Credit Union Service Organizations improve their security posture and meet their Information Security and Technology compliance requirements with a wide range of cost-effective solutions.

Contact an AdvantageCIO associate today to learn more about the services available designed to help you more effectively and efficiently allocate your time and resources as part of a robust security strategy.

Who We Are

The experienced technology consultants at **AdvantageCIO** are focused on the specific needs and requirements of the credit union industry, serving organizations large and small.

Our experts offer a unique blend of technology and business experience and understand how to align IT with your business goals, leveraging emerging technologies to strengthen your security posture, while maximizing the returns from shrinking budgets.

With threats to sensitive information growing in both number and sophistication every day, organizations cannot afford an outdated, legacy approach to security.

How confident are you in your organization's overall security posture?



Look inside for what we do

The AdvantageCIO Process

1. **Project Launch and Information Gathering**

The AdvantageCIO consulting engagement begins with a kick-off meeting to identify key individuals, discuss the goals and business objectives based on the status of the existing information security program, and collect existing documentation including previous assessment, audit, and examination reports.

2. **On-Site Assessment and Evaluation**

Our technology consultants will schedule an on-site visit to collect information relative to the Technology and Risk Assessments, Security Policies, and Business Continuity Plan. This will include interviews with key personnel, physical inspection of network infrastructure and access controls, and vulnerability scans from both inside and outside the network.

3. **Document Development and Review**

Once the required information has been gathered, the documentation is generated and presented for review. During the review process, any necessary modifications are made and final drafts delivered.

4. **Implementation and Preparation**

A qualified technology consultant will schedule a document walk-through with your management team to ensure the accuracy and understanding of the contents prior to approval by the Board of Directors. This process may be repeated prior to any scheduled IT audit or examination.

5. **Repeat Annually**

AdvantageCIO recommends that this process is repeated on an annual basis to ensure the documents remain accurate and relevant to your business operations and IT environment.

services catalog, offer new benefits and rewards for and skills available at your fingertips. Live and web

Technology Consulting Services from AdvantageCIO



Technology Assessment

To properly secure the organization's information and information systems, it's important to identify all of the components where information is stored, where it travels, and where it is accessed. The Technology Assessment will review the network topology, including data and voice, inventory the operating system on each appliance, and perform internal and external vulnerability scans to determine where security deficiencies exist. The information gathered is compared against industry guidelines and best practices. The results of the Technology Assessment will be provided in a detailed report including prioritized findings and recommendations for correcting any issues uncovered.



IT Risk Assessment

The purpose of the Information Security Program is to ensure the security and confidentiality of sensitive information, to protect against anticipated threats or hazards to the security or integrity of that information, to protect against unauthorized access to or use of that information, and to ensure the proper disposal of sensitive information. Designing an effective Information Security Program requires an understanding of how the information and information systems are used at the organization and the inherent and residual risk that threaten the security of that information.

Building on the information gathered during the Technology Assessment, the Information Security Risk Assessment reviews and evaluates the physical, logical/technical, and administrative controls currently in place to determine where deficiencies exist. These include policies and procedures, authentication and access controls, data security and encryption, security monitoring, service provider oversight, and much more. The results are provided in a detailed, NCUA-compliant report with categorized risk levels and prioritized recommendations for further mitigation.

Strategic Technology Consulting

Technology Consulting Services from AdvantageCIO (continued)

Comprehensive Information Security Policies (CISP)

The true strength of the Information Security Program can often be found not just in the strategies implemented, but in the relevance and completeness of the policies used to maintain and enforce it. These policies are the guardrails along the sides of the highway that enable your business to operate effectively, efficiently, and securely.

Whether refining existing policies or designing them from scratch, our experienced information security professionals will work with you to develop NCUA-compliant policies including: Acceptable Use, Access Controls, Patch Management, Social Media, Data Encryption, Security Training, Incident Response, Records Retention, Vendor Oversight, and more.

