I & IT Assurance

Solutions

SOLUTION MANUAL

CHAPTER ONE

Review Questions

1. Which system component is the most business critical and why?
The 5 system components are infrastructure, software, procedures, people and information. Even though information is often the result of computer processing, i.e., the end, it is the most important component of a system. Hardware and software are no doubt more complicated than information and usually more expensive. However, the type and extent of hardware and software needed depends on what information the system is intended to process and in turn produce.

2. How would you rank the system assurance criteria for a financial statement audit? For an internal audit?
The assurance criteria are completeness, authorization, accuracy, timeliness, occurrence and efficiency. Financial statement auditors are concerned about completeness, authorization, accuracy and occurrence equally. They are less concerned about timeliness; if timeliness affects the year end, it becomes a completeness issue. Financial statement auditors are not concerned about efficiency. Internal auditors are concerned about all criteria with efficiency the least concerning; this is because it is better to have reliable information that took a lot of effort to get than to have unreliable information that took only a few minutes to get.

3. Computing power doubles annually. How do you think this affects system assurance?
This allows organizations to collect, store and analyze more information. While that helps makes business more efficient and far reaching, it increases the risk of privacy intrusion, so the criterion affected is authorization in a potentially negative way. Authorization is also at greater risk as organizations increasingly empower their employees so employees have more direct access to systems and more tools at their disposal. The criteria that are favourably affected are accuracy and timeliness.

4. What are the criteria for assessing system criticality in a bank? A large retailer? A government?
The criteria for business criticality in a corporation addresses mainly profitability (including revenue and expenditure control) and customer service. These apply equally to most industries. On a finer scale, the riskier areas in a bank are credit and cash management. The riskier area in a retail company is supply chain management including inventory. The criteria for a government include safety, health, welfare, revenue and expenditure control. The criteria for a university would include education, faculty support, revenue and expenditure control.

I & IT Assurance

Solutions

5. What is the IT implication of International Financial Reporting Standard?
IFRS implementation will lead to changes in accounting systems depending on the industry and the extent of computerization in an organization. For example, IFRS does not permit LIFO.

6. How can IT auditors be proactive to help manage risks?
An internal auditor can make recommendations to control deficiencies to help improve controls. The internal audit department should adopt a systems development audit methodology to mirror the organization's systems development methodology in order to review systems development documentation as it is prepared to identify potential control deficiencies. The internal audit department should also establish a protocol with management to review draft policies and procedures to help ensure that there are adequate internal controls. External auditors' proactive roles include testing internal controls during the interim audit and bringing control deficiencies to management attention ASAP.

7. What do you see is the role of a computer audit specialist in a financial statement audit?
As the general population is more IT literate day by day, so are auditors. Today's auditors can understand and test some IT controls that, twenty years ago, required computer audit specialists. Meanwhile, IT is growing and becoming more sophisticated. Hence, there is still a need for IT audit specialists. A computer audit specialist should be used to assess infrastructure and software change controls as they tend to be more technical, for medium to large organizations.

8. Which of the current IT issues identified in the CICA survey do you think affect the financial statement audit more?

   A. *Data integrity directly affects the control assurance criteria of completeness, accuracy, authorization, accuracy and timeliness and there is crucial to the external auditors. Information management to prevent overload and ensure that the right information goes to the right manager is of less concern for non-financial information..*

   B. *Legislation, regulations and compliance – This is of high concern to the financial statement auditors because of the legal nature.*

   C. *New and emerging technologies – This is of concern to external auditors because if new technologies are deployed without proper testing and training, transactions may be processed incorrectly.*

   D. *Information skills and resources – This is of high concern to low to moderate concern to external auditors because inadequate knowledge can lead to incorrect transactions and inadequate staff can decrease segregation of duties.*

   E. *IT governance – This is of moderate concern to external auditors because governance forms the platform for internal controls. The concern is moderate because the controls actually exercised by senior management are less directly relevant to transaction processing.*

   F. *Outsourcing – This is of high concern to external auditors because it can affect their ability to test internal controls.*

G. *Public trust – This is of moderate concern to external auditors because the lack of public trust means systems are not reliable..*

H. *Management and operation of technology infrastructure – This is of high concern to external auditors because they affect infrastructure controls, including general controls.*

I. *Business continuity and pandemic awareness – This is of high concern to external auditors because of the going concern relevance.*

J. *Impact of the economy on information technology – This is of a moderate concern to external auditors. The concern stems from deteriorating segregation of duties potentially resulting from economic downturns.*

9. Which components of the CISA examination do you think are more relevant to the audit of financial statements?

The components are:

A. *Information systems audit process – This is directly relevant to external auditors because an audit that requires an external audit usually relies significantly on information systems.*

B. *IT governance - This is of moderate concern to external auditors because governance forms the platform for internal controls. The concern is moderate because the controls actually exercised by senior management are less directly relevant to transaction processing.*

C. *Systems and infrastructure life cycle – This is directly relevant because it is critical for management to management the life cycles to ensure systems continue to be reliable.*

D. *IT service delivery and support – This is highly relevant because unreliable service delivery and support will lead to incorrect transaction processing.*

E. *Protection of information assets – This is highly relevant to external auditors because inadequate information asset protection will lead to unauthorized or unsubstantiated transactions.*

F. *Business continuity and disaster recovery – This is relevant because of going concern.*

10. What kind of IT knowledge do you expect of the chief auditor of a large bank?

A large bank has extensive information systems so it is important for the chief auditor to be IT savvy on a wide scale and keep in touch with IT deployment in the bank. S/he has to be an IT generalist that is willing to learn from conferences, discussions with staff and meetings with IT executives. The chief auditor should be IT literate enough to have regular meetings with the chief information officer to assess IT risks at a corporate level.

I & IT Assurance

Solutions

CASE

1. What do you think are the causes of aging systems in the public sector?
   Governments have experienced funding constraints in recent years as a result of increasing public demand for services and decreasing tax revenues. This puts pressure on the IT budget. It can lead to a general attitude of keeping systems until they break, even if they are aging and require more and more patching. Patching (maintenance and fixing of source code) for functional reliability and efficiency, is risk and error prone in general.

2. Are the causes of aging systems applicable to the public sector also common to the private sector?
   These factors are also applicable to the private sector especially for companies with legacy systems that are not essentials. Companies that experience revenue contraction will have to cut expenses. Unlike governments, companies are more inclined to cut people instead of IT budget because efficient and reliable systems make them competitive.

3. How do the risks of government systems differ from private sector business systems?
   The risk factors of completeness, accuracy, authorization, timeliness, occurrence and efficiency apply to both the private and public sectors. Private sector organizations are more concerned about efficiency and timeliness than public sector organizations.

I & IT Assurance

Solutions

MULTIPLE CHOICE QUESTIONS

1. Which system component affects a system's importance the most?

A. Infrastructure

B. Information

C. Software

D. People

E. Procedures

2. Who is responsible for ensuring system reliability?

A. Management

B. Auditors

C. CIO

D. Chief risk officer

3. What should be CEO's main concern about the annual doubling of computing power?

A. Increasing spending

B. Impact on audit fee

C. Inappropriate use by employees

D. Opportunity and risk

4. What affects an IT strategy the most?

A. Annual doubling of computing power

B. Regulatory requirement

C. Business strategy

D. Systems development plan

5. Which type of system has benefited the most from fast growth in computing power?

A. Customer relationship management

B. ATM

C. Payroll

D. Local area network

6. Who should own the customer relationship management system in a major Canadian bank?

A. Chief financial officer

B. Chief executive officer

C. Head of personal banking

D. Chief information officer

I & IT Assurance

Solutions

7. Which system component is most critical to ensure system availability?

A. Information
B. Infrastructure
C. People
D. Software
E. Procedures

8. Which reliability concern is increased in cloud computing?

A. Completeness
B. Accuracy
C. Timeliness
D. Authorization
E. Efficiency

9. Which is the most relevant pair?

A. Quantum computing and big data
B. System owner and infrastructure
C. Privacy and accuracy
D. Peyton Manning and Roger Federer

10. Which position requires the most powerful system access?

A. Chief information officer
B. System owner
C. System administrator
D. Chief technology officer

I & IT Assurance

Solutions

CHAPTER TWO

1. How does automation affect segregation of duties?

Automation usually reduces the number of employees in a process. This means less segregation of duties. However, one might argue that some duties formerly carried out by people are now automated. Since computers don't lie or collude and seldom makes mistakes, even though there are fewer people left, segregation of duties has not suffered. Well, that is a misconception, because in thinking so, one has neglected the fact that computers are controlled by people and therefore people can use computers to collude. Thus, we are back to the initial assessment that automation reduces segregation of duties and that is generally the case.

2. What do you see are the responsibilities of a chief risk officer?

The chief risk officer should also develop and maintain the risk assessment and risk acceptance policy as well as supporting procedures to ensure consistent risk assessment in the organization. This executive should also provide a center of excellence in risk assessment. To maintain the risk registry, the chief risk officer has to coordinate periodic risk assessment and ensure that the findings are addressed with internal control improvements. There should be a corporate risk report broken down by business line and types of risks (e.g., IT, credit, market) submitted to senior management at least annually.

3. What are the risks of an ATM (banking) system?

Because of portability, the biggest risk faced by ATM users is the risk of unauthorized transactions. Unlike the risk of inaccuracy, incompleteness or untimeliness which can be prevented with system functions, the risk of unauthorized transactions can be magnified by users not safeguarding their cards and PINs properly.

4. Why are financial statement auditors content with moderate control risk?

Because the purpose of the audit of financial statements is to express an opinion on the fairness of the financial statements, rather than an opinion on controls, the level of control assurance sought by the external auditors is only moderate. This moderate level of assurance limits the extent of control testing conducted by external auditors. This is why external auditors typically use smaller sample sizes when testing controls compared to internal auditors. In fact, external auditors often rely on the work of internal auditors to further limit the extent of control testing conducted directly. Such reliance will help to keep the audit fee low.

When the external auditors can conclude that internal controls are moderately reliable, they can limit the scope of their substantive testing, i.e., the testing of transactions and account balances for substantiation. Substantive testing is generally more time consuming than internal control testing so it pays for the external auditors to seek a moderate level of internal control reliance. For *example, if the external auditors can conclude that internal controls over credit granting and sales processing are reliable, they can limit the scope of account confirmation and vouching to sales and payment details for substantiation.*

5. What is the relationship between sample size and risk?

   Both control testing and substantive testing involve sampling. The larger the sample size, the more likely that the sample result will reflect the state of population. Therefore, there is an inverse relationship between sample size and risk.

