Compliance Exposures in ERP Systems, Part 1

A White Paper by Ken Gorf FCMA

What's the Problem?

Major enterprises around the world rely on ERP systems for both operational purposes and financial reporting. In doing so, the ERP systems become an integral part of the corporate governance and legal compliance landscape.

Whilst most IT management attention seems to be on document retention, reporting quality, and security, there are much broader issues to be considered to ensure good governance and compliance with regulations such as Sarbanes-Oxley, IFRS and Basle II.

> These three regulations are directed at various aspects of governance, and have different origins. Sarbanes-Oxley (named after the two US law-makers that pushed through the legislation) resulted from a number of corporate scandals in America. IFRS is a European initiative with its origins in the accounting profession and a focus on accurate financial reporting. European subsidiaries of US companies will be subject to both Sarbanes-Oxley as well as IFRS. Basle II is concerned about risk and exposures in the financial services market.
>
> What they have in common is the objective to give various stakeholders timely, accurate, dependable information expressed in financial terms.
>
> They are also regulations with various degrees of bite. Because Sarbanes-Oxley was born out of financial scandal with subsequent legal actions, the legislation uses tough penalties as a threat for future law-breakers. IFRS and Basle II are less onerous, but the impact on a company's fortunes in the marketplace could be considerable and damaging if there were serious breaches.
>
> Since most enterprises that are subject to these regulations rely on ERP systems for the generation of their published financial information, and for the purpose of this document, they will be assumed to impose a common set of compliance requirements on ERP system users.

In particular, managements are required to demonstrate they have appropriate processes in place to support good value and risk management. In addition, auditors are now focused on verifying the processes that produce data in addition to the reported information itself.

> To meet compliance requirements, both managements and auditors must be able to show they have tested the processes and shown that they satisfy the legislation. Some pointers –

> For example, global cross-enterprise financial reporting must be consistent and comparable. In real terms, this means that the ERP systems employed in an international group must be the same [vendor] system, at the same release level, and be implemented in the same way.
>
> In addition, there is a need for transparency of information through detailed disclosure of enterprise-wide data, including an analysis and reporting of the business by segmentation – again, impossible without a common and consistent data source.

ERP systems are significant investments with long-term impacts on major enterprises. Meta Group reckons that the cost of a 1,000 users system is £21.7 million each year based on a five-year average. For all these reasons the compliance of any ERP system must be a focus for the CEO and CFO, and not assigned to IT as a technology project.

> Meta Group is one of the most respected IT observers and consultants with operations around the globe. Even if their figures are wrong by, say 10 –15%, the numbers are still significant.
>
> ERP systems are major investments, and are made only after thorough analysis and planning by the enterprises concerned, and intense sales campaigns by the ERP system vendors. In monetary terms, these investment decisions rank alongside the largest capital projects for any business, and the systems adopted will be expected to be used for ten to fifteen years. Senior executives will invest much management time and effort in considering the Return on Investment (ROI) before approving the expenditure. Multinational companies will often deploy systems for 10,000 and more users – hence the costs will often exceed hundreds of millions of pounds every year, and for many years.
>
> The legislation referred to above is continuous and has global reach.
>
> Hence, because of the numbers involved, and the significance of the impact of failure, compliance is not simply another IT project. Unfortunately, many companies have consigned ERP compliance to IT executives. This does not absolve the CEO and CFO from their legal obligations, and is also completely unreasonable on the IT team!

Evidence

A body of evidence is now available that points to serious issues with compliance and efficiency in the way ERP systems are implemented by companies and their consultants. West Trax Applications LLC, which provides analytical and diagnostic services for ERP systems, has undertaken some 300 benchmarks for over sixty enterprises across Europe in 2003-2005, and the results are disturbing.

- Not one organisation was using more than 50% of the vendor software they were licensed and paying for. Software that is never used only adds to costs without contributing to ROI. IT is not aligned with the business. (Remember the mustard allegory? The profit lies uneaten on the side of the plate).

  Typically, a contract for ERP software includes licence fees for the software and annual fees for maintenance – usually, maintenance is a percentage of the software licence fee, say, 15 to 20%.

  ERP systems are priced and contracted by functional module, e.g. finance, manufacturing, retail, warehousing, purchasing, human resources. Each module contains major elements, sub-systems, and individual transactions and processes.

  In addition to the licence and maintenance costs, ERP users incur significant people costs e.g. training, support. Typically, IT departments are organised around functional skills i.e. to match the ERP system modules. Hence, there is a key productivity issue when considering the ROI for the IT people investment.

