CYBER SECURITY
EXAMINATION
GUIDANCE
In a March 10, 2014 post to CU Insight, NCUA Board Chair Debbie Matz stated:

Lately, I’ve been doing a lot of thinking about the role of the regulator. I think I’ve figured out a different way to describe it: While optimists see the glass as half full, and pessimists see the glass as half empty, regulators instead worry the glass could shatter and cut someone’s hand. That explains why NCUA is constantly on the lookout for threats to credit unions’ safety and soundness.

Matz went on to discuss the NCUA’s concerns with respect to not only large scale security breaches such as what happened to the Target retail stores, but also with cyber terrorism in the financial services industry. The net result of these concerns is a new focus by the NCUA on credit union cyber security, along with of course, examinations on credit union information security.

As your data processor, CU*Answers can help with some of the cyber security related questions you may see from your examiners. We believe that while the emphasis may have changed for the NCUA, the new examinations are less a revision of previous information security audits and more ‘old wine in new bottles.’ Therefore, we’ve included information about CU*Answers’ cyber security and disaster recovery operations where applicable, to allow you and your examiners understand better how CU*Answers protects you and your members. This report can also be used as a template for you to develop your own cyber security reports when asked by your examiners. Expect your examiners to focus on member data protection, but also your network resiliency in the case of a disaster.

As a cooperative, CU*Answers works for the benefit of all our owners, clients, and their members. Your security is critical to our continued operations.
WHAT TO EXPECT WHEN YOU’RE EXPECTING (A CYBERSECURITY EXAM)

Credit unions undergoing an NCUA cybersecurity exam should be aware of a few key items. First, the NCUA’s development is new to the summer of 2014, and the actual examination team will likely have had only a couple of month’s review of the standards. Second, the examination itself will likely travel on ground that will be familiar to most credit unions. There are a few possibly new areas of focus that a credit union can focus on.

FFIEC AND NCUA RESOURCES

Both the NCUA and the FFIEC have published new online content for cybersecurity. Credit union should visit these pages, review the resources, and incorporate whenever possible the information on these websites into its internal reports. Most important of all is on the NCUA webpage regarding Information Sharing Forums on Cyber Threats, which gives three links to the Financial Services Information Sharing and Analysis Center (FSISAC), the United States Computer Emergency Readiness Team (US-CERT), and FBI Infragard. The most important to include are the reports from FSISAC, which should be included in monthly or quarterly reports to the credit union Board of Directors. In addition, reporting that certain security updates were performed in accordance with the US-CERT (see this Firefox update as an example) will also help your credit union during the examination.

MATURE

You can expect that examiners will review the “maturity” of your IT controls. This means, essentially, how long the controls have been in place and how effective these controls are (or how close to “best practices” your controls are). An example of a control maturity model can be found online from ISACA, pages 17-21.

GOVERNANCE

If your credit union does not already do so, it is highly advisable that executive management and the credit union board of directors be provided with, on no less than a quarterly basis, an update on the cybersecurity of the organization. This does not need to be an extensive report; in most cases just a few pages will suffice. Included should be key security events from the previous report, updates to technology, and most importantly, status on remediation of findings from previous IT exams and audits (even if the decision by the credit union is not to remediate at all). Vendor messages involving security, including those from CU*Answers, can also be very valuable content from the examiners perspective. The next page shows an example of what such a report might look like.

USING THIS DOCUMENT

To the extent possible, information you need to round out your vendor evaluation of CU*Answers’ cybersecurity is included here. As will be noted later in the report, not all information is included. This includes information that could be used to compromise CU*Answers if found by cybercriminals or terrorists.
SAMPLE CYBERSECURITY REPORT

Third Quarter 2014

KEY SECURITY EVENTS


SECURITY UPDATES

All Firefox users upgraded to Firefox 31, per the US-CERT bulletin of July 22, 2014.


WEBSITE HOSTED BY CU*ANSWERS NOT VULNERABLE TO HEARTBLEED

CU*Answers confirmed by website that the credit union’s hosted website is not vulnerable to the Heartbleed exploit.


