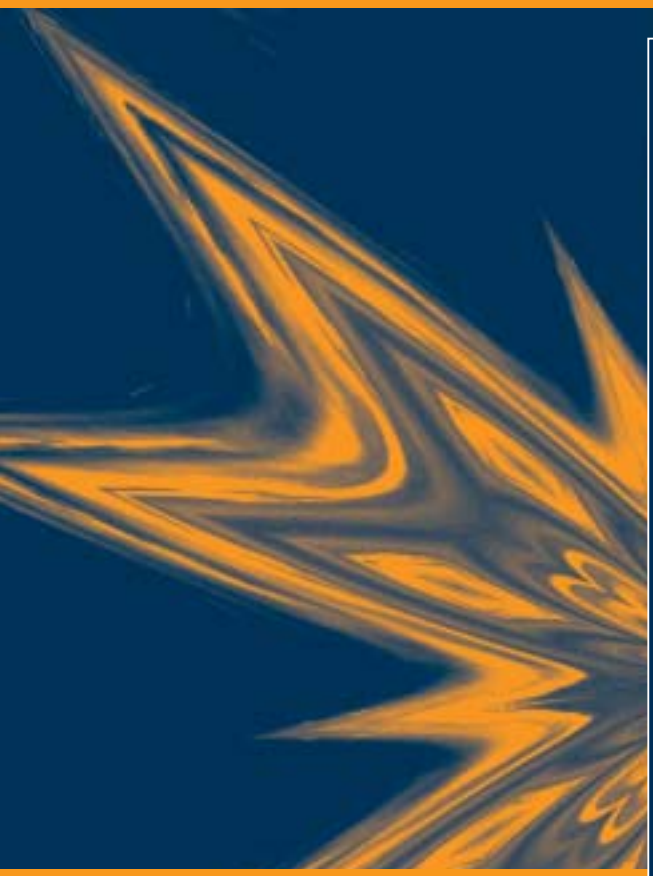
chapter

10

Monitoring reporting systems and reviewing reporting procedures



Learning objectives

- To learn about achieving completeness and accuracy of data.
- To discover methods of standardising input data and documentation.
- To know about maintaining appropriate backups.
- To learn about understanding and monitoring reporting requirements.

the story

It has been a very eventful few months for David and Mary. They have been heavily involved in the implementation process of their new accounting information system. Their internal accountant, Michael, has turned out to be an invaluable asset in helping them understand the various system issues. Michael has worked closely with the implementation partners to make sure that the system is stable and is able to produce timely, reliable information.

So far, all the staff have been very understanding and have not minded the regular interruptions for testing and training purposes. In fact, they have grown more committed to making the implementation as successful as possible. The key to maintaining their support has been the regular team meetings that have kept everyone informed of the progress of the various stages of the implementation project. Using the change request form has also proved to be an excellent way of keeping track of system issues as they arise and communicating functionality problems without creating stress.

As the project is drawing to an end, the consultants have begun asking the users to provide all of their standard forms so that they can be reviewed in the context of process simplification. By modifying some of the form designs and input screens, the consultants believe that they can reduce the number of errors and interactions users have with the system while processing their information.

In this chapter we discuss data preparation as it relates to the input processes and backup methodologies used to maintain complete data integrity. We then focus on the procedure for monitoring system output so that reporting timelines can be effectively managed.

key terms

integrated system A system in which various subsystems and/or phases of business operations share the same data

matching principle Accounting strictly for items and transactions relating to a given accounting period

reporting requirements Compliance with the *Corporations Act*, taxation law and other laws, and with the standards of various monitoring bodies

reporting system The component of an accounting information system concerned with the production of both routine and annual reports

introduction

When a system is implemented and is operational, it is important that the reports produced by it are complete and accurate. So long as the operating system performs to the standard for which it was designed and developed, the completeness and accuracy of the reports can be maintained by ensuring that the data entered into the system are complete and accurate. The completeness and accuracy of data is achieved through monitoring and reviewing input. The monitoring of **reporting systems** and the reviewing of reporting procedures is carried out in order to maintain the quality and reliability of the reports produced.

