

Preserving Integrity

Integrity of information is key to the finance function. Peter Morley recommends some regular checks.

Integrity is at the very core of the finance function. The principles of bookkeeping and double entry are founded on the principles of cross-checking and algebraic logic. An audit sign-off says more than just whether something adds up or not, it says whether it is 'true and fair'.

While the features embedded in modern financial systems can go a long way to helping maintain the integrity of information, they are not sufficient on their own to provide certainty. As an analogy: while all cars have some necessary safety features (such as an oil light) these rarely show all dangerous conditions and shouldn't be relied upon as the only 'health-check' point. Likewise, systems should alert their owners when fundamental

Further, in the case of larger enterprise resource planning (ERP) systems, data contained in the system is usually generated from a number of functions which, because of their different cultures, often have different data accuracy tolerances. This could lead to further data integrity issues – the accountant versus the salesman's tolerances, for example, may be very different.

The most basic integrity checks are highly objective, but as one moves around the control regime, the checks become increasingly subjective.

Below are some suggested integrity checks which should be performed as a matter of routine. There are three types:

1. Logical checks and balances that a system can control.
2. Looking for illogical data – ie, the data adds up but it does not make business sense.
3. Spotting fraudulent data.

The second and third of these categories can be further sub-divided based on:

- ◆ Personal integrity and fallibility – this is controlled by separating duties to perform the work (ie, human cross-checking).
- ◆ Extent of real-world verification and reconciliation – for example, when was the data last cross-checked or validated to reality? Issues here can include out-of-date data (eg, wrong postal address); duplicated data; perishable, time expired, lost or damaged assets; and un-reconciled data.

It is possible to devise a routine control regime that can mitigate these risks. The principles can be universal, but their precise definition will depend on the nature of your business. It is a key part of implementing a financial system to build into the supporting processes enough checks and balances to give confidence to the figures.

Obviously, integrity issues can also give rise to significant business risks. These risks may include:

- ◆ Double counting of income or expenditure.
- ◆ Duplicate payments – eg, original invoice and copy paid.
- ◆ Openness to fraud.
- ◆ Misleading accounts as value can be held where the asset has perished.
- ◆ Wasteful and expensive administrative re-work – eg, for a bank reconciliation.
- ◆ Wrong accounts where reporting hierarchies miss out accounts or duplicate values are reported.

The following are some integrity checks that we recommend are performed regularly:

1. Logical integrity:
 - ◆ Trial balance equals zero.

- ◆ Reporting hierarchies are comprehensive and complete.
- ◆ Account balance records (if held) agree with underlying transactions.
- ◆ Control accounts balance to open (unpaid) items on their subordinate sub-ledgers (eg, accounts payable).
- ◆ Bank reconciliation is complete, balanced to the penny and contains no items outstanding on the statement.

2. Data quality:

- ◆ Supplier and customer name and address data has been checked in the last two years and for duplicate postcode and bank account details.
- ◆ All amendments to payee bank details should require two levels of authorisation and if not used for say two years, should be put on 'hold' and only be used when released by a supervisor.
- ◆ Goods received not invoiced (GRNI) report should routinely have nothing older than 30 or less days; similar ageing checks should be carried out for outstanding purchase order commitments and incomplete orders.
- ◆ Fixed assets and stock should be verified at least once a year.
- ◆ User accounts and privileges should be re-verified every two years.

There are many more checks that can be performed, and these will depend on the nature of your business and type of organisation.

To ensure you identify and minimise the main risks to your business, we suggest you carry out a 'risk mind map' exercise on your organisation and select the risks with the highest impact on your business (irrespective of their probability) and carry out integrity checks around these risks, in addition to those listed above.

In conclusion, data integrity is a vital issue for any finance function. Some systems will support the regime suggested here more easily than others. But if you use a good report writer and adopt a rigorous approach to data integrity checks, it should help you implement the necessary controls to ensure integrity of information is maintained. It is well worth the effort.