6. What level of control risk can external auditors tolerate when giving an opinion on a client's compliance with Sarbanes Oxley Act?

   Sarbanes Oxley Act requires a public company to file a report with Securities Exchange Commission that includes an external audit opinion on the adequacy of internal controls that support the financial statements. This opinion is in addition to the external audit opinion on financial statements. Because there is now an opinion on internal controls, the control risk tolerable to the external auditors is low.

7. What risks do consultants cause to an organization?

   IT consultants are commonly used to fill the gap between business requirements for IT support and available staff resources or expertise. Consultants are more fluid and expensive and therefore should be subject to rigorous justification to hire and close monitoring. They may not be as familiar with the organization's rules of dos and don'ts so may need more guidance than employees.

8. What computer characteristics can both increase and decrease risk?

   Computers are fast so the risks of untimeliness and inefficiency go down. However, computers can also make mistakes fast and magnify financial loss if programs are wrong. Computers are consistent so there are few mistakes; they don't get tired. But computers are inferior to people in making judgements. Computers can store a lot of data so the risk of incompleteness goes down, but at the same time, a vast quantity of data can be accessed within a short time so the risk of unauthorized access goes up.

9. Referring to the top ten IT issues in Chapter One, which ones increase financial statement risks?

A. *Data integrity directly affects the control assurance criteria of completeness, accuracy, authorization, accuracy and timeliness and there is crucial to the external auditors. Information management to prevent overload and ensure that the right information goes to the right manager is of less concern for non-financial information..*

B. Legislation, regulations and compliance – This does not directly affect the risk of misleading financial statements in term of financial balances. The risk has to do with adequate disclosure of contingent liability resulting from failure to comply with legislations and regulations.

<u>Solutions</u>

C. *New and emerging technologies – The use of new and emerging technologies may lead to incorrect transactions if the systems or tools have not been properly tested or if users are not properly trained.*

D. *Information skills and resources – The risk relevant to financial statements is inadequate knowledge, which can result in incorrect transactions.*

E. *IT governance – This is a risk for financial statements because governance forms the platform for internal controls. The concern is moderate because the controls actually exercised by senior management are less directly relevant to transaction processing.*

F. *Outsourcing – This is a significant risk for financial statements because it can affect their ability to test internal controls.*

G. *Public trust – This risk has to do with systems used by the public. The lack of public trust means systems are not reliable so that means financial statements are not reliable.*

H. *Management and operation of technology infrastructure – The financial statement risk implication is high because improper management can lead to weak infrastructure controls, including general controls.*

I. *Business continuity and pandemic awareness – This is irrelevant to the financial statements but relevant to the audit opinion because of the l going concern issue.*

J. Impact of the economy on information technology – This is a moderate risk. The concern stems from deteriorating segregation of duties potentially resulting from economic downturns.

10. As an internal auditor, you have been asked by the CIO to develop a risk registry. How should you respond to this request?

Risks are owned by management and they should document risks and mitigation plans. Auditors can review the risk documentation and provide comments. Auditors can also provide input as requested before documentation is finalized and can even participate in working sessions as an advisor; but auditors should not develop risk documentation.

Solutions

CASE

Audit Planning Memo
To: Audit Partner
From: Junior Auditor
Re: Automotive Parts Incorporated (API)

I have analyzed the information provided on API, a returning audit client, and the following is my analysis.

Automotive Parts Incorporated (API) is a distributor of automotive parts. Its customers include service shops and retailers. At the beginning of the current fiscal year, the company had implemented a fully electronic sales system that includes order entry, invoicing, receivables and collection. This system connects the head office with 5 branch offices with a wide area network (WAN), where each branch has an individual warehouse. This new electronic system will increase our overall audit risk because as a new system, our auditors have never been exposed to it and tested the strengths of the system controls and effectiveness. Therefore there is a high level of inherent risk for this audit. The transfer of information from previous systems to this new system will also have a high propensity for errors. This system will be one of the primary focuses of our audit because it can affect many important figures on the financial statements such as accounts receivable, sales and inventory. The audit will be designed around testing the controls that exist within the system as well as conducting several substantive tests in areas where controls are weak.
The following is my analysis of the issues that have been provided as well as my suggestions as to the audit approach to address the issues.

Issues Identified:
Issue 1: In API's organization, the information technology (IT) manager reports to the CFO. There is a computer operations supervisor at head office and one at each branch. They report to the IT manager. They are specialists in operating systems and networks. In addition, they have been thoroughly trained in the use of the application software packages purchased by API.

Inherent Risk: There is always an inherent associated with multiple points of entry into any system. Multiple points of entry increase the chance of fraud or error. However, inherent risk may also decrease given that those given access are properly trained. It also decreases because there may be an increased chance of detection of any system errors.

Detection Risk: This memo is prepared using the information provided by the CIO. However, based on the above information provided by the CIO, the direct user of this system is not the CIO but the computer operations supervisor at each branch and head office (See Appendix). Therefore, there is a risk that as auditors we are not provided with the complete image of this system.

Solutions

Control Risk: There is a computer operations supervisor at each location whom are all well trained in the use of the application software. This decreases control risk because these supervisors, through their continuous exposure to the system would be able to detect system errors more easily than other employees. They would also be able to correct system errors before the error expands. Therefore, these supervisors serve as an added layer of control against system errors that might lead to material misstatements of financial figures. The IT Manager would also serve as an oversight control to ensure that no changes are made without proper authorization.

Audit Approach:

Completeness: Assurance needs to obtained in regards to the information that we as auditors have been given by the CIO is complete. In addition to the information provided by the CIO, our audit team needs to approach each computer operations supervisor and the IT Manager for additional information and concerns they have about the system. Method used to obtain information can be through individualized interviews.

Authorization: Additional information should be obtained in regards to how these supervisors obtain their access to the system. Through interviews, we should also understand whether the supervisors have authorization to make changes to data on the system or to the system itself. If they do, how are they monitored to ensure that they do not make inappropriate changes? Also, their access should also be secure to ensure that no one else can access the information.

Existence: Whether these supervisors have actually been trained adequately in the usage of this software system should also be verified to ensure that this control actually exists. Auditors can observe the supervisors and ask detailed questions concerning the system during the interview process.

Issue 2: A service shop or small retailer customer that wants to establish an account would access API's web site to complete a credit application. Besides the standard information normally associated with a credit application, the applicant must provide a valid credit card number or bank account number that will be charged for all purchases. The customer must also supply an email address.

Inherent Risk: Electronic commerce in general increases inherent risk because third parties are responsible for data entry into the API's system. Customers are not data entry experts, therefore information provided in reference to name and email address may be incorrect or entered in an incorrect format. For example, the usage of "-" in the entry of phone numbers and usage of brackets are preferences that differ among different individuals. This can be linked directly to a higher detection risk for audit company if not properly controlled.

Solutions

Control Risk: The system requires that the customer provide a *valid* credit card number or bank account number, which suggests that the system picks up anomalies in those data fields immediately upon entry. This decreases control risk, as the system will guarantee that the account exists before any purchases can be made. Since this is a low control risk, it is one of the key controls that can be relied upon in the audit procedures.

Detection Risk: Detection risk may increase due to the inherent risk of having third party users of the system. For example, as auditors, we frequently use CAAT systems to run through the data provided by the company in order to detect anomalies in the data. If the formats of the entries are all different, then using the CAAT, we may have a long list of anomalies that were simply the result of the customer adding dashes or brackets in the phone numbers and not actual incorrect entries.

Audit Approach

Existence: One of the key assertions that we have to test for is existence of the customer provided information, given that mistakes can be made in data entry. However, as we have stated earlier the data field control can be relied upon. Therefore, the auditor should first test the controls by running a CAAT to enter various credit card numbers that do not exist into the computer system and ensure that the system does not accept these numbers. As a precaution, we may also want to take a sample of bank account numbers and verify with the bank that these accounts do exist.

Accuracy: To ensure that the data entered by the customer is accurate, a sample of the customers could be contacted and asked whether the information in the system is accurate. Banks can also be used as a external source to ensure bank account numbers match customer names.
Completeness: CAAT could be used to pick up customer profiles that have important fields missing or incomplete.

Issue 3: The applicant's credit status is verified electronically with a credit rating agency, and the API credit manager approves the applicant as a customer within two business days. Upon approval, the customer's system ID and password are sent by separate registered letters. A customer can use the ID to access API's order entry web site.

Inherent Risk: The inherent risk or any non-automated system is the risk of human error. On the other hand, the inherent risk of automated systems is that they lack human judgment. One system glitch may cause many customers to be approved even though they have lower credit rating before it is detected. However, the additional API credit manager approval is an added measure to mitigate this inherent risk. However, as stated previously, systems are not biased nor do they make mistakes. By having the API manager in the process, there is added inherent risk of biases, fraud and human error.

Control Risk: There are multiple control factors here. The applicant is not given access to the website online purchasing system until after their credit rating have been approved. This decreases collection risk for the client because customers are more likely to be trustworthy. This can be directly tied to our auditing of the accounts receivable on the financial statements. The number of bad debt expense for customers that purchase through the website might be considerably lower than previous years. With automated systems there are always an inherent risk that a malfunction may not be easily detected. In this case customers with bad credit rating may be accepted. However API added a human verification process by using a credit manager to approve of all customers before they are sent their passwords and system IDs. This means that system errors may be noticed more quickly and adjustments made. This decreases the control risk. The customer's ID and password are also sent through separate letters. This ensures if a letter gets intercepted or opened by another person, they would not have the complete information to access API's online website.

Detection Risk: One particular issue that may be problematic for auditors is that there may be difficulty in ascertaining whether the system functioned correctly when it was verifying the credit risk of a potential customer. Credit ratings for customers can change overtime. Therefore, if the credit rating agency does not keep a record of historical credit ratings, it may be difficult for auditors to conduct accuracy assurance testing to ensure the system rejected the appropriate customers.

Audit Approach:

Accuracy: The system automatically verifying with a credit agency is a key control that can be relied upon in our audit. Therefore control testing becomes imperative. The credit rating company should be contacted with a selection of customers to match their ratings and ensure accuracy. A potential weakness of this system is that it may not update consistently when there is a negative change in the credit rating of a customer. This might mean that collection risk may still be an issue for the company.