STATUS ON IT EXAM FINDINGS


ETC.
The Director of Technical Resources for CU*Answers since 1994, Jody Karnes has over 20 years of financial product development experience working with thrift and credit union on-line and in-house products. Prior to coming to CU*Answers in 1994, Ms. Karnes served as the Assistant Vice President of Systems and Programming at Fiserv/Spokane, and has also held Systems Programmer/Analyst positions at various regional financial service and banking organizations.

As CIO, Ms. Karnes oversees the creation, maintenance, and development of all technical products offered by CU*Answers. Her day-to-day focus centers around the technical direction, operation, and development of programming, computer operations, and systems personnel.

For over 12 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 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 Network Services brand, David’s team is responsible for the operation of networks at CU*Answers, three partner CUSOs, and to over 200 credit unions.

David is well versed in network security systems, CISP development and disaster recovery planning and testing. In 2011, David organized AdvantageCIO, a virtual CIO firm specializing in executive technology planning
Joining CU*Answers in 2012, Brian Maurer is the VP of Software Development and oversees the seven teams that make up the CU*Answers programming department. This department oversees and produces all aspects of the CU*BASE core platform as well as It’s Me 247 online banking and related applications.

As an Information Technology leader with nearly 20 years of experience in managing all aspects of IT ranging from Network infrastructure and Software development to Information Security and consultative services, Brian guides the evolving design and functionality of the software development process to CU*Answers. Brian holds a BS degree in Computer Science and a Master’s degree in Computer Information Management from Grand Valley State University.

Since joining the credit union industry in 1985, Jim Vilker has been a strong advocate of managing and educating staff in compliance and audit functions. He launched his career as an examiner where he gained knowledge and depth of insight into regulatory compliance requirements of credit unions.

Jim’s tenure at CU*Answers began in 1998 where his knowledge and skills were immediately recognized as the CUSO’s resident advisor on regulatory compliance and audit functions. Jim has been instrumental in developing the strategic Audit Link business, educating clients through an online Advisor newsletter and designing premier training plans for clients of AuditLink and internal staff of CU*Answers’ credit unions. His experience in working with clients and CU*BASE tools uniquely qualifies him to write and instruct in the monitoring of regulated activities.
Patrick Sickels began his career as an attorney, and quickly branched out into the technological services industry, where he used his legal skills to help companies manage their compliance requirements. Patrick used these skills to develop into a classically trained auditor and risk manager. At CU*Answers, Patrick’s background of law and technology make him uniquely suited to assist credit union clients in managing their risk requirements with a minimum of cost. Patrick is a licensed Certification Information Systems Auditor (CISA), and is pursuing the Certified in Risk and Information Systems Control (CRISC) designation. Patrick has done extensive work in designing risk models and control frameworks for a vast array of commercial, manufacturing, and financial firms. Patrick’s specialty is the design of compliance models which meet legal standards at the lowest possible cost for the organization.

Joining CU*Answers in 2001, Jim Lawrence today oversees the robust Business Continuity program at CU*Answers, encompassing continuity and recovery strategies for each of the CUSO’s state-of-the-art datacenters, ensuring the availability of CU*BASE/GOLD core-processing services.

As a Certified Business Continuity Professional (CBCP) 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.). To complement this service, Jim regularly presents web-based and classroom educational courses on the principles of Business Continuity planning and the value it delivers to the organization through mitigating operational risk.
EXTERNAL IT AUDITS

On an 18-month rolling schedule, CU*Answers conducts three key external audits: an Internal Penetration Assessment, an External Penetration Assessment, and a Network Security Assessment. The Internal Penetration Assessment reviews the strength of CU*Answers’ controls and resiliency from inside our network, the External Penetration Assessment determines how effective CU*Answers is in repelling outside attacks, while the Network Security Assessment reviews the overall security posture of the organization.

These reports are not made available generally because they contain highly sensitive information regarding the CU*Answers’ network. However, the findings of these audits, and any remediation needed, are communicated to CU*Answers executive management and Board of Directors.

