DCU BULLETIN

Division of Credit Unions
Washington State Department of Financial Institutions
Phone: (360) 902-8701 ***FAX: (360) 704-6901***

August 11, 2009 No. B-09-06

Linking the Testing of Key Information Security Controls to the Risk Assessment

The risk assessment is an integral part of the information security program. As such, the risk assessment should guide the testing of key controls, systems and procedures associated with the information security program. Recently, Information Technology examiners expressed concern that they rarely find testing of security controls for key information and they are not finding the testing tied to the credit union's risk assessment. It is the Division's expectation that credit unions will tie the testing of key information security controls, systems and procedures to their risk assessment.

The information security risk assessment is the process used to identify and understand risks to the confidentiality, integrity, and availability of information and information systems. Thus, the resulting information from the risk assessment should be used to develop strategies to mitigate these risks/threats. Also, a sufficiently detailed risk assessment enables senior management and the board of directors to better understand the information security risks and the effectiveness of the controls in place to mitigate these risks/threats.

Assess Risk

The remainder of this Bulletin presumes your credit union has already completed a comprehensive information security risk assessment. An information security risk assessment should address the following:

- Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of member information or member information systems;
- Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of member information;
- Assess the sufficiency of policies, procedures, member information systems, and other arrangements in-place to control risks; [1]
- Identify the controls in-place to mitigate the identified threats.

After your credit union has a documented information security risk assessment, then the testing of controls, systems and procedures should occur next.

Testing of Controls, Systems and Procedures

Credit unions should regularly test the key information security controls and the systems and procedures related to these key controls. The frequency and nature of the control testing should be determined by the likelihood and potential damage of the threats identified in the risk assessment. Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs. **[2]**

The Risk Assessment Document Guides the Testing of Key Information Security Controls

The frequency in which your credit union tests controls should be based on the degree of identified risk. The degree of identified risk (low, medium, high) associated with each threat is determined by both the likelihood (low, medium, high) that a threat could occur and the impact (low, medium, high) that a successfully executed threat would have on your credit union. Highest rated risk equates to high likelihood and high impact, while lowest rated risk equates to low likelihood and low impact. The controls identified to mitigate higher risk threats should be tested more frequently. Each credit union should establish their testing frequency based on the risk level.

		Impact		
		High	Medium	Low
Likelihood	High			
	Medium			
	Low			

The following are examples of high and low identified risks:

High Risk:

Indentify Risk

- You identified as high-risk that a threat to the credit union's network's user passwords could be guessed or cracked allowing unauthorized network access.

Control

- You determined that a key authentication control was to be implemented requiring all users to create passwords at least 8 characters in length containing a combination of upper and lower case letters, numbers and special characters.

Frequency of Testing

- You decided the implemented key password authentication control will be independently tested every 12 months. This decision should then be documented in your risk assessment.

Test Implementation

- The next step is to have someone independent of designing or implementing this control perform testing to determine if the control works as intended. This control would be tested by checking that all passwords have to be at least 8 characters, the passwords are complex, default passwords have been changed, and passwords are not written down anywhere. In addition, the password reset process should also be tested. For example, this could be tested by checking that the help desk satisfactorily verifies password reset requests. The testing may also involve checking that passwords have been changed or accounts deleted for employees who have changed positions or left the credit union.

Low Risk:

Identify Risk ➢ You identified as a low-risk, the threat of a document containing non-public member information being stolen from a credit union employee’s work area.

Control ➢ You determined that a control was implemented to require shredding of all unnecessary documents containing non-public member information.

Frequency of Testing ➢ You decided this key control will be independently tested every 18 months, because employee training emphasizes the use of shredders.

Test Implementation ➢ The testing of this control could consist of checking work areas and trash cans to see if they find documents with non-public member information. If so, then the control (use of shredders) is not working correctly.

Once testing of information security controls is completed, the risk assessment should indicate either that a control is effective in mitigating the identified threat or indicate what corrective action(s) will be taken to address the ineffective control. Perhaps education is required to help employees more successfully implement the control. Also, a particular threat may require additional controls in order to properly mitigate risks/threats. The testing of new controls to augment the effectiveness of ineffective controls should be performed as soon as the new corrective action is implemented. For controls tested to be effective, tests should be repeated according to the frequency indicated in the risk assessment.

Please contact Glenn Ross at (360) 481-2551 or Doug Lacy-Roberts at (360) 902-0507
if you have any questions.

(1) 12 CFR 748 Appendix A, Section III B

(2) 12 CFR 748 Appendix A, Section III C 3