Authorization: To test the control of the credit manager having to approve all new clients, a sample of recently approved clients should be selected and the approval of the credit manager should be verified. Another authorization issue is the dual mailing of the ID and password. This control is not a key control as it is subject to much risk. Both letters can be mailed to the same wrong address. They could both be intercepted. Therefore, more details as to how this dual mailing process would actually help maintain confidentiality and ensuring that no unauthorized person obtains the ID and password would have to be known. A suggestion could be made to management to send ID electronically through email. When customer obtains ID, they can enter the website whereby they provide the ID plus additional personalize information that the system could match up to customer profile and then the password will be sent to the customer.

Issue 4: Using the ID and password, a customer can look up product availability at any of API's five warehouses and place an order.

Inherent Risk: There is inherent risk in fraud from identity theft as unauthorized individuals might steal customer's information and misuse their accounts. Moreover, customers will expect the information on the product availability at the warehouses to be both accurate and timely. Inherent risk arises as the information might not be accurate and customers might end up ordering products with no availability, thus, creating an error. This is evident through a later issue where warehouses have to sometimes fulfill orders for items that have been ordered from another warehouse. This particular risk is more of an important issue from internal auditors as it has a direct link to efficiency and transportation costs for the company. As external auditors, our concerns would be whether these internal transfers are properly accounted for as shipping costs. Another issue is the inventory count as products can be easily double counted if they are shifted between the warehouses. The transfer of inventory between warehouses effectively demonstrates that the system is not timely and consistently accurate on product availability. Therefore, this inventory count on the system itself cannot be relied upon by our auditors.

Control Risk: The ID and password only provide sufficient control to ensure proper authorization and low control risk in frauds if they have a high degree of security and cannot be easily guessed or attained by a third party. However, assuming that the password and ID is secure and customers have no access to the system aside from making orders, the security aspect of this internal control should be relied upon as it has a significantly low control risk, but should be tested to ensure reliability.

Audit Approach

Authorization: The ID and password system can be tested by sampling customers with positive confirmation by phone to ensure these orders have been properly authorized by these customers.

Accuracy: Accuracy pertains to the amount of inventory in the warehouse to the numbers entered into the system by the warehouse staff. This can be tested by sampling the warehouse to compare the amount inventory available and the number in the system. This assertion should be given greater caution as it is prone to human error in the inventory count.

Timeliness: Timeliness pertains to the number entered by the warehouse staff and the number that appears on the product availability online. This can be tested by sampling the numbers on the website and the numbers on the internal inventory system. This can effectively test whether the internal inventory system data are fed timely to the website's product availability counts to ensure timeliness of the data online.

Existence: For the inventory count, existence will be a major concern as the system does not update automatically. At the cut-off period year-end, it will become empirical to identify the exact amount of inventory in the five warehouses. The system as previously stated cannot be trusted to have the accurate amount. Auditors would have to use inspection of the five warehouses as well as look into shipping papers in order to determine the exact amount of inventory.

Solutions

Issue 5: For small customers, when a customer finishes placing an order, API's system connects to the previously identified bank or credit card network that will authorize the transfer of funds, to ensure that sufficient credit or cash on deposit is available. API records this code on an electronic order confirmation that has a unique order number assigned sequentially by API's computer to every order placed within its system. The order confirmation and invoice are emailed to the customer. Large customers are invoiced and they will pay based on the invoices.

Inherent Risk: For small customer, an inherent risk to the process is the accuracy of the e-mail provided by the customer. If the e-mail is not correct, the billing process could not be completed and the customer could not be notified for their payment. In addition, there is inherent risk in billing incorrect amount or incorrect account and possibility of billing to accounts with insufficient credit. For large customer, similar risk exist as the billing address and amount or account billed may be incorrect and the account might not have sufficient credit. Lastly, there is the inherent risk that some orders might not be billed.

Control Risk: There are controls in place to ensure the amount billed and the accounts billed to be correct and has credit available for the billed amount. Moreover, the billing information is controlled with sufficient system edit in place to ensure the validity of the information provided by customer upon their registration. Our recommendation would be to rely upon these controls as the control risk is low. However, as key controls they would need to be tested extensively to ensure that the system is functioning properly when it seeks to determine whether the client has enough credit and when it sends out order confirmations to clients.

Audit Approach

Existence and Accuracy: The amounts billed and accounts billed can be tested by sampling the invoices sent out to the customers and comparing to the original order received to ensure that the proper amount and account have been billed.

Completeness: To ensure all orders received have been billed, the billing record and order record could be compared to ensure that all orders have been billed with an invoice. Also, using a CAAT system, the auditors should test for whether there are duplicate order confirmation numbers and whether there are any missing sequence numbers.

Issue 6: For small customers, funds are electronically transferred to API's bank account one week after an order has been filled, to allow customers time to inspect goods before paying for them. The customers have the right to cancel the transfer of funds by informing the bank if the goods are not satisfactory.

Inherent Risk: There is inherent risk in the transfer of fund, whether or not the proper amount have been received from the proper account. Moreover, there is inherent risk in the cancel of the order, as customers might miss the 7 days deadline to cancel the transfer of fund. There are also inherent risks with allowing customers time to cancel the purchase of goods after the goods have already been shipped. The revenue recognition policy of

API should be observed to ensure that they do not recognize revenue prematurely as the risk is high that the customer may not accept the goods. Also, cut-off becomes an issue as the inventory goods would have left the warehouse but are not yet effectively sold to the customer. This risk will lead to an increase in detection risk as it can be difficult to determine which customers will keep the products and which will not. Also, if customers are widespread it becomes difficult to substantively test for the amount of inventory not currently in the warehouses.

Control Risk: There is an automatic system in place to transfer the amounts electronically. This greatly reduces the chance of human error and should be relied upon. However, it should be tested to ensure the system is reliable. In the case of a canceled transaction, fund would still be transferred if customers did not notify their banks. Thus, this should be tested in detail to ensure that there is no additional funds received for cancelled orders.

Audit Approach:

Accuracy and Completeness: The automatic system can be tested for its accuracy and completeness by a bank reconciliation. In addition, the bank reconciliation can test whether additional funds had been received for the cancelled orders.

Issue 7: During the day, the branch system processes transactions in "memo mode" only. "Memo mode" means that the branch's own inventory data base is updated instantly but that the transactions are not yet processed or transferred to the master files in head office. Orders are updated to the corporate system overnight.

Inherent Risk: the automation of updates will decrease inherent risk as it eliminates the possibility of human error when updating the database. In addition updates from the local branch to the corporate system occur every night. This systematic update of the files will decrease inherent risk as it is much easier to find errors between the branch database and corporate database due to systematic update. On the other hand inherent risk increases because of the timing of the updates of the master files. Since master files are not updated immediately in memo mode, there is an increased inherent risk of error between the timing of the updates. In between the updates of the local branch data base and the corporate master file, there is room for users to change information in the local database before it is updated. In addition, the corporate system will not be updated throughout the day, this may lead to customers ordering inventory that has already been sold to other customers.

Detection Risk: having electronic paper trail will allow CAATs to operate efficiently and detect errors easily thereby decreasing detection risk. However, having a completely electronic paper trail will increase detection risk as well. Without a physical paper trail, some transactions may be undetected or easily covered up if it is not recorded electronically.

Solutions

Control Risk: automation of the updates of the local data base to the corporate master file reduces the control risk associated with this process. It limits access to the files to prevent potential fraud or misstatement by a third party as the system will automatically update itself without. However, the lack of authorization to approve of updates of the local inventory data base to the corporate master file increases control risk because no one checks over the files that are sent to the corporate system to make sure they are correct.

Assertions

Completeness: One of the key assertions is to test for completeness. Auditors should perform a test of detailed balances by comparing the sub-ledger to the general ledger to make sure the local database matches master file. In addition, a sample of the update file can be taken to check if all transactions from the branch database goes to the corporate master file.

Accuracy: to ensure the master file is accurate, a sample of various local data bases should be taken and compared to the master file to ensure the balance from the local data base matches that of the master file.

Issue 8: Each evening, the network supervisor at each branch performs an end-of-day routine that identifies every transaction processed that day. The routine writes these transactions to an overnight transfer file. At the end of the daily update, head office sends a complete copy of all updated data files so that each branch has current customer, item number, order information and inventory levels at all branches.

Inherent Risk: by having the network supervisor identify each and every transaction processed that day, there is a high probability of human error and fraud which increases the inherent risk. For example, the network supervisor can record a transaction incorrectly, fail to include some transactions, double count transactions, or add false transactions. In addition, the quantity of the processes from the routine to the transfer to the head office and the update back to the local office increases the inherent risk as it allows for more room for misstatement at each stage of the process.

Detection Risk: the updated file sent to all branches from the head offices creates a paper trail that is frequently updated. This will decrease the detection risk as it gives auditors a paper trail to trace transactions that occur at each branch and compare it to the corporate master file.

Control Risk: by having only one person compile the report on every transaction processed in the day there is a lack of supervision and authorization over the routines. There is a lack of segregation of duties as well since this allows one person to include or not include transactions of his choosing in the report without supervision. As a result, the controls in place are not adequate and will increase control risk

I & IT Assurance

Solutions

Assertions

Existence: existence can be tested by taking a sample of the report on the end of the day routine at various branches and compare it with the master file at the head office. This can verify that the transactions have been recorded at both the branch database and corporate master file. In addition, sample transactions from the report on end of day routine can be taken and verified with branch managers or clients to ensure transactions have occurred.

Completeness: Completeness can be tested by performing a test of detailed balances to make sure the inventory levels and order information match at both the branch database and head office master file. CAATs can also be used to sure all transactions from the branch database go to the corporate master file as well.

Issue 9: Three types of packing slips are printed every morning from the updated file. For example, the three types of packing slips printed at Branch A would be:

- *Sales to Branch A's pre-assigned customers filled by Branch A's warehouse*
- *Sales to other branches' pre-assigned customers filled by Branch A's warehouse,*
- *Sales to Branch A's pre-assigned customers filled by other warehouses.*

Inherent Risk: the three types of packing slips increase the inherent risk as there is a human error aspect. The possibility of mixing up the packing slips and sending packages to the wrong customers or losing packing slips after they have been printed out are all human errors that may occur in the warehouse after printing the packing slips. In addition, printing the packing slips in the morning does not allow for updates to orders made last minute or updates to orders that are to be shipped later but have the printing slip already printed out. As a result, this will increase inherent risk

Detection Risk: the three types of printing slips provide a paper trail that can easily be used by auditors to detect. However, the constant movement of inventory (e.g. sending inventory from warehouse A to warehouse B customer, and vice versa) has the potential to create mass confusion between each branch’s warehouse and matching the inventory to a particular sale. There is the possibility of double counting inventory already assigned to another branch customer or not counting inventory that are in traffic from one warehouse to another. As a result it will increase detection risk because it makes it very difficult to keep track of inventory between the branches.