FINANCIAL

CU*Answers undergoes an annual financial audit by a third party firm, and publishes these results on our website. In addition, quarterly financial audits are also published here. Reports to owners can be located at this site.

EXAMINATIONS

CU*Answers is also examined by state and federal authorities with respect to information security, although not on a recurring schedule. The last examination took place in October of 2012 and was conducted by representatives from the State of Michigan (lead), State of Ohio, and the NCUA. CU*Answers is prohibited by law from sharing the results of this exam. Credit unions and examiners wishing to see the latest report must petition the State of Michigan Department of Financial Services.

INTERNAL

CU*Answers performs daily, weekly, monthly, quarterly, semi-annual, and annual reviews of its controls with respect to the security of member information and access controls. The results of these reports are published to the CU*Answers’ executive management and the Board of Directors.

SSAE-16

In order to provide our clients with a report on CU*Answers’ controls, CU*Answers conducts an external SSAE-16 review (formerly SAS-70), also on a rolling 18 month schedule. This report can be downloaded here, and describes CU*Answers’ controls with respect to the development of CU*BASE, including Its Me 247 online banking.
HIRING

All potential CU*Answers employees are screened by a third party firm, and all must be bondable against fraud and dishonesty prior to working at CU*Answers. All employees must go through a 90 day probationary period prior to hiring.

POLICIES

CU*Answers has two policy manuals: a general policy manual and an IS&T manual. CU*Answers employees are responsible for reviewing and understanding their security responsibilities contained in these manuals. Included in these manuals are policies on Acceptable Use, Building Security, Client Service, Security Incident Response, and Member Privacy. A copy of the general policy manual is available upon request. The IS&T manual contains information which is sensitive and not provided except to those employees entrusted with fulfilling those responsibilities.

TRAINING

All employees are required to attend building and IT security training as part of their orientation period, and to continue to attend security training at CU*Answers for the duration of their employment.

EMPLOYEE DISCIPLINE

Employees are tracked each month for any policy violations, and these violations are reported to executive management and the Board of Directors. Discipline for policy violations may include termination of employment.

IT STRATEGIC REPORT

CU*Answers internally publishes an annual Strategic Technology Report. This report reviews CU*Answers direction, capacity planning, and other key items for information technology.

SOFTWARE DEVELOPMENT

CU*Answers follows an SDLC program for updates of CU*BASE and other data processing software, including online banking. This process involves project development approval (including customer requests), development process, and quality testing before a release into production.

BADGES AND KEYFOBS

CU*Answers facilities are locked down, requiring keyfob entrance. All visitors must wear badges to identify their status (e.g. Visitor) and visitors must be escorted through the building. Access to CU*Answers’ data centers is strictly controlled and strictly limited to those persons who must enter for operational reasons.

LOGICAL ACCESS

Most CU*Answers employees are not local administrators to their workstations. Critical system access review is completed on a regular basis. When employees leave, network access is removed no less than 48 hours (usually completed almost immediately upon termination).
LOGGING, INCIDENT, PATCH, AND VENDOR MANAGEMENT

LOG MANAGEMENT
CU*Answers utilizes firewalls, DMZs, and intrusion detection as part of its strategy against hostile attacks from outside the network. Alerts and logs are reviewed and included in the network run sheets. The run sheets are reviewed by the auditing team to ensure completeness of the record.

Critical systems that power CU*BASE are reviewed by that systems team. Environmental controls and alerts are present in each of the data centers.

INCIDENT MANAGEMENT
CU*Answers uses an automated ticketing system (Latitude) to manage incidents and their priority. Tickets are reviewed by management and escalated depending on the priority of the incidents and the length of time the incident remains without being closed.

PATCH MANAGEMENT
CU*Answers subscribes to a service that reviews patches for the various OS and software used to power and control systems. Patches are reviewed for their critically and evaluated for risk.

Antivirus is managed centrally, and local workstations are controlled by a central patch management system.

VENDOR MANAGEMENT
For its critical IT services, CU*Answers uses major providers such as IBM, Dell, CenturyLink, and Comcast. Other services go through a screening and budgeting process requiring executive management approval.