Monitoring reporting systems

The reporting system is monitored to ensure that the information provided by the reports can be relied upon by decision makers. The factors involved in achieving this objective are:

- confirming that the data input are complete, accurate and relate to the appropriate accounting period
- ensuring that the employees are well aware of the processes for recording and classifying the transactions and that procedures for internal verification of records are in place
- standardising the source documents using structured formats so as to minimise human error.

There are practices and procedures that ensure a new system has integrity. These same practices and procedures also monitor the accuracy and reliability of reports. These procedures are discussed below.

Achieving completeness and correctness of data

Achieving correct data input begins with assigning the correct account codes to the data. There should be a set of properly described account codes for this purpose. This will help to avoid any ambiguity. The assignment of account codes is further checked and approved by an authorisation process. This authorisation process also serves as a control mechanism that helps to prevent the input of unwanted data. The account code descriptions should be checked when entering the data. The account code should also be checked by the data entry clerk for its content. For example, an account code is checked to see whether it has the number of digits it is intended to have. Also, a check should be made to confirm that every account code is currently in use. Computers are able to perform most of this scrutinising through built-in software checks, thus automatically rejecting any account code that is currently not in use. For example, popular accounting systems, like *Oracle Financials* or *MYOB*, have this type of basic error-control function. If an inactive or nonexistent account code is entered, and providing the user has system administrator privileges, the system will prompt the user to either create the account code or activate it. Otherwise, a warning message will appear advising the user to speak with the system administrator.

The accuracy of input data is assumed in an **integrated system** where an input in one system leads to the complete maintenance of correct data in a number of systems. For example, when an invoice for a sale is entered into an integrated system, the data calculated by the system as the total sales value will be recorded in the debtors' system as money owed (accounts receivable), and in the general ledger system as sales. Hence, when the invoice is checked for the accuracy of the sales value (i.e. quantity $\times$ price $=$ value), it can be safely assumed that all the other data recorded are correct. In batch processing, the total of the values on each document in a batch can be matched against the total produced by the computer for that batch in order to verify the correctness of the original input.

Ensuring that the data is complete is achieved by doing a transaction count. Counting the number of transactions input and comparing that number with the number of transactions intended to be input reveals any data entry discrepancies. Completeness can also be achieved through prenumbering the data sources and then matching these numbers with those generated by the computer during the input process. The total number of documents or the total number of transactions on all the documents of a batch when matched with the totals produced by the computer verifies the completeness in batch processing. There should be appropriate checks in place in the organisation to prevent any transaction document from being inadvertently left out without being processed. That is, it should be ensured that all the transactions are accounted for.

The **matching principle** relating to data input for an accounting period should be strictly adhered to so as to confirm that the transactions accounted for actually belong to the appropriate accounting period. To achieve this, the dates of the transactions should be carefully checked. A structured authorisation process will

also assist users in adhering to the matching principle. At the close of an accounting period checks should also be in place to ensure that no transactions relating to that accounting period are left out. Any missed transactions will subsequently be processed in an inappropriate accounting period, thus jeopardising the accuracy of the reports.

Documenting procedures and account codes

The transaction recording procedures need to be documented. This document is kept up-to-date by incorporating any changes in the procedures as they arise. The procedures serve as a reference for the existing staff and as training material for new staff.

A detailed dictionary for account codes is also maintained and kept up-to-date by making adding and deleting accounting codes as and when necessary. This dictionary is used by the existing staff to clarify any doubts they may have regarding the correctness of codes used. In addition, the code dictionary certainly helps new staff apply the correct codes from the outset.

The set procedures and the account code dictionary should be made available to staff so that they are regularly used as a reference for internal verification of records (i.e. in the gathering and evaluation of evidential matter) by independent persons and, in particular, by internal auditors. The account code dictionary is also referred to during the approval process of a transaction.

Standardising source documents

Standardising source documents into a structured format helps minimise human error during the data entry process. Standardised structures allow similar types of information to be recorded in a particular place on the form. This helps the staff to readily recognise the nature and type of data recorded. Further, standardising and prenumbering of the documents assists in maintaining the completeness of the data input. When they are prenumbered, any missing items can be investigated to prevent errors. If any of the prenumbered forms are cancelled, they are marked as such and retained safely to help in confirming that all transactions are properly accounted for.

