DCU BULLETIN

Division of Credit Unions
Washington State Department of Financial Institutions

Phone: (360) 902-8701 ***FAX: (360) 704-6901***

May 30, 2001 No. B-01-11

Information Systems & Technology (IS & T) Exams Beginning July 2, 2001

Results of Initial Exams

As reported in Bulletin B-01-01, the Division conducted eight IS & T exams during the first four months of this year. We solicited comments from the credit unions examined to aid us in structuring the IS & T exams from this point forward.

Those exams were conducted using the FFIEC Information Services rating system adapted to credit unions. Attachment I provides a description of those ratings. The distribution of ratings was: four "1" rated, three "2" rated, and one "3" rated credit union. In general, most credit unions are working hard to provide all of the key elements of a sound information system (IS).

However, we did find a number of areas of surprising weakness. While there was no single weakness that was common to all eight credit unions, areas of weakness included: inadequate audit of IS functions, lack of board approval of IS policies and plans, inadequate system security or security reviews, and inadequate disaster recovery planning or testing.

Future IS & T Exams

On July 2, 2001, the Division will begin the IS & T exams for all credit unions. Those exams will generally occur during the regularly scheduled safety and soundness exams. However, our third party contractor, DHK Associates, will be conducting the IS & T portions of the exams. We will be using the NCUA's E-commerce and Electronic Data Processing Review Questionnaires as the starting point for the exams. Those questionnaires may be found at www.ncua.gov, under Information Systems & Technology, under Letters to Credit Unions.

We will bill each credit union for the cost of each I S & T exam as permitted by WAC 208-418-070 (3). We anticipate that most IS & T examinations will be completed in three to five days and that all credit unions will receive their first I S & T examination within the next eighteen months.

The safety and soundness report will be modified to include a separate rating and findings comments for the IS & T efforts of each credit union. The ratings reflected in Attachment I will continue to be used for this element of the exam. While that rating will be reflected separately in the report, it will also be necessary to incorporate the effects of the IS & T rating into the Management component to maintain consistency with NCUA's CAMEL ratings.

The Division will generally be sending a first day Summary of Information request list for IS & T items to credit unions eight to ten weeks before the exam. That request list has been abbreviated and adapted to be consistent with the NCUA E-commerce and Electronic Data Processing Review Questionnaires. A copy of that list is included as Attachment II and is available on the Division web site at www.wa.gov/dfi/cu/home.htm.

When the IS & T portion of the exam identifies areas of weakness, those items will generally be incorporated into the Items for Management Action page of the safety and soundness exam for CAMEL 1 and 2 rated credit unions and into Supervisory Agreements for 3, 4 or 5 rated credit unions.

If you have questions about I S & T examinations, please call Mike Delimont at (360) 902-8790.

Attachment I

IS & T Composite Ratings

The composite rating can range from 1 through 5, with 1 representing the best and 5 the worst rating. To arrive at the composite rating, the interrelationships and relative importance of the functions rated under the component category must be considered. Occasionally there will be factors that are not reflected in any specific performance rating, but are important to the credit union's overall condition. They should be reflected in the organization's final composite rating. Each composite rating is described as follows:

IS & T Composite – 1

Credit unions in this group are sound in almost every respect. If deficiencies are noted, they are minor and can be handled routinely and without further supervisory involvement.

IS & T Composite – 2

Credit unions in this group are fundamentally sound, but may reflect modest weaknesses. Deficiencies are generally corrected in the normal course of business. Therefore, the need for supervisory response is usually limited.

IS & T Composite – 3

Credit unions in the group experience a combination of adverse factors that require timely corrective action. Problems are well defined and require more than ordinary supervisory concern and monitoring. The overall strength of management and supporting staff and the financial capacity of the data center is such as to make operation failure only a remote possibility.

IS & T Composite – 4

Credit unions in this group are operating under unacceptable conditions that could impair future viability. A high potential for operational and/or financial failure is present. Still weaknesses are not so severe as to threaten the immediate failure of the data center. Immediate affirmative action and supervision by the regulator are necessary.

IS & T Composite – 5

Credit unions in this group exhibit a combination of weaknesses and adverse trends that are pronounced to a point that threatens the ultimate continuation of the operation. Immediate affirmative action and continuous supervision, as required by the regulator, are necessary.