NETWORK REDUNDANCY
CU*Answers has multiple, redundant, and secure network connections from and to each of its data centers.

SERVER REDUNDANCY
Critical servers are mirrored, and data is backed up and/or replicated amongst multiple data centers located in three different locations. One location is over 50 miles apart from the others.

BACKUPS
Most critical systems are backed up virtually, and immediately, through VM ware mirroring.

On systems that uses backup tapes, these tapes are encrypted, copied, and stored in secure locations or

ENCRYPTION
Sensitive data is encrypted over secured connections to and from CU*Answers’ data centers. This data is also encrypted in storage.
CU*Answers maintains a Disaster Recovery Plan which is updated on a bi-annual basis. The basic outline of the plan can be found here. Details of CU*Answers Disaster Recovery plans can be found here.

As part of an ongoing business continuity program, CU*Answers actively maintains a high-availability (HA) core-processing environment with real-time CU*BASE/GOLD data replication between identical hosts located at two geographically dispersed, state-of-the-art datacenters.

CU*Answers performs regular testing of recovery plans. These testing exercises provide the maintenance windows needed to give our systems a tune-up through hardware and operating-system upgrades and replacement without requiring application downtime. Keeping our systems running on all cylinders increases availability when we and our clients need it most.

In addition to our Hot Site and HA Recovery Plans, regular tests are performed on other applications and critical-vendor system processing including our Item Processing and Statement Printing Services.

A minimum of twice each year, HA rollover events are scheduled to redirect core-processing and operations to the secondary datacenter for a minimum period of three business days. At the completion of each event, core-processing is redirected back and operations resumed at the primary datacenter. These HA rollover events are invaluable in our effort to validate our procedures and ensure our ability of recovering CU*BASE core processing in an effective and timely manner.

You can review the latest report here.
Whether your requirements call for the development of a new recovery plan or program or to improve an existing one, our goal is still the same: to quickly and effectively ensure your organization is prepared for a disruption, while also setting the foundation for a long-term continuity program that adapts to your changing needs in both business and technology.

The same talent, skills and expertise used to safeguard core processing for the CU*Answers network is available to your organization. Our experience in the credit union industry will help guide your program so that it properly measures up to regulatory requirements (NCUA, FFIEC, etc.), standards and guidelines, peers in the industry, and professional best practices. To accomplish this, we offer the right mix of professional services shown below in the following groups:

Contact a CU*Answers Continuity Consultant today to custom design an engagement that best meets your business objectives.
PLANNING AND CONSULTING SERVICES

Meetings and Conversations to help raise awareness and gain an understanding of business continuity principles and practices and how they help protect core assets.

Needs Assessments to evaluate where your organization’s preparedness level is today and develop goals and objectives to bring it where it needs to be.

Review previous Audits, Examinations and Incidents and identify gaps to help design a roadmap highlighting the steps and resources required to implement a continuity program that meets your business objectives and best prepares you for the next one.

DESIGN AND DEVELOPMENT SERVICES

A plan “Health Check” to Review and Recommend enhancements and improvements for existing recovery and continuity plans to ensure accuracy, completeness, and compliance with organizational goals and industry standards where appropriate.

Design and Develop a new (or upgrade an existing) recovery and continuity plan with scopes ranging from basic core processing recovery to comprehensive IT and business resumption.

On-going Plan Maintenance and change management to ensure your plan is complete, current and relevant to your organization today.

Identify Continuity and Recovery Strategies to improve existing controls and procedures to bridge the gap where recovery capabilities do not match with recovery objectives today.

IMPLEMENTATION AND COORDINATION SERVICES

Design and coordinate Training and Awareness programs and events to help build a “culture of continuity” and to ensure staff is knowledgeable of their roles and responsibilities within the recovery and continuity plans.

Design and coordinate plan Testing and Exercising program to validate procedures and sharpen recovery skills for personnel with roles and responsibilities within the plan, and build confidence in your organization’s ability to recover in a timely and effective manner.

