DCU BULLETIN

Division of Credit Unions
Washington State Department of Financial Institutions
Phone: (360) 902-8701 FAX: (877) 330-6870

October 23, 2015 No. B-15-13

Changes to Information Technology Exams in Washington State

Cybersecurity has been identified as a significant threat to financial institutions and credit unions and banks are a primary target for cyber theft. Additionally, data breaches and credit card losses have become much more frequent and expensive. Because of this, the Division of Credit Unions (Division) decided to allocate more examination resources to cybersecurity and information technology (IT) exams. We did this by selecting an IT contractor (see below) to assist us on performing IT examinations. The following are the main reasons why the Division decided to use an IT vendor rather than internal resources to improve its IT exam program: (1) We currently do not have the IT experience or resources on staff; and (2) The Division has the financial resources to pay for the vendor contract.

New Contractor for IT Exams

The Division selected Security Compliance Associates (SCA) as its primary vendor to assist the Division in performing IT examinations from November 2015 through the end of the current biennium (June 30, 2017). SCA has approximately 170 credit union clients in 40 states, and has performed IT security work for credit unions and other clients for over 10 years. SCA was selected as a result of the state contracts bid process in which eight applicants submitted bids to the Division.

The goals of the IT examination contract are to improve the Division's IT examination program and to increase its effectiveness in helping credit unions further develop their IT security programs. The process of performing Division IT exams will remain mostly the same (e.g. IT exams will be conducted during safety and soundness exams and most of the IT questionnaires and requested exam documents will remain the same), and Glenn Ross, Division IT examiner, will continue to perform IT examinations. The main difference will be more resources and hours will be devoted to IT examinations (i.e. one to two additional days will be added to the standard IT exams beginning in 2016). Examination hours will be scaled either down or up given the types of technologies used by credit union and given other IT risk factors. Also, we will update our IT examination templates and questionnaires to make them more useful. This will include, updating the IT pre-exam letter and summary of information request, and refining the IT questionnaires.

IT Examination Focus

Future IT examinations will focus on cybersecurity (see below) and will identify areas of IT security and cybersecurity weaknesses at state chartered credit unions.

Cybersecurity - We highly encourage credit unions to use the new FFIEC cybersecurity assessment tool to help assess their cybersecurity preparedness and to advance their IT security programs. The cybersecurity assessment tool is a good baseline assessment. Credit unions who use the assessment should strive to an assessed program maturity level that is appropriate for the credit union, given the credit union's inherent cybersecurity risk profile.

The use of the FFIEC cybersecurity assessment tool is optional; however, and it will not be used by examiners to perform IT examinations. It is designed as a credit union self-assessment tool and not as an examination tool or examination questionnaire.

Beginning in January 2016, Division IT examiners, including SCA examiners, will ask credit unions whether they have performed the FFIEC cybersecurity assessment, and if so, examiners will review and go over the FFIEC cybersecurity assessment with the credit union's IT personnel.

It is incumbent upon senior management and the board of directors to be sufficiently knowledgeable about cybersecurity in order to manage the credit union's IT risks.

NCUA provides cyber security resources at http://www.ncua.gov/Resources/Pages/cyber-security-resources.aspx.

Other areas of IT examination focus are:

- **Incident Response Program –** How prepared is your credit union to successfully respond to a security breach of confidential member information? Has the credit union's incident response program been documented and is the program periodically tested? Could business operations successfully recover after a security breach or cybersecurity incident?

- **Security Awareness Education & Training –** Training and education of staff and volunteers is fundamental to protecting confidential information and helping to prevent or detect cyber-attacks and to minimize their impact on continuing operations.

- **Information Security Policies and Procedures –** Strong policies and procedures are important to a solid IT security program.

- **Vendor Oversight as it Relates to Keeping Sensitive Member Information Secure –** Not only is it important that the credit union have strong IT internal controls and testing, the credit union must take the necessary precautions and perform due diligence to ensure the vendors its uses keeps member confidential information secure.

The Division understands that cybersecurity and information security does not have a one size fits all solution and that the success of an information security program is dependent upon a credit union's business model, size, complexity, product offerings and delivery.

Any questions regarding this Bulletin should be directed to Doug Lacy-Roberts at Doug.Lacy-Roberts@dfi.wa.gov or (360) 902-8753.