



RAS News Report

SUMMER 2008 NEWSLETTER

The CSA has issued Staff Notice 52-320 relating to the disclosure of expected changes in accounting policies regarding the January 1, 2011 changeover date. Once again, organizations are feeling the pressure to clearly disclose pertinent financial details while making sure plans to ensure a smooth conversion to IFRS are underway.

IFRS ALERT: Preparing for the Conversion Process

The Canadian Accounting Standards Board recently confirmed January 1, 2011 as the date public companies will need to disclose the details of their IFRS conversion plans. Outlined below is a summary of the IFRS disclosure requirements broken down by key dates:

2008 – For all interim and annual periods of the financial year ending December 31, 2008 (other than investment fund issuers)

Public enterprises converting to IFRS should disclose key elements and a timeline of its IFRS conversion plan no later than in its annual MD&A. Key elements of an issuer's plan may address the impact of IFRS on the following:

- Accounting policies, including choices among policies permitted under IFRS and implementation decisions such as whether certain changes will be applied on a retrospective or a prospective basis;
- Information technology and data systems; and
- Internal control over financial reporting.

2009 – For all interim and annual periods of the financial year ending December 31, 2009 (other than investment fund issuers)

In the interim MD&A, an update of progress on the company's IFRS changeover plan and any changes in the plan must be disclosed. The annual MD&A should also describe the major identified differences between the issuer's current accounting policies and those the issuer is required or expects to apply in preparing IFRS financial statements. Such differences include



CONTACT INFO

BDO Dunwoody LLP's Risk Advisory Services practice is a dedicated national risk practice. Our approach to risk management combines talent, experience and an exceptionally motivated team to provide you with innovative, cost-effective and value-added services. Business risks are mitigated; organizational goals are defined and achieved; operational performance is continuously assessed and improved.

For more information on the BDO Dunwoody LLP Risk Advisory Services group please contact us at www.bdo.ca/ras or contact any of our team members in the following regions:

Partner

Sam Khoury
Telephone: 416.369.6030
E-mail: skhoury@bdo.ca

Quebec Region

Michael Rodger
Telephone: 514.934.1122
E-mail: mrodger@bdo.ca

Central Region

Carlo Mariglia
Telephone: 416.369.3078
E-mail: cmariglia@bdo.ca

Western Region

Nitin Khare - nkhare@bdo.ca
Telephone: 604.443.4715
or 403.205.5767

any difference due to an expected change in accounting policy even though the issuer's existing policy under Canadian GAAP is permissible under IFRS.

2010 – For all interim and annual periods of the financial year ending December 31, 2010 (other than investment fund issuers)

One year prior to the implementation of IFRS, issuer's must disclose an updated discussion of changeover preparations currently underway in both its interim and annual MD&A discussions. Issuer's will need to prepare quantified information about the impact of IFRS on each line item presented in the financial statements for the interim and annual periods of the year preceding changeover.

Conversion to IFRS by investment fund issuers

An investment fund should discuss the changeover to IFRS for each fund or fund family in either the management report of fund performance (MRFP) or the notes to the financial statements. In the year before changeover, disclosure should include quantitative impact of the changeover to IFRS.

ALERT - National Instrument (NI) 52-109 Major Changes

On April 28, 2008, the CSA released the details of its proposed new approach for additional provisions relating to ICFR. If adopted, these amendments will take effect December 15, 2008. Important highlights from the CSA's proposed NI 52-109 Certification of Disclosure in an Issuers' Annual Interim Filings propose:

- To replace the current MI 52-109;
- No requirement for external auditor attestation; and
- A different set of requirements for Venture Issuers vs. Non-Venture Issuers.

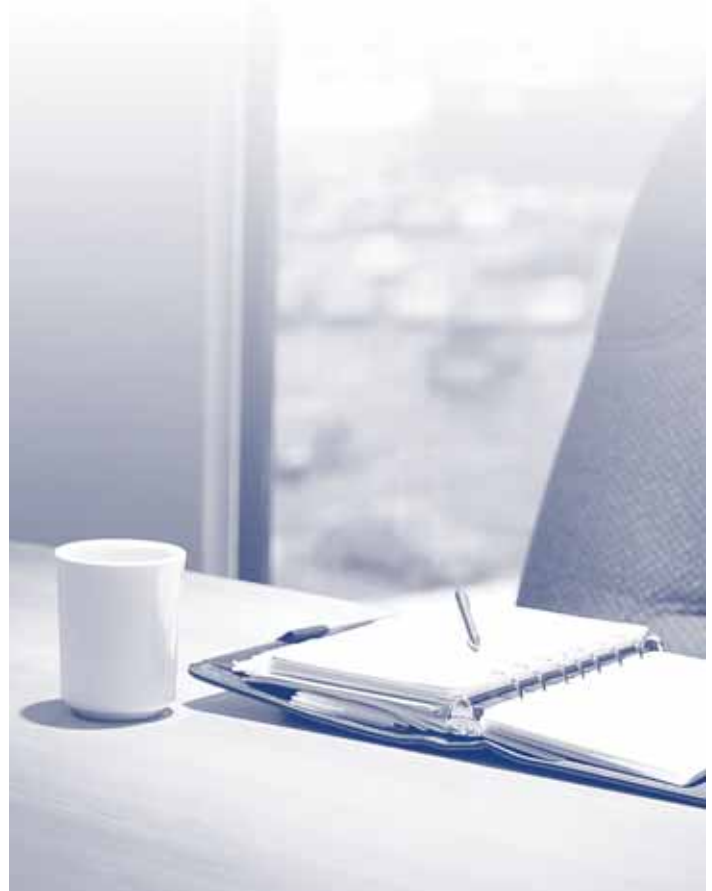
For further information regarding the CSA's proposed changes and how they affect publicly listed companies, please visit www.bdo.ca/ras.