Control Risk: there is a lack of control as no one checks over the packing slips when they are printed or checks the proper packing slip is assigned to its package. This can create errors with sales as no one verifies accuracy of the packing slips and allow employees to steal inventory as employees can discard packing slips and steal inventory that was to be shipped from the packing slips. The lack of authorization and proper sign off for the packing slips increases control risk.

I & IT Assurance

Solutions

Assertions

Accuracy: a sample of shipped packages can be verified with packing slip to ensure accuracy of shipment. In addition, printed packing slips can be compared with the sales orders on database to ensure sales orders are correct and match the system database

Existence: physically sampling packages to ensure they are properly classified and going to the correct customers can be used to ensure existence. In addition, contact with the customers can be used to verify that the orders were received, all parts from the order were received and which warehouse the order was sent from.

Issue 10: Using hand-held computers, the shipping clerks scan the bar-coded shelf labels and enter the quantity they ship using the numeric keys.

Inherent risk: There is a high inherent risk in this manual process of scanning each item been shipped as there is always a high risk of human errors associated with manual data entry. First of all, as the client's main business is inventory, keeping track of inventory is always a high-risk area. This is especially the case for API as their inventory is automotive parts which can come in all sizes and value. A small part can be worth a significant value. Thus, having to scan each part that has been shipped, there is a risk of something not been scanned properly, missed or scanned twice. This can be linked directly to a higher detection risk for Audit Company if not properly controlled. For example, to test if all items on a customer's order are correctly shipped, audits might do a CAAT run to pick up any items that are on the customer's order but did not show up on the list of scanned items by the shipping clerk. This list will only show items that were supposed to be shipped, but not correctly scanned. It will not however show any incorrectly shipped items that were not on the customer's order list and not scanned correctly by the shipping clerk. Also, the quantity of the shipment also needs to be entered manually. This inherent the risk of human error as quantities can be entered incorrectly.

Control Risk: This process of keeping track of shipments requires the shipping clerk to scan each item with the hand held computer and enter in the shipment quantity using the numeric keys. This means, given all shipment is scanned correctly, any inventory that does not belong to the shipment should be alerted to the shipping clerk through the hand held computer. However, there is no control to ensure all shipment is scanned correctly and no item is missed. Because if an item is missed, there is no other control to alert the shipping clerk that an item is not scanned or does not belong to the shipment. In addition, there is no control to ensure that the quantity for shipment is correctly entered using the numerical keys. This increases control risk, as the process cannot guarantee the accuracy and completeness of the shipment orders. Since this is a high control risk, it is one of the key controls that cannot be relied upon in the audit procedures.

I & IT Assurance

Solutions

Audit Approach:

Existence: One of the key assertions that we have to test for is existence of each shipment, given that mistakes can be made in data entry of the quantities shipped and scanning. Because we cannot rely on control, there will be relatively more substantive testing to be done. To test if shipments exist, we can take a sample of customers and send out positive confirmation letters to verify the quantity and value of their order and whether they have been correctly shipped. We can also reconcile the electronic shipping record to the general ledger. We can also do analytical procedures by trace inventory movement with CATT and predicting the level of inventory that should be shipped.
Accuracy: We will need to reconcile the list of items prepared for shipment to the electronic recorded of items that is been scanned and shipped. To ensure that the shipment items scanned and entered by the shipping clerk is accurate, we can also take a sample of customers and send out positive confirmation letters to verify the quantity and value of their order and whether they have been correctly shipped. A random sample can also be taken from the orders of items that are going to be shipped and test if they have been scanned and recorded correctly by the shipping clerk.

Completeness: We need to reconcile year-end inventory and see if the quantity of shipment matches the associated decrease in inventory in addition to the testing we have done above.

MC Questions

1. . Which of the following is most likely to cause privacy breach?
   A. Enterprise resource planning system
   B. Batch systems
   C. Customer relationship management system
   D. Managing and retaining data

2. Which risk is best mitigated by a database management system?
   A. Occurrence
   B. Privacy
   C. Integrity
   D. Authorization

3. Which is the right formula for residual risk?

a) Inherent risk x detection risk
b) Inherent risk x audit risk
c) Inherent risk x control risk
d) Control risk x detection risk
e) Control risk – audit risk

I & IT Assurance

Solutions

4. Which risk increases the most with virtualization?

a) Program errors
b) Data entry errors
c) Improper data access
d) Data redundancy
e) Data loss

5. What will happen if two bits are altered during data communication, i.e., a 0 becoming a 1 and vice versa?

a) The transaction will be incorrectly recorded.
b) Confidentiality will be breached.
c) The network will be jammed.
d) The message will be intact because of the offsetting errors.

6. "Passwords may be easily broken." This is a(n):

a) inherent risk.
b) weakness.
c) control risk.
d) conclusion.

7. "With the current infrastructure, we stand to lose $2 million of business a year as a result of system breakdown." This is a(n):

a) exposure.
b) conclusion.
c) residual risk.
d) accepted risk.

8. A manager creates an Excel spreadsheet for his staff members to enter hours worked. The spreadsheet is then imported to the payroll system. What is the greatest risk?

a) Staff getting paid for hours not worked.
b) Employees may see the numbers of hours worked by others.
c) Staff do not enter hours worked.
d) The spreadsheet is not signed by employees.
e) The spreadsheet cannot be printed properly.

9. Outsourcing increases

a) audit risk.
b) control risk.
c) inherent risk.
d) detection risk.

10. When the shareholders' auditors find that internal controls are less reliable than expected, they should

a) assess control risk as lower.
b) increase materiality.
c) reduce the planned detection risk.

d) assess inherent risk as higher.

CHAPTER THREE

1. What is the relationship between software change controls and systems development controls?

   Software change controls apply to all software changes regardless of the size of a change. A system development project includes software changes. Some systems development controls depend on software change controls. For example, the validity of testing depends on the rigour in controlling software versions to ensure that tested programs are not changed without going through further testing.

2. Who should approve the corporate disaster recovery plan?

   Even though disaster recovery requires a lot of IT resources, IT exists to enable business so the DRP should be approved by management and the CIO. The corporate DRP applies to the entire organization so it should be approved by the organization's head, i.e., the CEO.

3. How often should a disaster recovery plan be tested?

   Many application supported by a DRP are business applications that have a maximum financial cycle of one year. Therefore, a DRP should be validated and tested at least annually.

4. Who should the CIO report to?

   The IT department is a common service function in an organization. To ensure that IT services are equitably distributed among other functions, the CIO should report to a senior corporate person. The most impartial senior corporate person is either the CEO or the COO. Ideally, the CIO should report to the CEO to show to the rest of the organization that the IT department is a highly valued service that should be used effectively.

5. What is the best approach to moving software to the production library?

   A common question is whether the source code only or the object code only should be moved between libraries or both? Let's explore the pros and cons of these three options.

   Option 1: Moving Source Code Only – This means that the source code has to be recompiled in the destination library because in order for the programs to be used for testing, they have to operate in a computer (machine) language.

   Option 2: Moving the Object Code Only – There is no recompilation needed.

   Option 3: Moving Both Object Code and Source Code – There is no recompilation needed.

Solutions

On surface, option 1 seems to be the least desirable.

Even though source code, if everything goes well, is not needed in the common development library as well as the SIT and UAT libraries, it is needed in the production library. This is because when a programmer begins working on a changed request, s/he needs the current source code, which should reside in the production library. The production library consists of programs that have been fully signed off and are working. This is the official version of the programs. Therefore, to maintain continuity and ensure completeness of transferring programs at each stage, source code should be moved between libraries throughout the cycle. Now option 2 does not look attractive. Further, when testing reveals a program bug, the software change management system will need the associated source code to tell the change control coordinator which source programs have to be fixed. So it is important to have source code in all libraries.

Option 3 moves the source code and object code between libraries. This introduces the risk of source code not compatible with object code because the wrong versions were moved. For example, the change control coordinator may have moved version 3 of object code but version 2 of source code. Moving is prone to losing things.

Under option 1, although only the source code is moved between libraries, object code can be created in each library by compiling from the source code. This ensures that object code is compatible with the source code. Option 1 seems to be the most desirable method to ensure synchronization between source code and object code. However, one would argue that if the wrong version of source code is moved, the compiled object code will be wrong. Well, let's adopt another option, option 4, which is the safest.

Option 4 – Move the source code and the object code to the next library. Once moved, recompile the source code and compared the compiled object code with the moved object code. This will make sure the correct versions of source code and object code have been moved.

6. What is the difference between an environment and a library?
   An environment is the hardware that holds a library. A library is a collection of programs at a certain stage of development or in operation. For example, there are programmer library, development library, test library etc. There are also programming environment, development environment, test environment etc.

7. What does an auditor see in an organization chart?
   An org chart defines who reports to whom and what the job titles are. These two pieces of information allows an auditor to assess segregation of duties.

8. What is the drawback of parity check?
   It does not detect offsetting errors. For example, if a 1 bit becomes a 0 and vice

versa, parity check will not detect these 2 errors will lead to a wrong information being transmitted.

9. How often should a bank back up its transaction files and why?

   Banking is a highly online and time sensitive business. There is often no paper trail and also a bank cannot afford lose a transaction as an individual transaction could be huge in amount. It is critical for a bank to back up its transactions frequently throughout the day. In fact, a bank should use redundant servers to record every transaction at least twice in distant locations.

10. What kind of system is the grandparent-parent-child backup approach used for?

    Grandparent-parent-child backup method requires keeping at least 3 generations of a master file. This is more suitable for batch applications where the master files are updated daily. It is not suitable for online systems where the master files are updated continuously, because in this case, 3 generations of a master file may mean, at the extreme, only the updates by 3 transactions. That would be inadequate.