Components

IS & T components will not receive separate ratings. The components that will be considered will include a general category, risk assessment, compliance and legal, audit and consulting services, vendor management, member service and support, personnel, systems architecture and controls, security controls, business continuity and performance monitoring.

Attachment II

Information Services & Technology (IS & T)
Summary of Information Request

Exam cutoff date: July 1, 2001

Previous examination date: Not Applicable

Projected examination start date: July 2, 2001

DFI takes steps to protect the confidentiality of personal information, to the extent permitted by law. However, all information collected by DFI becomes a public record and may be subject to inspection and copying by the public, unless an exemption or other protection in law exists. A copy of our privacy policy is available upon request.

General Directions

Reports and information should be prepared as of the exam cutoff date. Management may wish to discuss individual credit union report options with the Examination Supervisor or the EIC examiner prior to the exam start. **If you cannot provide the documents or answers requested, please indicate why. If a particular question is not applicable, simply indicate N/A.**

Supporting Documentation

Some questions in the EC-1 questionnaire require supporting documentation in order to verify the response given. For each of the major sections of the EC-1 questionnaire, examples of supporting documentation are listed below. To the extent appropriate, please have this documentation available for the examiners.

Section 1. General:

1.1. Please complete the attached EC-1 Questionnaire

1.2. Provide all written policies and procedures that relate to information technology management, E-commerce, electronic delivery systems, and information technology security

1.3. Board packets for the most recent 12 months, including reports from the Supervisory Committee and any other committees involved in technology initiatives

1.4. a) Credit Union organizational charts, including b) IT and E-Commerce departments

1.5. Copies of any strategic or business plans related to technology initiatives

Section 2. Risk Assessment

2.1. a) Risk Assessments of E-Commerce, Information Technology and related activities. b) Include any responses and evidence of corrective actions.

Section 3. Compliance and Legal

3.1. a) Legal opinions or b) other related correspondence from counsel related to E-Commerce.

3.2. a) Most recent insurance coverage review and b) recommendations performed by the bonding company, as well as a c) copy of the current bond policy

Section 4. Audit and Consulting Services

4.1. a) The resume and b) job description for the internal auditor

4.2. a) Audit standards, b) schedules and c) programs for IT and EC activities.

4.3. a) Internal and b) external audit reports issued within the past eighteen months, c) including management responses and evidence of corrective actions.

4.4. Copies of any a) internal or b) external reports related to penetration testing and intrusion detection.

Section 5. Vendor Management

5.1. Audit reports (e.g. SAS70) from vendors of core business systems, including all E-Commerce systems

5.2. Evidence of the financial stability of primary IT/EC vendors.

5.3. Vendor contracts and service agreements.

5.4. Outline participation in user groups, advisory councils, etc.

5.5. Performance reports and logs of member service calls

Section 6. Member Service and Support

6.1. Incident reporting logs and reports.

6.2. Member help documentation for E-Commerce applications

Section 7. Personnel

7.1. a) Training plans and b) profiles for IT personnel

7.2. Certification and other professional credentials possessed by staff

7.3. a) Employee development plans and b) succession plans

Section 8. System Architecture and Controls

8.1. Network Topology Diagram (Do not include actual IP addresses)

8.2. Hardware and Software inventory (Do not include individual Workstations)

Section 9. Security Controls

9.1. Inventory of Security hardware and software, including firewalls, intrusion detection, user access controls, encryption devices, secure modems, user authentication components, virus protection software, etc.

9.2. Copies of recent reports related to authentication and intrusion detection.

9.3. Access control logs showing addition, changes and deletion of user privileges, including evidence of periodic management review

9.4. Description of physical security controls for IT hardware and software.

9.5. Evidence of updates to virus protection and intrusion detection applications

Section 10. Business Continuity

10.1. Copy of the Disaster Recovery and/or Business Continuity Plan

10.2. Copies of reports related to tests of the Disaster Recovery/Business Continuity plans done within last 18 months

10.3. List of the backup tapes, disks, documentation, supplies, etc. kept at your off-premises storage facility

10.4. Copies of Disaster Recovery Plans and agreements with Service Providers

Section 11. Performance Monitoring

11.1. Reports related to E-Commerce usage and activity levels

11.2. Member feedback regarding E-Commerce applications