MYPDR: Meeting Your Professional Development Requirements

BDO's series of professional development seminars aim to meet the professional development requirements set by your professional association. This latest session, "Employee Fraud — What You Don't Know CAN Hurt You", featured Sam Khoury, Partner of the Risk Advisory Services group, and took place on Friday May 30, 2008 at the Delta Markham hotel. Sam provided valuable information in regards to this challenging subject and touched upon the following:

- Internal control weaknesses attract fraud
- Preventative measures against fraud
- Best measures and prevention for dealing with fraud

The next installment in the MYPDR seminar series will take place on September 12, 2008. Space is limited due to an overwhelmingly positive response to our professional development seminars, so be sure to register early and reserve your place.



Fraud Prevention

Safeguarding your business

Fraud is an issue all businesses, big and small deal with at one point or another. It can range from minor employee theft like helping yourself to a stapler, to unproductive behaviour, to more extreme actions such as asset misappropriation, fraudulent financial reporting or even corruption. Whatever the case, fraudulent activities can have a serious impact on a company's bottom line.

In recent years, high-profile cases of corporate fraudulent activity have changed the way business is conducted. In light of major scandals such as Enron, Tyco International and WorldCom, many companies recognize that the losses which can be sustained due to fraud from both business and industry perspectives are enormous. The market value of a company can be severely compromised, its reputation ruined and in the case of the previously mentioned examples, entire enterprises can collapse altogether. These extreme incidences of corporate fraud have caused many organizations to take proactive steps to prevent and deter fraudulent activity from occurring within their organization.

Assessing the fraud risks inherent to a company is crucial to mitigating their occurrence. Harnessing the expertise and knowledge of trained professionals to help outline these risks can provide a unique advantage; no one knows your business better than you do and that knowledge, coupled with a niche providers understanding of risk management, can lead to the creation and implementation of controls that can significantly reduce the occurrence of fraud. Taking measures to ensure organizational security will lead to increased stakeholder faith and a positive public reputation.

Making the Right Moves

A sound, proactive and business-driven approach to fraud prevention is broken down into three categories: Prevention, detection and reaction. Risk management professionals identify key risks, rank these risks and work with client companies to establish a clear code of conduct to deter fraud and implement the necessary controls to achieve this. An example of a solid program will include the following:

Prevention

- Identifying and measuring fraud risks
- Setting the 'tone at the top'
- Developing a code of conduct
- Introducing regular employee education programs to communicate key messages
- Creating a positive work environment which will dissuade employees from committing acts of fraud
- Hiring, retaining and promoting ethical and honest employees

Detection

- Instituting a hotline
- Implementing and monitoring internal controls
- Partnering with an independent and reputable audit committee
- Hiring Certified Fraud Examiners and internal auditors

Reaction

- Implementing investigative protocols
- Setting a consistent disciplinary protocol

The Payoff

Oftentimes fraud is not detected until it's too late; once acts of fraud have occurred, companies are rarely able to recoup the stolen assets. Utilizing the expertise and knowledge of risk management professionals to identify risk factors and make provisions to protect vulnerable areas in the business will help to significantly reduce cases of fraud. Once this process is complete, it's critical for management to place a strong emphasis on implementing organization-wide policies and controls to protect the business and its stakeholders. Setting the 'tone at the top', regularly communicating the company's zero-tolerance stance on fraud and clearly defining the consequences when caught go a long way to deter employees from committing fraudulent acts.

In a perfect world preventative and deterrence-based measures would be enough to protect corporate fraud from occurring. Unfortunately, we do not live in a perfect world; therefore, organizations need to implement strong controls to constantly monitor potential risks for fraud and misconduct. Partnering with an independent audit committee and implementing controls based upon the organizations fraud risk assessment helps to uncover fraudulent activity and mitigate losses and damage done. Likewise, implementing a hotline can be a very effective tool in encouraging employees who are aware of shady dealings to come forward and disclose sensitive information in a safe, unthreatening manner. Providing staff with the opportunity to anonymously reveal serious information without fear of persecution when normal channels for reporting unethical behaviour (i.e. informing supervisors and human resources) are out of the question still provides employees with the opportunity to follow the company's code of conduct and do the right thing.

In the event that fraudulent activity is discovered it is imperative that management take a hard-line stance; explicitly condemning misconduct and clearly outlining the consequences of committing fraud is absolutely critical not just to the success of an anti-fraud program but to the viability of the organization. There can be no 'minor' instances of fraud; actions leading to the misappropriation of assets and fraudulent financial reporting must be taken seriously. Persons who intentionally seek to pillage their companies for their own personal gain must be dealt with appropriately. The financial costs are too high and the effects it can have on a company's reputation can be irreversible.

While some businesses are less susceptible to fraud, it is a problem that all must deal with. Having proactive measures in place to prevent fraud and mitigate loss help to maintain the financial viability of your business.