CASE – Progressive Realtor

To: President and Manager of the Information Services Division
From: IT Audit Advisor
RE: Control of activities in the Information Technology Division

After performing a thorough analysis of the activities in the Information Technology Division at Progressive Realtors Ltd (PRL), I have noted a number of weaknesses in the department's internal controls:

1. Organization of Controls

I would like to start my analysis with the company's organization of controls. It is important to ensure that information technology practices are consistent throughout the organization. Based on my review of PRL's activities in the Information Technology Division, I have several concerns:

(1) I & IT Strategy

The first issue, with regards to organization controls, that must be addressed is the alignment of the company's IT strategy with its business strategy. As I'm sure you're aware, Mr. Chow operates independently of the rest of the organization with minimal input from other managers. It is therefore important to review whether the IT department's functional strategy is congruent with that of PRL's overall business strategy. The implementation of a congruent IT strategy should include a description of the importance of IT and the organization's dependence on. The strategy should include how the development of the IT function will foster growth within the organization and what specific projects and methods will be used to facilitate growth. Due to the fact that IT encompasses 15% of the company's total expenses, a proper approach to managing the investment and operations of this function would be important. The investments may need to be handled by a separate individual or a specific project-oriented budget may need to be prepared in order to ensure that investments are sound.

(2) IT Governance

IT governance controls help to ensure accountability. The same parties accountable for corporate governance should be accountable for IT governance. This means that Billy Chow should have the support of other executives in carrying out the company's IT governance framework. If necessary, an IT steering committee could be implemented in order to set the IT strategy and further approve major IT projects. Furthermore, a defined organizational reporting relationship should be established between Mr. Chow and perhaps you, the president of the organization, in order to ensure that information is transferred on a timely basis. This will be an effective control as it will not undermine the resources of the IT department and Mr. Chow's decision making abilities. By implementing a clear cut IT strategy, performance indicators and drivers of the IT department's performance can be established and can be better communicated to the executives of the organization. Functionality mapping and developing clear goals for each sector will ensure a proper consistency between PRL's operations and its IT strategy. In addition, it will aid with assessing the gaps between the operations of the IT department and those of the rest of the organization.

(3) Staff Development Controls

Staff development controls and procedures need to be established in order to ensure that PRL's Information Services Department continues to only employ only the best IT professionals. This could include hiring practices that clearly identify the specific skills and attributes that successful candidates should have. I would also recommend further training in order to ensure that the translation of data to an auditable format is accomplished.

(4) IT Budget Certification

Certification that the budget is adequately being utilized for IT procedures should also be a concern for the organization. Such procedures could involve the execution of budget review practices and better supervision of the IT function.

2. Segregation of Duties

Ensuring proper internal and external segregation of the IT function can help to establish proper accountability standards within a firm. As it stands, I have a few concerns with the segregation of duties at PRL:

(1) Segregating IT from Other Functions

First of all, the organization effectively separates the IT function from other corporate functions. More specifically, as I observed, Mr. Chow's team of workers primarily focuses on the programming, testing and maintenance of a number of information systems.

(2) Segregation of IT Function

While the IT function is satisfactorily segregated from other corporate functions, there is little segregation of duties within the IT function itself. There should be separation of systems development and systems operations. This means that the department's programmers and analysts should not be collaborating with system administrators when they are unable to interpret instructions or are on break. This area should be adequately staffed. Furthermore, the programmers/analysts should not be working with TREB and ASP customers online to troubleshoot any problems that arise since this is an area of operations not development. The separation of these functions would mitigate risks of programmers implementing programs without approval, changing business information, and changing system functions.

3. Software Change Controls

Given that PRL has recently completed developing and refining its computer-based management information system and that internal company operations such as accounting and billing are supported by in-house developed systems, the company must have adequate system change controls in place.

(1) System Change Control Policy and Procedures

As I've already mentioned, it is my understanding that there is very little control exercised over the Information Services Division by other parties within the company. As such, any change control policies have been developed by the Information Services Division rather than the organization itself. Given the extensive implications that in-house developed systems have on functions such as accounting and billing, it is crucial for the organization to take a more active role in defining change management policies, particularly with regards to the thresholds for approving changes. A change control board, consisting of IT management and cross-section managers, will also be beneficial as it will create more pressure for the development of systems that provide data that can be analyzed using standard management information retrieval tools.

(2) System Change Tracking

Unfortunately, during my review of the activities of the Information Services Division, I did not come across any systems that are in place that adequately document and communicate system changes to management and the rest of the organization. It is crucial for the company to have change management systems in place, for both planned and emergency changes, that document changes, create audit trails, and send an automated notice to management. This will help PRL ensure that all changes are properly documented, tested, and approved and that all key managers are aware of any updates made to the information systems that they are currently using in their functions.

(3) Code Comparison

Solutions

Given that a complete and detailed audit trail is provided by means of extensive transaction code and related to the batches of original vouchers that are stored on optical disks, it is important for PRL to compare current source code for all internally developed systems to the backup or yesterday's source code. Changes should then be reconciled with the approval audit trail. This will ensure that the automated audit trail will clearly show the impact of system changes on transaction information. PRL's current system change control policies do not require such reconciliations and therefore do not provide internal and external auditors with the information they need to evaluate the effectiveness of the company's internal controls.

4. Access Controls

It is important for organizations to secure access to computing environments, specific systems, and important functions. Based on my observations, the company must strengthen its access controls in the following areas:

(1) Information Access Controls

First of all, in terms of information access controls, PRL does not have any processes in place that assess the sensitivity of information in order to link this information to specific security tools. As it stands, a substantial amount of sensitive information, including salesmen's commission statements, payroll registers, and customer mortgage statements, are provided to all major departments of PRL without consideration as to whether access to this information should be limited in order to reduce the risk of this information being manipulated or misused. There are also no security standards in place that address privacy concerns associated with the wide distribution of this information. PRL can therefore not address the concern as to whether the information that it distributes has been handled appropriately and with confidentiality. In order to preserve the integrity of its sensitive information, the organization must first define what information and reports each department needs in order to perform their functions. Next, the organization must have a system in place that identifies and tracks all of the information and reports that each recipient in a department receives. This will allow PRL to trace any changes made to this information to a specific department or recipient and will ensure that access to sensitive information is limited to individuals who can specifically be held accountable for the security and use of this information.

Secondly, the company does not have procedures in place to prevent the insertion of "non-essential" data to files. In addition, a user department clerk can add and change data within a file without hard copy documentation. This gives rise to considerable concerns over the authenticity and reliability of information in PRL's data files. In order to remedy such weaknesses, the organization must have a repository of information owners which contains the names and titles of all individuals that make additions or changes to information in data files. The company must also maintain hard copy documentation of all major changes made to data files. Once again, I would also like to stress the importance of having user authentication systems in place such as password controls to ensure that only specified individuals are capable of accessing and changing data files.

(2) Physical Access Controls

Solutions

Currently, the organization does not have sufficient access controls in place to limit access to important functions. For example, one of the organization's most important functions (the mortgage system) can be accessed from any one of the firm's 300 workstations. This creates an opportunity for any user to access, change, or delete any information in PRL's key function systems.

The organization must have procedures in place to grant and disable access to important systems and information stored in these systems (e.g. user authentication through password controls) and must keep detailed access logs in order to better identify and investigate any unauthorized access. The organization may also want to consider physical access controls such as having only a limited number of workstations that can access important functions. These data centres should be separate from the other workstations and the use of these data centres should be monitored and limited to only certain individuals.

(3) General Access Controls

Aside from the specific access controls mentioned above, there are also a number of general access controls that the organization must have in place. Most notably, because the company uses a wide area network that is accessible from each of the 10 branches in Canada, automated controls such as firewalls, intrusion detection systems, and encryption software must be in place. PRL must also have a system in place that identifies and grants access to representatives of each branch to share information systems and data files. Intrusion prevention and detection as well as privacy are of considerable concern as PRL must have sufficient security standards in place to ensure that any information shared amongst its 10 branches will be used appropriately.

5. Systems Development and Acquisition Controls

I am sure that you are aware that systems development methodology is critical for effectively initiating and approving IT projects, I do however have some concerns about the systems development methodology currently used by PRL:

(1) Senior Management Involvement

A major weakness in the development of information technology systems at PRL is the lack of senior management involvement in the development process. This lack of oversight by senior management and reluctance to become involved in information technology development is a substantial weakness because it leads to a development process void of important senior management feedback.

Improving the systems development process requires the joint efforts of senior management and the manager of the Information Services Division, Billy Chow. This joint effort would create synergy in the development process as Mr. Chow provides an expert development perspective while management may offer a more high level organizational perspective. This suggested control would not only improve the development process but also mitigate the risk of development failure due to having only a single source of input, which is currently only Mr. Chow.

Solutions

In order to further mitigate the risks of systems development, management should create and enforce a comprehensive process for the development of projects in the information technology division. This process should include criteria that new projects must meet in order to receive approval, and a number of senior management signoffs at important milestones in the project's life. The process for systems development approval should be carefully designed to balance out two very important aspects: 1) to involve management in the development process and 2) to empower Mr. Chow to continue his highly productive work. This can be achieved through a process which allows Mr. Chow to receive quick approval in order to avoid slowing down his progress in development.

(2) Extent of Documentation

Another weakness in the systems development process is the lack of documentation. Documentation allows other employees and auditors to gain a better understanding of the development process and the results of final products. This mitigates the risk of having a small group of people lead the development of an important project. While producing the documentation may slow down the development process, it is vital to reducing risk and therefore should be done as part of the development process.

6. Disaster Prevention Controls

PRL should take steps to protect its information technology systems against general threats of disaster which any organization faces. General disaster prevention includes taking measures such as installing fire extinguishers in data centres, surveillance equipment monitoring high threat areas, alarm systems, back-up power generators, and adequate cooling systems for machinery. While I have noted some disaster prevention controls implemented by PRL, there are some areas that are lacking:

(1) Adequate Communication

Upon my investigation of the Information Services Division at PRL, I noted a lack of communication between Mr. Chow and the rest of the organization. Due to the prominent role that Mr. Chow plays in the Information Systems Division of the company, any prolonged period of loss of communication with him could lead to serious problems. In order to mitigate this risk, the organization should be capable of functioning normally without him.

While Mr. Chow claims his division staff could continue without him, the facts paint the opposite impression. It appears as though Mr. Chow prefers to work in isolation, independently of team members or senior management and has engineered several of the company's internal systems himself. To reduce this risk, staff in his division should be adequately trained to continue without Mr. Chow. Proper documentation of information systems, testing, and changes should also be made to enable staff to gain insight into any existing information systems.

Other avenues are also available to help mitigate the risk of disaster at PRL such as purchasing an appropriate insurance policy. The company should also create a comprehensive disaster recovery plan to expedite the recovery after a disaster does occur.