Strategic Technology Planning

When technology investments are not aligned with business goals and objectives, many organizations overspend on technology that they may not actually need, or perhaps worse, underspend on technology resulting in gaps in protection when securing sensitive information and information systems. This often leads to frustration among staff, difficulty in maintaining meeting budget requirements, and deficiencies cited in audit and examination reports.

The Strategic Technology Planning engagement with AdvantageCIO seeks to bring all sides together by assessing where we are today (Technology Assessment) in relation to the business plan and budget, agreeing on the desired target state, and designing a 1 to 3-year roadmap and implementation plan for getting there.

Business Continuity Planning

Business Continuity is defined as “the ability to maintain operations and services, both technology and business, in the event of a disruption to normal operations and services.” Having a recovery plan to “put things back together” when they fail is no longer sufficient. What’s now required is a plan to “continue serving” your members, even during a disruptive event.

Building on the information gathered during the Business Impact Analysis, we are able to prioritize our efforts in developing continuity and recovery strategies to minimize the probability and impact of downtime to business operations. The results are a Business Continuity Plan tailored to your business operations and environment and a testing schedule to validate the procedures in the plan and train personnel on their roles and responsibilities within the plan.

Annual Report to the Board

The Board of Directors (or appropriate committee) is responsible for satisfying the requirements to ensure that the information security program is developed, implemented, and maintained under the supervision of those who are ultimately responsible. To meet this requirement, the members of the Board must be regularly informed of the overall status of the program and compliance with security guidelines. That’s the purpose of the annual report.

The annual report to the Board of Directors will include an ongoing risk management report, examination response and resolution plan, third-party audit results, and any incident response and breach activity.

Exam Preparation

On a regular basis, auditors and examiners will review the Information Security Program to ensure it meets regulatory compliance and security best practices. This process usually involves a list of pre-exam questions and requested documentation. Our information security professionals will assist you in answering the questions and preparing the requested documentation, as well as assist in developing the response to the provided report.

Strategic Technology Consulting



About Us

Addressing your organization's security posture means investing in the tight technology, processes and procedures, as well as taking a proactive approach to building an effective strategic security plan. That just happens to be our specialty.

The professional technology consultants at AdvantageCIO have gained the extensive knowledge and experience required in the credit union industry at all levels, including core data processors, CUSOs, and a network of more than 280 credit unions across the country.

Put our experience to work for you and take your information security program to a higher level. Contact an AdvantageCIO associate today to learn more.

AdvantageCIO is a technology consulting division of:



www.cuanswers.com

Dave Wordhouse

Executive Vice President of Technology

For more than 18 years, David has served in the credit union industry, architecting and implementing network infrastructure and security solutions for CU*Answers, a Credit Union Service Organization, as well as individual credit unions. As Executive Vice President of Network Technologies, David directs a team of nearly 40 information technology professionals in the design, delivery, support and operation of large-scale LAN and WAN solutions, core application platforms, and high availability configurations. Under the CU*Answers

Matt Sawtell

Vice President of Managed Technology Services

Since 2002, Matt has been serving CU*Answers and their credit union clients and owners as an expert across many areas in IT and cyber security. As VP of Managed Technology Services, he leads the Network Services teams in product design, delivery and ongoing support and management for over 280 credit union clients.

Jim Lawrence

Vice President of Business Continuity

As a Certified Business Continuity and Cybersecurity Professional (CBCP/CISSP) and with more than 20 years of experience in IT Management, Information Security, and Disaster Recovery roles, Jim assists credit unions large and small in the design, implementation and testing of their Disaster Recovery and Business Continuity plans, adhering to industry standards and guidelines (NCUA, FFIEC, etc.).

Contact Information:

AdvantageCIO

6000 28th Street SE

Grand Rapids, MI 49546

Tel. 800.327.3478

sales@advantagecio.com

www.advantagecio.com