The data on a source document, such as a supplier's invoice, is transferred onto a standardised input document with a structured format to assist in the entry of data. Information, such as the invoice number and the invoice date, on the original source documents (the supplier's invoice in this example) is found at different locations in different documents because these documents are produced externally. Further, the size of the documents will vary from supplier to supplier. Thus, a standardised input document not only assists in easy entry of data, it also ensures that all relevant data are extracted from source documents and recorded in the spaces on the form.

Any new form introduced should follow the pattern of the existing forms, as the employees will already be used to this style. If a new form does not conform to the existing pattern, the staff may find it difficult to comprehend and apply, thereby effecting a potential increase in both the processing time and processing errors. Any

changes proposed to the standardised forms should be monitored for consistency and conformity with the existing form design.

Staff should be consulted regarding any proposed changes to the format of standardised forms. This consultation process will identify any difficulties with the use and completion of the forms and will also avoid any potential resistance to change by staff. Any reasonable change that will result in data processing efficiency should be explained to the staff and their acceptance of the change obtained. It is also important that new features are explained to the staff and that they receive training on how to use the form.

Backups

Having taken steps to account correctly and completely for the transactions relating to the accounting period, it is important that the data in the system are safeguarded against any possible loss or corruption due to:

- corruption in the software
- failure of the computer hardware
- damage to the computer system due to disasters such as earthquakes, floods, fire, and so on
- accidental damage to software
- intentional damage to software from worms and other viruses
- hiccups during processing.

The data need to be backed up at regular intervals and stored away in a secure place. In case of data loss or corruption, the organisation should be able to rely on these backups. Software should also be backed up in case it is lost or corrupted. Software backup need not be as regular as data backup but it should be done at least at every stage when modifications or improvements are made to software.

The organisation should consider all the factors of risk management and set down in written form their own procedures for backups. These procedures should be regularly reviewed to check their suitability to the current situation. An organisation may introduce new computer hardware that may need a different type of backup. For example, a personal computer user might have been using a Zip drive with a 250 megabyte capacity as a backup device. If the computer hardware capacity is increased, then a change to a compact disk (CD) storage device, which has more capacity, may be advisable. It should be noted that any change considered should take into account the capacity of the storage device, the ease with which it can be handled and the longevity of the medium for recording. The storage medium must be one that facilitates easy retrieval of the data contained in it if the necessity arises.

In addition to any audit requirements, there are *Corporations Act* and taxation law requirements that stipulate the need for an organisation to retain their source documents for a certain extended period. These documents can be either hard copies or electronic copies. Where possible, they should be stored in a fireproof and vermin proof environment.

Regular backups of electronic data are made with storage media (diskette, tape and compact disk) that are suitably marked and indexed. Copies of this backup should be stored on site for immediate use when needed and stored off site in a safe environment in case there is a complete disaster, such as a fire in the building housing the computer. A logbook detailing the time, date, and other required information on the backed-up data should be maintained in order to facilitate easy access when required.

In a small system, the responsible staff perform a backup just before they leave work for the day. In a larger system, automated overnight backups are generally performed either at the site or remotely from a different site. The backup may also be done at a time when the system is not fully occupied. In a smaller system it may not be necessary to backup all the data. The data to be backed up is determined by its sensitivity and the degree of difficulty that would be experienced if it needed to be reconstructed from source documents. In a larger system, it is customary to backup all the data as it is very difficult and impractical to identify who updated which data during the day. Also, daily transaction logs are printed and stored for use in case data needs to be reconstructed. In the case of a corruption, the data is restored from the latest available backed-up data. It is made current by re-entering the data processed since that backup was made. The daily transaction log of the data processed helps in identifying the data entered after the backup was made.

