BRITISH COLUMBIA | Financial Institutions Commission

February 1, 2016
File No.: 71000-05
Ref. No.: 1385

To: CEOs/General Managers, British Columbia Credit Unions

Re: CUPSA Information Technology (IT) Audit Guidance

The Credit Union Prudential Supervisors Association (CUPSA) has issued IT Audit Guidance, which outlines sound principles and practices for undertaking an IT audit at a Canadian credit union. The guidance is consistent with international standards and is scalable to the relative size, scope and complexity of individual credit unions.

FICOM encourages BC credit unions to review the CUPSA guidance to help inform their own IT audit regimes. IT and audit committees may also find this guidance useful in discharging their oversight functions.

CUPSA is an interprovincial association composed of credit union prudential supervisors across Canada that works toward maintaining a sound and sustainable credit union sector. For further information, visit CUPSA's website at www.cupsa-aspc.ca.

If you have any questions regarding the CUPSA guidance, please contact Hugh Poon, IT Risk Specialist, FICOM at Hugh.Poon@ficombc.ca.

Sincerely,

Frank Chong

Frank Chong
Deputy Superintendent, Regulation
Financial Institutions Commission

Enclosure

MOB/db

2800, 555 West Hastings
Vancouver, BC V6B 4N6
Telephone: 604 660-3555
Facsimile: 604 660-3365
www.fic.gov.bc.ca

Information Technology Audit Guidance

An information technology (IT) audit is an assessment of the practices, policies and controls within an organization's computing environment that collects and evaluates evidence of an organization's information systems, practices and operations. The evaluation of this evidence determines if the information systems are safeguarding the information assets, maintaining data integrity, protecting against cybersecurity risks and operating effectively and efficiently to achieve the organization's business goals or objectives.

Incorrectly, the concept of an IT audit is often used synonymously with the concept of an IT security audit. While IT security is a component of an IT audit, other aspects of IT governance, risk management and operations are necessary for a comprehensive IT audit. IT audits also consider effectiveness, efficiency, value for money, return on investment, culture and people related issues that might affect the ability for the IT environment to support organizational goals.

This guidance paper was developed for credit unions and caisses populaires to increase awareness of IT audit concepts, and to assist senior managers when considering the use of an IT audit within their organizations.[1] The IT audit areas noted in this guidance are intended to be scalable to the relative size, scope, complexity and risk profile of an institution.

Common IT Audit Practices

Defining the purpose and scope of the IT audit is critical to receiving the assurance required by the board of directors and management. This section outlines various areas of a traditional IT audit. Each audit may consist of these elements in varying measures; some audits may scrutinize one or more of these elements. Each credit union or caisse populaire should evaluate the appropriateness of these areas when considering the scope of an IT audit. Appendix A lists additional web-based resources[2] to help readers better understand each of the audit areas below in more detail.

[1] CUPSA encourages credit unions to also review recommended IT audit principles and practices of international standard-setting bodies (e.g. ISACA, Institute of Internal Audit (IIA), International Organization for Standardization (ISO), etc.).

[2] Resources provided are for information purposes only and are not endorsed by CUPSA.

Business/IT Strategic Alignment Review

Business/IT strategic alignment reviews involve determining if information technology resources are aligned with the credit union's strategic plan and operational needs. Common practices could include:

- Assessing whether mechanisms and metrics exist to ensure that IT projects are aligned with corporate objectives;
- Assessing whether senior management has reliable information on IT projects for decision-making purposes; and
- Evaluating how the credit union or caisse populaire measures the value obtained from investment in IT.

Systems Administration Review

System administration reviews involve assessing the adequacy and effectiveness of administration procedures, security practices, and maintenance processes of internal servers and systems, including operating systems, virtualized platforms, database systems, etc. Common practices could include:

- Reviewing management, maintenance, and security practices around internal servers and workstations; and
- Reviewing policies and procedures around system administration (e.g. patch management, licensing).

Application Review

Application reviews, or application control reviews, assess an organization's critical business applications, information processing systems, and management information systems. It is critical that the auditor is knowledgeable in the organization's business functions in order to perform these types of reviews. Common auditing practices could include:

- Reviewing an application's adherence to business rules in the flow and accuracy of processing;
- Confirming validation capabilities of data inputs within each application;
- Reviewing access control and authorizations of all users within an application; and
- Verifying application error and exception handling, logging, and audit trails.

Network Security Assessment

Network security assessments focus on the internal and external network architecture that supports an organization's computing environment, including firewalls, routers, switches, etc. Common auditing practices could include:

- Reviewing the organization's network architecture;

- Reviewing perimeter security countermeasures (e.g. firewalls, intrusion detection/prevention systems, etc.);
- Reviewing the overall internal security architecture and policies;
- Reviewing the effectiveness and completeness of networking infrastructure implementations/configurations (e.g. access controls); and
- Reviewing policies and procedures for security management processes (e.g. incident management, vulnerability assessment, patch management).

Business Continuity Review

Business continuity reviews focus on the appropriateness and effectiveness of an organization's disaster recovery and business continuity documentation, capabilities and infrastructure. Common practices could include:

- Evaluating the quality and appropriateness of business continuity planning/disaster recovery planning (BCP/DRP) documentation and processes;
- Reviewing maintenance and testing procedures of BCP/DRP documentation and processes; and
- Evaluating DR site capabilities and resumption strategy in order to meet organizational requirements.