Solutions

In the short-term, after a disaster the use of redundant communication lines helps access vital information, while for the long-term additional back-ups should be implemented.

7. Incident and Disaster Recovery Controls

According to Mr. Chow, PRL has been able to maintain strict, high-quality incident and disaster recovery controls through the use of simulated emergency situations. Nonetheless, to ensure that the operations are not disrupted during unforeseen circumstances, the company must establish internal controls in the following areas:

(1) Data Retention and Backup

PRL currently uses an optical disk to store batches of original vouchers for transactions. Such use of physical storage increases the possibility of tape mishandling and should be replaced with an electronic vaulting system. Furthermore, the new system must have an automated backup system that saves data on a regular basis.

(2) Software Backup

The source and object code for ongoing software projects must be backed up on a daily basis or as changes are made.

(3) Data Backup for Batch Systems

The batch system used to process the transactions is critical for producing accurate financial data. Therefore the backup for this system must be updated on a daily basis. For master and transaction files, I have noted that the organization only keeps one version of these files. This indicates that the files do not contain a sufficient amount of data as required by the Canada Revenue Agency and the Internal Revenue Service (i.e. they contain less than 7 years of data). PRL must establish a strict policy to keep at least three versions of such files. This would also support the audit of the current fiscal year's financial statements.

(4) Data Backup for Online Systems

The backup procedure for the online system master file is completed in a different manner than the procedures followed for the backup of a master file for a regular batch system. The file must be updated as transactions occur and a new file must be created on a daily basis to accommodate any important changes. In addition, the organization must decide on how many times the backup must be updated throughout the day.

(5) Incident Response Procedures

Specific incident response procedures must be developed to provide employees with proper guidance on how to handle certain situations. When deciding on the procedures, management must designate an appropriate number of levels (generally less than 5 levels) to ensure that the process is not too bureaucratic or cumbersome.

Solutions

8. System Operations Controls

It is clear that Mr. Chow maintains a control-free approach to system operations controls dealing with daily operations. Therefore I would specifically like to address controls in the following five important areas in order to achieve sufficient system operations controls:

(1) Procedures to Cover IT Purchases

It is critical for management to maintain a Total Cost of Ownership (TCO) approach in its IT purchase approval procedures where a designated authority approves purchases depending on the value of the transactions. In addition, because PRL purchases a proportion of its software from outside sources, the organization must ensure that the software is compatible with the company's operating system before the purchase.

(2) Procedures to Cover IT Deployment

PRL must develop a policy to ensure that installing new software or hardware is always approved by management and only done by qualified personnel who have expertise in the field. Similarly, certain configuration standards must be decided on and distributed to employees to increase system uniformity.

(3) Network Documentation

The programmers and analysts at PRL do not follow specific documentation procedures even though they are continuously involved in the programming, testing, and maintenance of several information systems. Although this approach allows programmers to interactively work on a program, PRL must have network documentation in place to troubleshoot and effectively implement network changes. Under the current system, analysts only provide assistance on a needs basis, which may not be sufficient when a proper change needs to be implemented. Troubleshooting for TREB and ASP systems are also provided inconsistently and formal documentation should be established to better address customer needs.

(4) Server and Network Configuration

PRL should develop different policies and procedures to guide the server and network configuration for TREB and ASP systems. They must be regularly updated and reviewed to make any necessary changes.

(5) Network Monitoring Procedures

There are three ways that PRL can prevent errors in network monitoring: 1) using equipment that generates the least amount of errors, 2) designing safe circuit configurations, and 3) choosing the appropriate data transmission methodology. In particular, it is important to have data transmission redundancy procedures using methods such as parity checking and cyclical redundancy checking to minimize data loss.

I & IT Assurance

Solutions

MC Questions How does Investor Confidence Rules affect IT governance? It

a) requires management to certify internal controls.
b) prohibits an accounting firm from providing consulting service to an audit client.
c) requires the appointment of a chief risk officer.
d) requires the appointment of a chief privacy officer.
e) requires the rotation of auditors every five years.

2. In which environment is source code accessed the most?

a) Production
b) Development
c) Testing
d) Staging
e) Audit

3. Which of the following is an internal control?

a) Segregation of duties.
b) The organization will hire only honest employees.
c) Software change requests must be approved by the chief information officer.
d) Source code must be compiled to object code before user acceptance testing.
e) Information system risks are assessed annually.

4. Which environment should a program be sent to if user acceptance testing reveals an error?

a) Development
b) Testing
c) Production
d) Programmer
e) Backup

5. Which is the most effective control over system administrators?

a) Code of ethics
b) Reference check
c) Supervision
d) Management review of activity log
e) Performance appraisal

6. Who are responsible for IT governance?

a) Chief financial officer

b) Chief risk officer

c) Chief auditor

d) Senior executives

e) Board of directors

7. Which of the following is a back-up procedure?

a) Keeping transactions for seven years

b) Compressing historical transactions

c) Sending historical transactions offsite

d) Keeping a duplicate of the master file

e) Keeping the computer printouts and the master file

8. Which one is the correct one-to-one correspondence in number?

a) Library and environment

b) Programmers and testers

c) Source code and object code

d) Master file and transaction file

9. Which of the following library can be accessed by programmers extensively?

a) Test

b) Development

c) Staging

d) Production

10. Which of the following statements represents an undesirable practice?

a) Appointing the chief auditor to the firm’s IT steering committee

b) Assigning accountants to systems project teams

c) Hiring outside consultants occasionally to advise with respect to system development activities

d) Appointing the CIO to the firm's IT steering committee

I & IT Assurance

Solutions

CHAPTER FOUR

Review Questions

1. What are the different phases of system testing and who are involved?
   Programmers test their own code and this is called unit testing. Peer testing among programmers is called string testing, sometimes involving the testing of code written by different programmers. The entire system or a major subsystem is tested by independent testers and this is called system integration testing. Finally, user representatives test the entire system and this is called user acceptance testing.

2. If an organization hires a firm to develop a system, how does the organization ensure that the system will be maintainable?
   The user organization can include in the contract that the source code and related system documentation like system flowcharts will be given to the user organization upon contract breach by the developer or another form of contract termination. Arrangement can also be made for such documentation to be periodically provided to the user organization during the contract. A third control is to arrange for the source code and supporting documentation to be periodically deposited with an escrow which will allow the user organization to access the documentation upon contract breach by the developer or the developer going out of business, or upon certain other forms of contract termination.

3. What should be included in a request for proposal?
   The RFP should include detailed user requirements. Additional components of the RFP include the evaluation criteria, deadline for submitting bids and a standard.

4. What are the pros and cons of buying a system?
   Pros: Products available without lengthy developmental periods
   Soundly designed and well-tested and thus efficient and reliable
   Reasonable pricing
   Lowers change control risk as the customer is unlikely to have the source code
   ζ *Cons: General in nature, may not meet all requirements.*
   ζ *Acquiring firm is dependent on the software vendor for support*
   and maintenance and
   upgrades

5. What is a good use of the critical path diagram?
   The purpose is to assess the impact of any delayed tasks on timely completion of the project. Any activity or task on the critical path, if delayed, will delay project completion unless the slack is made up by other activities. There is only one critical path in a project. It is the path of predecessor dependent activities that will take the longest elapsed time.

<u>Solutions</u>

6. Who should sign off the user requirements?
   Project sponsor, project manager, system design manager, system architecture manager, internal audit, chief information security officer.

7. When should internal controls be first included in a systems development project?
   User requirement phase; this is because users are the best people who know what controls should be in the system.

8. Who should the project manager report to?
   Project sponsor

9. Write a job advertisement for a project manager.
   We are looking for a result oriented IT professional who has experience in managing IT related projects. The person will be responsible for managing IT development projects of varying sizes and working with different business areas of the organization. You will be part of a professional team of project managers in our corporate project management office. Your background should include five years of progressive experience in an IT related field and detailed knowledge of the systems development life cycles for traditional systems and fast paced development. Possession of the Project Management Professional designation will give you an edge. Other skills we look for include:
   - *Team building*
   - *Contract management*
   - *Strong communication*
   - *Consensus building*
   - *Organization*
   - *Financial management*
   - *Project accounting*
   - *Internet networking*

10. Who should be the sponsor of a student records system?
    Registrar

CASE SOLUTION

For this SUD audit of National Land & Water Information Service Project, the audit objectives are identified under three different categories: Project Governance, Business Requirements and Project Management. Procedures were then identified on the basis of the various objectives in order to outline ones that would best achieve the findings described in the audit report.

PROJECT GOVERNANCE

1. Unclear Roles and Responsibilities

OBJECTIVE: "Whether the roles and responsibilities of senior management committees, key project members, users, stakeholders and technical management are clearly defined, documented and performed."

PROCEDURE:

- Verify that roles, responsibilities and authorities are documented in sufficient detail in the Project Governance Chart.
- Verify whether the Project Governance Chart is up-to-date with all recent changes.
- Identify whether there are any inconsistencies between the Project Charter and the observed roles and authorities.
- Identify roles and responsibilities which are in the process of changing, ensure that the changes are constructive and compile evidence, if any, of any confusion these changes may bring regarding authorities.

2. Diverse Representation

OBJECTIVE: "Whether the Project Steering Committee has a diverse membership including the Senior Project Advisory Committee (SPAC), IT and senior management who, together, would provide full coverage of the Project risks, issues, benefits realization, alignment with business objectives and business needs."

PROCEDURE:

- Document who is on the Steering Committee, what professional background they have and their level of seniority.
- Identify any weaknesses in the existing composition of the Steering Committee. Consider unaddressed issues, flow of information and diversity of background experience.

3. Adequate Stakeholder Representation

OBJECTIVE: "Whether the Project Steering Committee has adequate senior representation from NLWIS users."

PROCEDURE:

- Identify stakeholders to the NLWIS project and perform interviews with them to understand their views and expectations for the Steering Committee.
- Assess whether stakeholders are appropriately represented by members on the Steering Committee.

Solutions

4. Adequate Segregation of Duties

OBJECTIVE: “Whether there are conflicting duties that endanger appropriate segregation of duties.”

PROCEDURE:

- Verify that there is appropriate segregation of duties between all Steering Committee members by reviewing all roles and responsibilities and identifying sharing of roles.
- Ensure that the Quality Assurance lead has a direct communication path to the NLWIS Executive Director so that the Project Manager is not perceived as a “filter”.