Backups are kept on a different storage device each day. If the backup immediately prior to the failure becomes useless, the previous backup is used to restore the data. This process is called the 'rotation of backup'. Although rotation of three of these storage devices is recommended for backups, the use of five devices is not uncommon. In this process, the backup on a particular day is made on one storage device, on the second day it is made on the second storage device and so on. For example, the backup on Monday night may be made on a tape marked 'A'. On Tuesday night it may be made on a tape marked 'B' and on Wednesday night it may be made on a tape marked 'C'. If only three tapes are used, the tape marked 'A' will be used again on Thursday night.

It is advisable not to limit the backups to three or five rotations. It might be wise to retain backups for some other specific days. For example, in addition to retaining backups for every day of the week, the backups could also be retained for, say, the last three weekends. Also, it may be useful to retain backups for the month-ends for one year. This is advisable in a large organisation where staff may accidentally delete certain files and subsequently request a restored copy. For example, someone may find out after a month that they have deleted a file that is required for month-end processing.

Most of the large organisations run computer systems in a resilient mode where the main database (primary system) is duplicated simultaneously onto another (secondary) system so that, if the primary system fails, the secondary system takes over and maintains the workflow.

Reviewing reporting procedures

Reviewing reporting procedures serves the same purpose as monitoring reporting systems—to ensure the reliability and accuracy of the reports these systems produce by checking the integrity of data. This process is another action taken by management to maintain the quality and reliability of reports. This action may include:

- systematically checking sources of input data and documentation records for accuracy and reliability
- establishing **reporting requirements** and analysing these requirements regularly to identify any variations
- checking reporting requirements for compliance with the established processes for recording and classifying the transactions of the organisation
- maintaining explanatory notes and financial results as source documents to support any reports.

These review actions are discussed in more detail below.

Checking the source of input data

There can be a variety of sources of input data and documentation records, or simply, source documents. The procedure to be employed when checking a source document depends on the particular source document itself. One method of checking a source document received from an external supplier is to match it with another source document internally created so as to confirm its accuracy. For example, the number of items purchased shown on an invoice received from a vendor can be matched with a goods received note, created by the stores department of the organisation, which shows the number of items received by that department.

Another method of checking a source document is to compare the amount shown on it with the standard information available within the organisation. For example, the price per item shown on the invoice received from a vendor can be matched with the pre-agreed price and the applicable quantity discounts from the price list available within the organisation.

Sometimes, a standard set within an organisation can be used to check a source document. For example, a time sheet submitted by an organisation's employee can be checked against the standard starting time which could be, say, not earlier than 7.30 am. If an employee writes their starting time as 6 am, before inputting the data, it should be checked whether a prior approval to start work at 6 am was given.

The calculations made on source documents are also scrutinised for their accuracy. For example, the quantity received multiplied by the unit price will show the value paid for the item. Again, the values of different items are added together to get the invoice value. These values are generally scrutinised by two independent people before the input is made. The first person who checks the calculations may also be the person who translates the information into the standardised format used by the organisation. The second person who scrutinises this also approves the transaction to be input. A test check in the process of internal auditing also strengthens the checking of source documents for accuracy and reliability.

Monitoring reporting requirements

Reporting requirements and the procedures for preparing reports have to be established and should be documented. This documentation should show a brief description of each report, the procedures for preparation, standard formats and the timetable for release of the various reports. This is particularly important when a specific report is prepared infrequently, as the documentation serves as a reference for the staff who are involved in the preparation of reports. The documentation also helps new staff when they are preparing reports for the first time.

Once established, the reporting requirements and procedures need to be modified as required to comply with changes in circumstances. The set requirements and procedures serve as a reference against which compliance with the current reporting requirements and procedures is checked. Any discrepancies revealed by this checking process may well be due to staff taking short cuts with regard to the established requirements or procedures. By short-cutting established procedures, staff may jeopardise the accuracy and reliability of output reports. Conversely, the discrepancies can be caused by adaptations to changes in circumstances that have not yet been incorporated into the procedure documentation. In the former situation, staff can be advised, reprimanded or retrained. In the latter situation, the procedure documentation should be promptly modified to reflect the current situation.