Assist in Plan and Program Implementation, complementing and collaborating with existing teams, eliminating the need to hire, train, and retain additional skilled personnel with DR/BC expertise.
A “one-size-fits-all” approach is not realistic or cost effective. An initial consultation to identify the objectives and scope of the engagement will help us build a custom blend of services to best meet your specific needs.

Affordable solutions are available ranging from high-level planning and consulting engagements, to plan health checks and full program development and implementations. Custom statement of work and proposals are provided for each project.

For more information, contact a CU*Answers Continuity Consultant today!
ADVANTAGE CIO

Many small and medium businesses recognize the need for senior strategic technical leadership but may not have the income statement or business plan to justify a full time Officer level position. They understand they are not reaping enough ROI from their technology, may have difficulty pushing projects through to completion on time and on budget, or simply need direction.

AdvantageCIO provides technical leadership engagements on demand to propel organizations through their business plans in a cost effective and efficient manner with no long term commitments while realizing ROI on technology, perhaps for the first time.

REVIEW BUSINESS PLANS

Effective IT leadership begins with understanding the client’s business plans. Where is the firm now, and where do they want to go? Where are they struggling with IT and where are they winning? Only by understanding goals and timelines can an effective IT strategy be conceived and executed.

SET IT VISION AND STRATEGY

Once the business plans are understood, AdvantageCIO will develop a vision and execution strategy for leveraging IT resources to accomplish stated objectives. The vision will be focused and on target and the strategy engineered to accomplish goals within defined budget parameters.

PLANNING AND PROCESS

The IT strategy must be implemented according to a well defined plan with measurable milestones that are understood by all stakeholders. Sometimes multi-level plans targeted with sections targeted towards business leaders and technical implementation and support staff are required. Policy development and modification is almost certainly a part of this process as are risk assessments and modifications of disaster recovery and business continuity documentation. Audit compliance is a significant factor in this phase.

INTEGRATE IT FOR SUCCESS

Many times technology exists to serve itself, not the goals of the business or for the benefit of the user base. This is a common scenario in many organizations where technical staff have implemented or attempted to implement solutions that exceed business requirements or require after purchase maintenance and support commitments that are not fully understood by leaders in
advance. Another common problem occurs when requirements are not properly defined or communicated in advance of executing on a project.

**CULTIVATE IT TALENT**

How does today’s business leader make hiring decisions for technical talent? How do they effectively complete annual planning sessions for a position for which they have little understanding? How does one motivate a “nerd”? How does one navigate a technical resume and effectively sift through piles of candidates for the right hire?

More often than not, today’s non-technical manager is lost dealing with technical talent and making effective hiring decisions. AdvantageCIO’s staff is expert at hiring and managing IT staff and performing effective annual planning sessions that will cultivate and grow talent so they remain challenged and focused on executing at the highest level.

**MAKE IT HAPPEN**

Too many large technical implementations fail. The causes are varied: lack of executive buy in, incomplete or incorrect requirements, selecting the wrong vendor, scope creep, over complication (“gold plating” the solution), lack of effective milestones, inability to enforce milestones, under estimating the budget. Almost all of these can be tied to ineffective project management. The successful project will successfully navigate these pitfalls and drive the project through to completion by understanding the business requirements and use of well developed and thoroughly executed implementation processes.

Learn more about AdvantageCIO online!
AuditLink as a service has been in business since May 2008. True to its commitment, AuditLink reduces the added work imposed by regulations and compliance. Factors inherent in changing regulations mandate continuous training and frequent exposure to compliance issues with applied auditor solutions. The forecast indicates greater focus in these areas, with stringent penalties for violators. Consequently, this places a higher degree of accountability on your staff to assure these regulatory requirements are met. This increases day-to-day activities at an alarming rate absorbing time that should be devoted to serving your members.

Each month, AuditLink provides you and your staff with an Executive Summary stating the auditing activities performed with their outcomes. Written recommendations seek to improve your internal procedures and provide ongoing training.

Download the AuditLink Services Brochure