Data Integrity Review

Data integrity reviews observe live data in transit and storage to verify the strength and appropriateness of controls, the impact of weaknesses, and the reliability and trustworthiness of data and information within the organization. Common practices could include:

- Reviewing the accuracy and consistency of data stored in databases, data warehouses, data marts, etc.;
- Reviewing the ongoing use of error checking and validation routines; and
- Assessing protection mechanisms such as data encryption, backup, access controls, input/data validation, etc.

Physical Security Review

Physical reviews include assessments of physical security, power supply, air conditioning, humidity control, fire suppression and other environmental factors and their effect on information technology operations. Common practices could include:

- Performing remote intelligence gathering and reconnaissance activities;
- Reviewing physical security controls of buildings, data centers and other facilities related to information technology resources;
- Undertaking physical penetration testing and evaluating countermeasures; and

- From a BCP/DRP perspective, determining the level of protection, resilience and resumption provided by physical premises.

Project Management and Change Management Review

Project management/change management reviews evaluate project management practices and change management processes that are used during the planning, design, development, implementation and testing phases of IT initiatives.

Common practices could include:

- Assessing and reviewing the use of project management deliverables during IT-based projects (charters, plans, change requests, etc.);
- Performing post-mortems on completed projects to evaluate the achievement of goals and objectives, meeting or exceeding user or system expectations, and adherence to scope, timelines, budgets, etc.; and
- Reviewing change management processes for the integration of new systems, and determining how recent systems have been introduced to users and computing environments.

IT Audit Roles and Responsibilities

A sound understanding of appropriate roles and responsibilities is essential to an effective IT audit function. CUPSA has identified key roles and responsibilities[3] as follows:

Board of Directors/Audit Committee

- Ensuring that IT audit is included and addressed within the internal control framework;
- Determining the most effective method of obtaining IT audit resources (in-house vs outsourced);
- Ensuring an effective level of knowledge and understanding of IT among board directors;
- Reviewing and approving appropriate IT audit plans;
- Evaluating management responses to audit findings and recommendations;
- Evaluating performance of IT audit initiatives;
- Preserving independence of IT auditors, regardless of choice for IT audit; and
- Receiving and reviewing reports from senior management on material IT risk, including processes to manage these risks.

[3] Roles and responsibilities outlined should be applied based on the size, scope and complexity of individual credit unions or caisses populaires.

Senior Management

- Determining the most effective method of obtaining IT audit resources (in-house vs outsourced) – this responsibility should be shared with the Board of Directors;
- Identifying areas of IT-related risk through the internal risk management function;
- Assessing and approving the organization's IT control framework;
- Addressing IT audit findings and recommendations and implementing control improvements; and
- Obtain evidence of IT audits on products and services that are outsourced to third party providers.[4]

External/Internal Audit

- Assessing IT controls and practices based on approved audit plans;
- Obtaining outside expertise for IT audit areas that require additional knowledge and skills; and
- Regularly communicating results of IT audit findings to the Board or Audit Committee.

Third Party Service Providers

- Providing evidence of IT audits on products and services that they offer credit unions and caisses populaires.

Regulators

- Assessing whether IT risks to which the credit union is exposed are managed using an IT governance framework; and
- Encouraging credit unions and caisses populaires to obtain confirmation that all IT products and services (both in-house and outsourced) are being audited or reviewed by a third party and that audit recommendations are being addressed.

[4] When relying upon third party service provider audit reports, it is management's responsibility to ensure that the scope of the audit matches the services being received by the credit union/caisse populaire.

CUPSA | ASPC

Appendix A – Additional IT Audit Resources

Business/IT Strategic Alignment Review

- http://info.knowledgeleader.com/bid/179384/Auditing-IT-Management-Aligning-IT-with-Business-Priorities
- https://businessitalignment.wordpress.com/2010/12/22/strategic-alignment-maturity-model-luftman/
- http://www.gvv-web.nl/alignmentMeasure.html

Systems Administration Review

- http://www.sans.org/reading-room/whitepapers/bestprac/system-administrator-security-practices-657
- http://www.sfisaca.org/download/gensecaudpgm.pdf

Application Review

- http://www.theiia.org/bookstore/downloads/freetomembers/0_1033.dl_gtag8.pdf
- http://resources.infosecinstitute.com/itac-application-controls/
- http://www.sans.org/reading-room/whitepapers/auditing/application-audit-process-guide-information-security-professionals-1534

Network Security Assessment

- http://www.sans.org/reading-room/whitepapers/auditing/base-security-assessment-methodology-1587
- http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

Business Continuity Review

- http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Business-Continuity-Management-Audit-Assurance-Program.aspx
- http://www.computerweekly.com/feature/Disaster-recovery-audit-maintenance-and-continuous-improvement
- http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/bsnss-cntnt-plnnng/index-eng.aspx

Data Integrity Review

- http://info.knowledgeleader.com/bid/161188/What-is-Data-Integrity-Risk
- http://www.ironmountain.com/Knowledge-Center/Reference-Library/View-by-Document-Type/White-Papers-Briefs/T/Top-10-Reasons-to-Audit-the-Integrity-of-Your-Data.aspx
- http://www.testingexcellence.com/what-is-data-and-database-integrity-testing/

Physical Security Review

- http://www.sans.org/reading-room/whitepapers/physical/implementing-robust-physical-security-1447
- http://www.securestate.com/Services/Profiling/Pages/Physical-Security-Assessment.aspx
- http://www.sans.edu/research/security-laboratory/article/281

Project Management and Change Management Review

- https://iaonline.theiia.org/auditing-it-project-management
- http://www.brighthubpm.com/monitoring-projects/32883-project-management-audit-process/
- https://www.bia.ca/articles/UndertakingaSuccessfulProjectAudit.htm