It is vital to constantly review reporting procedures in order to accommodate changing circumstances

The reporting requirements and procedures are established in conjunction with the established processes for recording and classifying transactions. Generally, a top-down approach is taken in establishing the processes for recording and classifying transactions based on the reporting requirements. A reporting requirement may be varied due to changes in the legislation and management requirements. These changes to the requirement will bring about changes in reporting procedures, which, in turn, may bring in changes to the established processes for recording and classifying transactions.

It is possible that staff, either deliberately or ignorantly, may not incorporate the required changes in the established processes for recording and classifying transactions to match the new reporting requirements. They may, instead, develop some short cuts to produce various reports. An example of this could be a report required by management to identify the overhead expenditure of each unit of different departments of the organisation. If the current established process is to record overheads only at a departmental level, staff may take steps to apportion the overheads on a percentage basis that they think is appropriate in order to produce the required management report. Staff should have modified the process to record the overheads at unit level and although the produced report gives some value it cannot be complete and accurate.

An internal audit should be able to establish whether the reporting procedures comply with the reporting requirements. Further, an internal audit should compare the actual practice against the established procedures to ensure that the practice follows the established procedures. The established procedures for reporting should also be compared with the established processes for recording and classifying transactions with the view to confirming compliance. If compliance cannot be confirmed corrective action should be taken. It need not always be the function of an internal audit, but a procedure for internally reviewing these aspects at regular intervals and at every level of operations and management will be beneficial once established in an organisation. These internal reviews lead to either self-correction to comply with the procedures or to modification of the established procedures to suit the changed circumstances. This phenomenon can be termed a ‘systems appraisal’. A systems appraisal is a review of a system to determine how well the system actually works. This appraisal is the responsibility of line management and is normally performed by people responsible for the relevant accounting functions.

Explanatory notes and financial results

Most of the reports produced for middle- and lower-level management are automated, that is they are produced by the system automatically. Reports for senior management and external parties are generally produced individually using automated reports from the system, such as financial results and some reports specially prepared by middle and lower management for this purpose. Further, some conclusions in reports for senior management and external parties are arrived at

using information already available. Thus, reports that are for senior management and external parties have the following items as supporting documents:

- specific written reports prepared by individual managers
- explanatory notes giving the details on how the numbers and conclusions given in the report were arrived at
- the financial results from which the information, if any, for the reports was extracted.

The person who releases the report makes sure that these supporting documents are available before the reports are released. The maintenance of supporting documents for the reports is also checked by an internal audit procedure.

summary

Data loss or corruption presents a serious disruption to the flow of business activities and to the reporting cycle, so it is critical to ensure that effective control measures are in place that help to circumvent any potential system threats. To that end, our intention in this chapter has been to help you better understand the importance of:

- achieving completeness and accuracy of data
- standardising the input data and documentation
- maintaining appropriate backups
- monitoring the reporting requirements of the organisation.

Checkpoint

1. What is your understanding of the completeness of data input?
2. What is your understanding of the accuracy of data input?
3. How are correctness and completeness of data input achieved?
4. What are the causes of data loss or data corruption?
5. Give three examples of how the accuracy of input data can be checked.
6. What is your understanding of reporting requirements and procedures?
7. State three supporting information requirements necessary when preparing reports for top management and external parties.

Multiple-choice questions

Circle the letter corresponding to the correct answer.

1 Completeness and accuracy of data may be achieved by:
- **(a)** monitoring the output
- **(b)** monitoring and reviewing input
- **(c)** monitoring the input
- **(d)** none of the above

2 Which of the following is not a cause for corruption of data?
- **(a)** computer hardware failure
- **(b)** accidental damage to software
- **(c)** use of a faulty mouse
- **(d)** hiccups during processing

3 Reporting requirements may be varied when there are:
- **(a)** changes in legislation
- **(b)** changes in management requirements
- **(c)** changes in established processes for recording and classifying information
- **(d)** all of the above

4 The quality and reliability of reports are maintained by:
- **(a)** monitoring the reporting system
- **(b)** reviewing the reporting procedures
- **(c)** ensuring the completeness and accuracy of data input
- **(d)** all of the above