BUSINESS REQUIREMENTS

5. Adequate Prioritization and Validation of Business Requirements

OBJECTIVE: “Whether there is a formal process to assess, document and manage user requirements in system design, construction and process execution.”

PROCEDURES:

- Obtain information from management regarding methods for collecting user requirements. Verify that these methods are consistent and effective.
- Ensure that stakeholders have approved architecture and application designs and that there is evidence of their participation and walk-through in the review and approval stages.
- Obtain confirmations from users through interviews that they feel appropriately involved in the process, that communication between them and management is effective and that their concerns are appropriately addressed.
- Trace business requirements through to the design and construction phases through meeting minutes to confirm that that the requirements were delivered by the project.
- Ensure that a thorough and unbiased cost-and-benefit analysis is performed in which stakeholder requirements are prioritized.

PROJECT MANAGEMENT

6. Non-Compliance with Change Management Controls

OBJECTIVE: “To find a mature process for the management of project and system related changes as well as evidence for that the process is followed. A mature process would involve users, development staff and in some cases IS/IT security personnel.”

PROCEDURES:

- Identify the roles of the members of the committee responsible for approving the changes
- Confirm that items recorded in the change control log can be traced to the recorded decisions
- Ensure that all key stakeholder groups have the ability to input change requests, by reviewing history of change requests and interviewing parties who are able to input requests, to ensure there is no obstacle preventing them to do so
- Trace a sample of recent changes to the minutes of the Change Control Board meetings, to ensure that no change requests were made without appropriate approval

Solutions

7. Ineffective Risk Management

OBJECTIVE: "To find a mature risk management process whereby risk mitigation plans are developed, monitored and escalated as required. There should also be sufficient evidence of risks being addressed on a timely and proactive basis"

PROCEDURES:

- Check to see if management is using tools, such as the Risk Matrix, to identify components of high risk, and how they can mitigate them
- Ensure that risk mitigation plans are signed off by a designated person upon completion
- Inquire with management and review risk-related reports generated by the company
- Check for meeting minutes of risk management committees to ensure that managers are considering risk management aspects regarding the project as well as that any questions/issues concerning risks are being address in a timely manner

- Review project planning proposals and ensure that there is detailed documentation concerning the progress of the projects as well as any risks involved

8. Limited Performance Monitoring & Reporting

OBJECTIVE: "To find a mature performance monitoring process that leverages standard industry techniques, such as critical path analysis and earned value reporting, to support decision-making and transparency by enabling timely and fulsome performance reporting. Also, to find evidence of effective and mature performance reporting that supports project monitoring described above as well as address reporting requirements.“

*Critical path diagram on page 202: it shows the interdependence and sequence of tasks needed to be performed as part of a project, and their duration, to identify the length of the project and set budgets and deadlines.

**Earned value is a very useful metric used in financial monitoring procedures which measures benefits realization by identifying whether actual expenses incurred are consistent with business plans; in essence, earned value measures the extent of useful time spent on a project

PROCEDURES:

- Verify that an adequate monitoring infrastructure is present for all full-time and part-time project resources.
- Identify the existing performance metrics and confirm that no gaps exist in performance reporting.
- Verify that realized benefits are effectively measured and linked to cost.
- Ensure that a system is in place to provide a complete assessment of project status regarding schedule, budget, benefits and the nature of existing or potential problems. Confirm that the system reports further on the "earned value", incorporating delivery of benefits and outcomes.

9. Insufficient Transition Planning

OBJECTIVE: "To find evidence of an end-state plan for the NLWIS Project in order for the project team to transition NLWIS to the future business owner responsible for ongoing service delivery."

I & IT Assurance

Solutions

PROCEDURES:

- Accumulate evidence of transition planning, specifically the end-state impact of the NLWIS project. Evaluate whether sufficient estimates and information is provided on how the project will be sustained after completion. (e.g. annual operating costs).
- Ensure that the in-service model for NLWIS is updated regularly, as per changes undertaken throughout its development stages.
- Evaluate whether it is reasonable to conclude that the project will reach a timely completion.
- Identify the team responsible for sustaining the project after completion and ensure that their roles and responsibilities are sufficiently documented.

MC Questions

1. A company has hired a consulting firm to develop a system, but the consulting firm does not want to release the source code to the company? What would protect the company's interest in terms of the system's upgradeability and maintainability?

a) Registration of the system
b) Confidentiality agreement
c) Non-compete agreement
d) Source code escrow agreement
e) Access control

2. Which risk goes up the most when an organization outsources systems development?

a) System integrity
b) System reliability
c) System maintainability
d) Unauthorized data access
e) System responsiveness

3. Is which systems development phases are flowcharts prepared?

a) User requirement
b) Programming
c) Design
d) Procedures development
e) Conversion

4. Which pair of activities can often be carried out concurrently?

a) Training and procedures writing
b) Testing and conversion
c) User requirements development and system design
d) Project planning and system design
e) Design and programming

Solutions

5. When internal auditors are asked by a project manager to provide user requirements to a system development project, they should

a) refuse in order to maintain independence.
b) provide as comprehensive requirements as possible by thinking like the business users to ensure the system is complete.
c) address the system's auditability.
d) address the system's disaster recovery capability.
e) facilitate the user requirement workshops.

6. What is the relationship between systems development controls and software change controls?

a) They are mutually exclusive.
b) Software change controls depend on systems development controls.
c) They are inter-dependent.
d) Systems development controls depend on software change controls.
e) For a system under development, software change controls should be applied before engaging systems development controls.

7. Which of the following concern is most common to systems development controls and software change controls?

a) User requirement definition
b) Testing
c) Feasibility study
d) Database design
e) Emergency fixes

8. What is the correct sequence of system development documentation?

a) System architecture, user requirements, flowcharts, programs.
b) Project plan, test plan, user requirements, flowcharts.
c) Entity relationship diagram, user requirements, Gantt chart, flowcharts
d) Business case, feasibility study, test plan, user requirements.
e) User requirements, entity relationship diagrams, system architecture, flowcharts.

9. How do user representatives sign off computer programs?

a) Review of design documentation
b) Review of user requirements
c) Review of computer programs
d) Testing
e) Post-implementation review

10. Which phase is avoided when an organization purchases a software package rather than developing it in house?

a) Defining information requirements
b) Identifying alternatives
c) Design
d) Testing

Solutions

CHAPTER FIVE

1. What is the similarity between PIPEDA and Electronic Commerce Act?
   They both protect consumers and apply to organizations that offer eBusiness.

2. Which risk does eBusiness affect the most?
   eBusiness increases the concern about transaction authorization and information privacy because of the nature of the Internet.

3. What is the consequence if a domain name server is hacked?
   A user may be directed to a hacker site or if the DNS is down, outgoing traffic can come to a halt.

4. What are the audit implications of EDI?
   More reliance on controls, e.g., EDI controls particularly with respect to security. Less substantive testing for inventory because companies can use EDI to achieve better "just in time" inventory.

5. What is the difference between URL, IP address and MAC address and what are the risk implications?
   Every Internet transaction has to include these addresses in order for it to be routable. A URL is essentially a web site address like www.ontario.ca. An IP address is a numeric address consisting of four 8-bit bytes and in more advanced networks, four 32-bit bytes. A MAC address is hard coded address assigned to a network adaptor by the manufacturer, like a vehicle identification number. URLs and IP addresses can be assigned dynamically. In other words, a computer may be assigned different URLs or different IP addresses from time to time, however, the MAC address does not change. The MAC address is therefore crucial for a network to route traffic. It also provides a permanent audit trail of which computer was used to carry out an activity and this information is useful in forensic investigation.

6. What are the risk implications of RFID?
   One fairly wide concern about RFID is privacy. For example, if an organization attaches a tag to a consumer product, can the organization track where the product is used and perhaps who uses it? This concern is understandable as privacy breaches are often reported in the media. The risk and control implications of RFID, however, go beyond privacy. In fact, the basic reliability factors of completeness, accuracy, authorization, timeliness, occurrence and efficiency have to be considered as they can be compromised by less than adequately controlled deployment of RFID.

Solutions

7. What are the key controls to protect intellectual property?
   Registration
   Access controls
   Contracts with software developers, consultants and employees re intellectual rights.
   Management monitoring of access to and use of intellectual property
   Employee education

8. How do you think the audit of Google differs from that of General Electric?
   More control testing for a company like Google and less substantive testing. This is not to say that control testing is not important for GE. There are more systems in GE so the variety of controls is higher. More real time testing for Google because of the higher fluidity of transaction. No inventory in Google.

9. How does eBusiness affect the five system components of infrastructure, software, people, procedures and information?
   More complicated infrastructure
   More software
   Few people in customer service but more technical developers
   Less in house procedures but more help screens and features for customers
   Higher information risk because of the fluidity and online nature of information.

10. Referring to the general controls discussed in Chapter Three, which types do you think are more affected by eBusiness?
    Access and availability.

CASE SOLUTION

Unauthorized User:

This may be the result from several different scenarios:

□ An unauthorized user may access the authorized user’s account without the knowledge of the authorized user.

□ An unauthorized user may access the authorized user’s account and make changes with the authorized user’s knowledge however this would be a breach of the usage policy and the transactions of the unauthorized user may not be acknowledged by the authorized user. For example, a husband gives his wife his username and password and the wife submits claims without the husband knowing.

The consequences:

The authorized user may not take responsibility for the transactions processed by the unauthorized user. This may lead to confusion regarding health and dental balances and investigations will have to take place in order for rectification; investigations may be timely and cause inconvenience to both the insurance company and the client

Preventative Measures

1) **Confirmation:** Any transactions processed must be verified by the client through a faxed confirmation. The online claim is sent to the claims department for processing however before payment for the claim is dispersed, the client must print the claim verification, and sign the confirmation and return it to the insurance company for payment disbursement. The client will have 10 business days to fax the claim verification form back to the insurance company. This process may be timely and inconvenient; therefore we can set a threshold for claims over $500. The insurance company should also have signature cards on file to match the claims verification. This will ensure an unauthorized user cannot process claims and deposit the payment into another account.

2) Set up direct deposit for the claimants. The bank information must correspond to the direct deposit information submitted by the claimant's company. Henceforth, any deposits are deposited directly into the pay account of the claimant submitted by the company. Any changes to the direct deposit account must be submitted by the company and not the claimant.

3) Challenge Response: This allow authentication of the user and ensure access is granted to a human being and not a hacking robotic tool.

