IT Questions (Taxation)

Chartered Professional Accountants of Canada, CPA Canada, CPA
are trademarks and/or certification marks of the Chartered Professional Accountants of Canada.
© 2019, Chartered Professional Accountants of Canada. All Rights Reserved.

Les désignations « Comptables professionnels agréés du Canada », « CPA Canada » et « CPA »
sont des marques de commerce ou de certification de Comptables professionnels agréés du Canada.
© 2019 Comptables professionnels agréés du Canada. Tous droits réservés.

IT QUESTIONS (TAXATION)

Sample Problem 1

Explain how the Canada Revenue Agency (CRA) is increasing its use of big data and partnerships to combat offshore tax evasion and aggressive tax avoidance schemes.

Sample Problem 2

What are some of the advantages and disadvantages of using of analytics to detect non-compliance in organizations such as the CRA?

Sample Problem 3

Does the CRA require a taxpayer's consent to use his or her information? What data sources can be used?

Sample Problem 4

What is the mandate of the Offshore Compliance Advisory Committee?

Sample Problem 5

What security measures does the CRA have in place to protect taxpayer data?

Solutions

Solution to Sample Problem 1

The CRA is increasing its use of big data as part of its efforts to combat offshore tax evasion and aggressive tax avoidance schemes. Some of the measures that have been taken include the following:

- setting up a committee (the Offshore Compliance Advisory Committee) to provide advice on administrative issues regarding offshore compliance; the committee has recommended:
  - extending data analysis efforts beyond high-net-worth individuals to other types of taxpayers
  - working with other countries to ensure data mining and analysis techniques become and remain among the most sophisticated in the world
  - developing metrics for assessing the success of those techniques
- exchanging international banking data through an information exchange program between treaty countries that will provide access to additional information to better identify potential tax avoidance schemes
- developing predictive analytics using machine learning to identify areas of non-compliance
- collaborating and sharing information with international and domestic partners including the Department of Justice, the RCMP, and the OECD

Solution to Sample Problem 2

Using technology and data analytics can transform compliance operations from a randomized, periodic process into an intelligence-led, risk-based operation. This transformation can result in significant gains in speed and efficiency.

One direct benefit of the introduction of technology and data analytics to monitor compliance is cost reduction. Patterns and abnormalities can be detected using data analytics in a cost-effective manner. What would have once taken a human several hours (or weeks) to review can now be vetted by a machine in a matter of minutes. The availability of low-cost data storage and analytical tools, combined with high-power computing, makes processing large amounts of data possible.

Another benefit is that tax authorities can allocate resources more effectively because they are able to better predict where non-compliance will arise. More precise targets result in fewer audits and a reduction of administration.

An additional benefit is the availability of large amounts of information. Data lakes in large organizations are used as data sources for tax authorities. The amount of financial

data relating to taxpayers is substantially larger than was previously available to the CRA.

However, there are also some drawbacks to introducing technology and data analytics to an organization. The greatest disadvantage to working with big data is the need to address data quality issues. Data scientists and analysts need to ensure that the information they are using is accurate and relevant, and in the proper format for analysis. This requirement slows the reporting process considerably, but if organizations do not address data quality issues, they may find that the insights generated by their analytics are worthless — or even harmful if acted upon.

While using data to predict non-compliance may reduce risk in some areas, storing big data, particularly sensitive data, can make the CRA a more attractive target for cyberattacks, thereby increasing the need for increased data security and protocol at all levels of the organization.

Solution to Sample Problem 3

The Analytics and Data Solutions Division (ADSD) of the CRA does not obtain consent from taxpayers. The information collected from taxpayers' income tax returns, applications for benefits and credits, and various other forms concerning programs administered by the CRA is housed in source systems.

When taxpayers provide this information to the CRA, they are aware that it will be used for the administration and enforcement of the CRA's programs and legislation, and consent is therefore implied. In addition, the Individual (T1) Income Tax Return and Schedules contain a statement that informs taxpayers that the information collected will be stored in Personal Information Bank (PIB) CRA PPU 005.

Solution to Sample Problem 4

The mandate of the Offshore Compliance Advisory Committee is to provide advice, input, and recommendations to the Minister of National Revenue (the Minister) and to the CRA on the CRA's administration, policies, procedures, and priorities for offshore compliance.

The scope includes both businesses and high-net-worth individuals, as well as their advisors. It does not include recommendations for specific legislative proposals; however, it may include broadly framed recommendations on relevant areas of legislation to be considered by the CRA for review, and perspectives on potential implications of legislative changes.

Solution to Sample Problem 5

The CRA has a multipronged approach to security.

All communications and transactions with the CRA are protected and are conducted on secure platforms. As phishing scams become more frequent, the CRA becomes more proactive in warning the public about fraudulent communications claiming to be from the CRA.

External services are protected by firewalls and intrusion prevention tools to detect and prevent unauthorized access to CRA systems and to block malware.

During online transactions, the CRA encrypts data as it is transmitted between a taxpayer's computer and the CRA's web servers. Controls in place to protect collected data from external threats include network and host security systems such as corporate firewalls, anti-virus software, intrusion detection and prevention measures, and identity and access management controls.

Network components such as servers and routers are stored in secured and locked rooms or cabinets, accessible only to authorized personnel.

CRA employees must use approved levels of encryption on all removable devices (such as USB storage media) and during the transmission of private information externally to authorized recipients.