5 Information provided by accounting reports can be relied on if:
- **(a)** reports are produced on a timely basis
- **(b)** reports are presented in an attractive format with visual aids
- **(c)** data input are complete, accurate and relate to the appropriate accounting period
- **(d)** the use of source documents is minimised

6 **All transactions applicable to an accounting period must be processed. This is ensured by:**
- **(a)** matching the total number of transactions on all documents with the totals produced by the computer
- **(b)** incorporating appropriate checks in computer programs
- **(c)** following a structured authorisation process and careful checking
- **(d)** (a) and (c) only

7 **A standardised input document is useful because:**
- **(a)** all relevant information is recorded on it from source documents
- **(b)** all suppliers can be forced to design their forms in the same way
- **(c)** it will increase the processing time
- **(d)** an opportunity arises to train staff

8 **When selecting devices for the backup of data in a system, the factor which is least important is:**
- **(a)** the capacity of the backup device
- **(b)** the ease of data retrieval
- **(c)** the cost of the device
- **(d)** the longevity of the device

9 **Systems appraisal means:**
- **(a)** carrying out an internal audit
- **(b)** an audit performed by external auditors
- **(c)** an internal review of procedures
- **(d)** none of the above

10 **Which of the following is not a supporting document for financial reports?**
- **(a)** explanatory notes about various points covered in the report
- **(b)** a statement showing how certain figures in the report were arrived at
- **(c)** source documents used for preparing the report
- **(d)** special reports prepared by experts

Activities

1 **Why are account codes important? What steps would you take to ensure that account codes are assigned properly to transactions?**

2 **What is meant by 'standardisation of source documents in a structured format'? Why is such a document used for inputting data?**

3 **Explain how you would ensure that all electronic data are safeguarded.**

4 **How would you ensure that any accounting reports produced are reliable?**

5 **How would you ensure that reporting procedures comply with reporting requirements?**

6 **How would you ensure that a new system had robust integrity?**

7 **How would you monitor the accuracy and reliability of financial information provided by a new system?**

Case study

David of P & S Furniture Mart came across a book on accounting information systems while he was in the library waiting for Mary to finish her shopping. He was interested in the section titled 'Coding structures' in the book which said:

> *There are three coding structures, namely sequence coding, block coding and group coding.*
>
> *Sequence coding is the assignment of numbers or letters in a designated consecutive order. This technique enables a user to account for all items because any missing items will create a gap in the sequence code.*
>
> *A block code involves reserving blocks of numbers within a numerical sequence. Each block corresponds to a category which is meaningful to the user.*
>
> *Group coding consists of two or more subgroups of digits or letters combined in a field to designate a number of classifications. Each subgroup specifies a data classification in a series. The series is generally a left–right arrangement with the positions, blocks or designators becoming more specific the further right they are in the series. Group coding allows for the sorting, summarising, and retrieval of information based on one or more of the subgroups.*

David wondered about the details of the coding system in the new computer system being implemented at P & S Furniture Mart. He wanted to confirm that the coding structures he had read about were followed when the coding for the new system was being designed. As a starting point David noted down the information he would need for decision making in order to confirm whether the coding could facilitate suitable reporting.

At the moment P & S Furniture Mart only has one showroom but it is on the verge of opening one, if not two, more showrooms. David also plans to venture into tendering for the supply of furniture to organisations which are newly built or being refurbished such as hotels, motels, schools and government departments. To do this he may have to rely on other manufacturers. Alternatively he is seriously considering manufacturing within his own business in order to increase the profit margin.

David would like to get reports prepared which show details of sales of various products, and sales by various customer groups. He would also like to know the cost of production for various items of furniture. David thinks that this information will help him in his decision-making process regarding tender pricing and product continuity.

The day after discovering the book in the library, David meets with Michael, the internal accountant at P & S Furniture Mart and raises his doubts about the suitability of the accounting codes used in the new system. Michael reassures him that all these codes have been thought of as distinct possibilities in the design process by the consultants. Michael continued to inform David about the coding structures of the new system.

What do you think Michael would have given as examples for the three coding structures? What general factors should the consultant have considered before the coding system was designed and implemented.