Detective Measures

1) Management and Independent Review: We can implement a control system to compare claims year over year to observe whether claims are consistent in terms of type and amount. Also, we can compare similar claims over time to see whether the claims are submitted in reasonable timeframes. For example, dental claims for regular dental cleaning

are generally submitted every 6 months. If there are irregularities, we can confirm the claim with the client before processing.

2) Negative Confirmation: We can send a letter right after payment to the client's home address to verify that they have received the claim. If there are any discrepancies, we can advise the client to contact the claims department immediately. This is a negative confirmation to confirm that the claim was properly processed and payment was made to the authorized client.

2. User Input Error

This risk is related to the authorized user inputting the claims information incorrectly.

Consequences:

The claim may be processed under the wrong category or for an incorrect amount

Preventative Measures

1) We can implement system edits to ensure that appropriate information is inputted into the correct fields.

For example:

a. Payment amounts must be numerical and in a specific format.

b. First Name and Last Name fields must be alphabetical characters

c. We can have a drop down menus for the allowed types of claims (dental, medical, orthodontics, other)

d. Postal codes should be in the correct sequence

2) If claim values are above the benefit dollars we can have a message to prompt the client to enter a lower amount that is allowed.

Detective Measures

1) Boundaries: We should set upper and lower limits for the most common claim values for specific types of claims. If the client inputs higher or lower claim amounts that do not fall within these limits we should have further verification procedures before processing the claim. We can contact the client or the medical professional directly to investigate the details of the claim. This will ensure the claim type is correct and legitimate.

2) For claims over a material amount such as $5000, we should have secondary verification by a claims specialist before payment processing. Since these are large claims we can investigate to ensure there is are no keying input errors. Also, this investigation can further ensure the claims are legitimate, follow the insurance claim criteria, and ensure fraudulent activities are not occurring.

I & IT Assurance

Solutions

Solutions

3. Unauthorized Transactions

Employees risk losing the chip based coverage card, employee's personal information may be stolen in the process of accessing website - unauthorized transactions

Preventive

1) eBusiness Encryption - Secure Sockets Layer (SSL) creates an environment where there is a secure area for data which runs between the web browser and the web server; ABC's website must have access to a server that is supporting the SSL application. This requires both parties to have the appropriate technology, SSL is normally present in Microsoft Internet Explorer browser.

2) Password - Employees are encouraged to change their passwords frequently, therefore, even if the employee lose their card, unauthorized users cannot log into their accounts even if they "steal" the cards from the employees

Detective

1) Access Card - employees required to sign a form upon card issuance committing to inform ABC when the card is lost, the access control system online should track all the card usage. Access cards should be coded to indicate the employee that is using the card (confidentiality)

2) Lock - Since dentists and pharmacies insert their coverage card to a card reader on their PCs to submit claims, there should be instructions given to laptop or PC users to lock it to fixtures while unattended, furthermore, ABC should periodically patrol for compliance.

4. Unauthorized Changes to Employee Profile

Employers can enrol their employees via the web site - thus, employers may be able to change employee's profiles or compromise their information

Preventive

1) Access Control List - Different users should have different rights to access the information. Although employers can enrol their employees via the website, the right to make changes to information should only be granted to the employee, although employers still have the right to read the information. Therefore, the system has to be told who to allow to access to what and to what depth through an access control list. The employee should have full access to its information (read, write, delete), but employers should only have the right to read (unless the employee have stopped working for the company, then employer has the right to delete too). This ensures access only based on authorization, to maintain the confidentiality and integrity of information provided to both the employee and the employer.

2) Passwords - Again, employees are encouraged to change their passwords often, so that its employers will not have unauthorized access to their accounts. Furthermore, the employees is encourage to adopt different passwords for different systems, as this will

help decrease the risk of exposing all of one's records in all systems when the password is compromised.

Solutions

Detective

1) Monitoring and Alerts - To ensure the unauthorized changes are identified in a timelier manner and to minimize the damage that ABC's customers may face, effective monitoring processes must be implemented. First, a log entry must be created for any events that happen on the account. Furthermore, a mechanism should be implemented to notify the employees of these events if there are changes to their accounts (even if the changes were made by them). The mechanisms can be an email alert, or a telephone message.

2) Log-in feature - A security feature that ABC may implement on its web site is to allow employees to see the last few accesses made to their own account. Therefore, if anybody else, such as their employer have been able to log into the employee's account, then the employee is able to acquire this information by verifying the last login activity feature. ABC should provide employee the detail as to when the account was accessed, whether it was using a regular web browser, or from a mobile device, furthermore, the IP address should be identified as well. For employees, seeing information such as the IP address is important because if the employee know that they always use the same computer to access the account, the IP address will be the same, however, if it is a significantly different address that they see, the employee is able to detect that someone else had access their account.

5. Unsecured Channel

Employers can enrol their employees via the website – possible unsecured channel for transferring confidential information

□ It is expected that when employers create an account for their employees they would be transferring highly confidential materials such as bank accounts, sin number, address etc. If not handled properly, it is possible to have their accounts breached and identity stolen or hackers may have information altered before reaching ABC

Preventive

1) A representative from ABC Life Insurance can visit their clients on a regular basis to personally collect information from the employers. After giving personal information to the representative from ABC, the employer should require them to sign a document indicating that they have received the documents. In the event of a breach, the people who had access would be held accountable; hence, with action accountability, the people would be less likely to misappropriate use the information

2) If information were to be sent via the website, there should be an encryption of the information. In order to access the locked document, it would require a decryption key. The decryption key would be sent via another channel (e.g. mailed or e-mailed) or at a different point in time

Solutions

Detective

1) On a regular basis contact ABC to ensure the banking information which they received is identical to those provided by the employer. There should be a materiality level depending on the size of the company.

2) Firewall/ Intrusion Detective and Prevention Standard – which scans the source of the incoming traffic which it uses to determine the likelihood of an intrusion. Of course, this would require the systems to have previously designed protective/ preemptive measures when the system detects an intrusion. For example, if it detects a foreign/ undisclosed IP address that would prompt the system to be aware of the incoming information and to take precaution when dealing with it. As there are chances that it is virus which will steal confidential information from ABC's system.

6. Direct Deposit Information Exposed

Claims submitted online can be paid by direct deposit – there are two problems first, it can be hacked so that these claims are deposited into another person's bank account. Second, the direct deposit information can be exposed to unknown parties.

Preventive

1) After ABC has received a claim submission, they should confirm with the employee before approving the payment with regards to the amount and the bank account

2) ABC should attain WebTrust and/ or SysTrust certification which indicates that they have sufficient controls for online transactions

Detective

1) ABC should provide guidelines on how long the employee should wait before they receive their payment. If it has been an exceeding amount of time then that particular claim/ transaction should be investigated.

2) After the deposit has been made by ABC, the employee has to (within a certain period of time) confirm payment in the correct amount. Then ABC can sample a number of claim of a period of time to identify the instances which the claims was processed incorrectly.

7. Risk of Online Claims Submission by Dentists and Pharmacies

Dentists and pharmacies can submit claims online - giving access to 3rd party and making it inherently risky (privacy concerns since unauthorized transactions more likely)

Preventative

1) Instead of giving access to dentists and pharmacies, they can hire someone or put a current employee in charge of inputting the information for dentists and pharmacies. This gives them less access and give them the ability to control the risks of information getting out to other parties (although may not be cost effective)

Solutions

2) Add finger print login for the websites (new laptops typically have finger print identification systems – ex. Yahoo enables users to login by finger print)

Detective

1) Review claims submitted by pharmacies and dentists on a daily basis. Ensure that appropriate information and amounts are being inputted, as well as checking for any errors that may have been inputted

2) Send customers a copy of their claims and ask for an affirmative response. Ask them to reply if it is correct or if there are misstatements on the claims

8. No Mitigation of Risk of Unauthorized Transactions

Chips were launched at an accelerated scale - they're not doing themselves a favor and aren't mitigating the risk of unauthorized transactions

Preventative

1) Launch limited chips for the dentists and pharmacies. Limiting the amount of dentists and pharmacies that can use this chip will lead to lower risks of fraud

2) Go through a screening process that will only grant chips to trustworthy dentists and/or pharmacies or only grant chips to long-term dentists and pharmacies associated with ABC Life Insurance

3) Limit all the chips transactions to occur at a certain hour of the day to avoid suspicious chip activity

Detective

1) Call customers and employers randomly, one a week, to verify transactions and to ensure that each transaction exists and/or is accurate

2) Have someone authorize transactions of amounts higher than the materiality level (which should be set by ABC Life Insurance Company)

3) Review claims annually to ensure adequate provision for responsibilities, billing arrangements, security and privacy

I & IT Assurance

Solutions

MC Questions

1. Which of the following violates the Personal Information Protection and Electronic Documents Act?

a) A professor shares your grades with other professors in your university.
b) A prospective employer asks for your citizenship.
c) A bank uses an employee’s doctor notes to assess whether to approve the employee’s loan application.
d) A life insurance company asks about your medical history.
e) A government job application form asking about your citizenship.

2. Which of the following has the most privacy impact?

a) Intellectual property
b) Cookie
c) Sarbanes-Oxley Act
d) Database management system
e) Enterprise resource planning system

3. What does P3P automate?

a) Privacy policy
b) Password change
c) Cookies
d) Favourite web sites
e) Web history blocking

4. Which type of controls does the Ontario Electronic Commerce Act affect the most?

a) General
b) Access
c) Input
d) Processing
e) Application

5. If a bank does not post its privacy policy on its web site, which principle is it violating?

a) Accountability
b) Limiting use
c) Openness
d) Individual access

6. Which of the following is most likely to occur if a domain name server breaks down?

a) Business transactions can be decrypted by unauthorized parties.
b) Users will be spammed.
c) Users’ transactions cannot be forwarded.
d) User computers will be infected.

I & IT Assurance

Solutions

7. Which of the following types of intellectual property is infringed on when someone distributes purchased music to a large group of friends?

a) Patent
b) Trademark
c) Copyright
d) Goodwill

8. Which type of control does intellectual property registration belong to?

a) Corrective
b) Preventive
c) Detective
d) Restrictive

9. Which organization is subject to PIPEDA?

a) A Canadian bank
b) Ryerson University
c) Government of Ontario
d) Toronto Hospital
e) Department of National Defence

10. Which risk do EDI payments mitigate?

a) Late payment
b) Overpayment
c) Underpayment
d) Paying the wrong party
e) Bounced checks

I & IT Assurance

Solutions