  The benchmark database shows that, on average, enterprises use less than 50% of the transactions and processes within each module licensed. Some transactions may not be needed by the specific enterprise or subsidiary, some may be inappropriate and require modification, some may simply be overlooked. However, the benchmark sample shows that companies are paying a significant overhead or premium for the software they are actually using. There is also the strong probability that they are missing valuable opportunities to optimise their systems and operations by not implementing available software that they are already paying for.

  Enterprises cannot achieve optimal ROI if they don't use the software. Who is tasked within the enterprise to continuously review this untapped opportunity? IT? Finance?

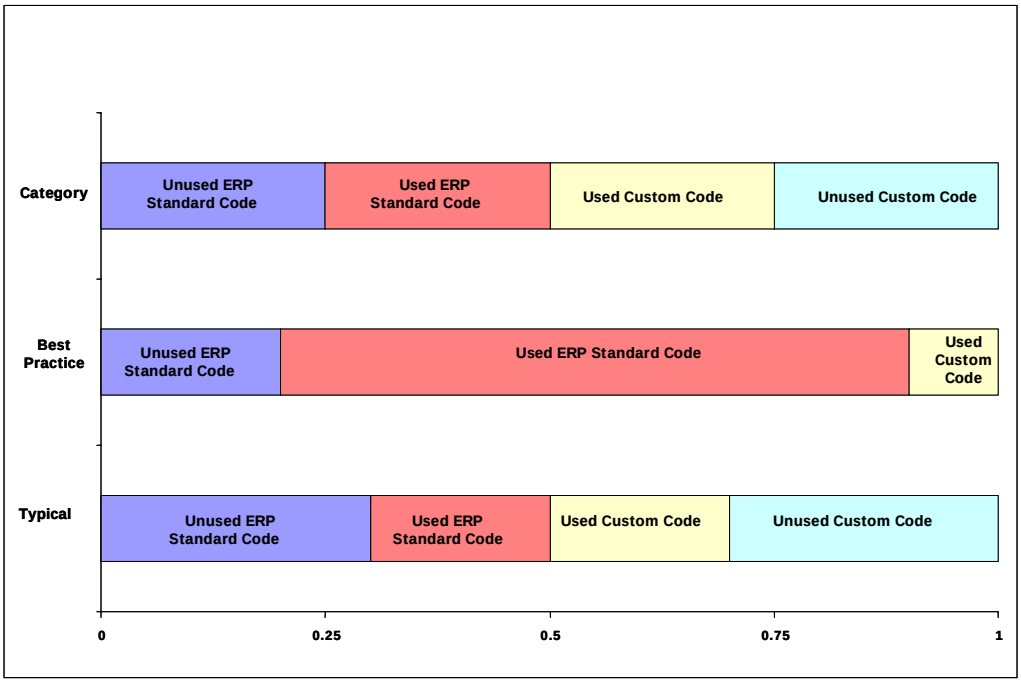
  One of the key features of leading ERP systems is the integration between the various modules, enabling processes to easily span functions. This is both efficient and also provides a solid internal control structure – a key compliance requirement. Hence, compliance is weakened when software modules are not fully implemented and a process or transaction is interrupted or incomplete.

- In most of the systems analysed, the proportion of ERP vendor transactions used was surprisingly low. More than half of the software actually used was custom code written by internal staff or external consultants. The ERP vendor software may be compliant, but not necessarily the total system.

Every system consists of four elements –

1. Standard vendor software used
2. Standard vendor software, unused
3. Custom written software, used
4. Custom written software, unused

Chart 1 Software Components in an ERP System



Clearly, the most effective systems will use as much standard vendor code as possible, will minimise the use of custom code, and will have no unused custom code.

Therefore, the benchmark results show that most enterprises are far away from the ideal situation. It also raises key questions about the costs incurred in writing custom code (internal and external resources), and whether the custom code meets compliance regulations.

Other evidence suggests that this situation worsens over time i.e. divergence from the ideal state continues unless action is taken to counter the trend. This characteristic has been labelled “application erosion” – where the proportion of vendor code is reduced and the proportion of custom code increases.

The result is that compliance issues will become an increasing problem unless tackled aggressively.

> Acquisitions & Mergers – Due Diligence
>
> There is an interesting aspect of compliance worthy of mention at this point, and this relates to companies that are the subject/target of A&M activity.
>
> It is well known that different computer systems can impede or even prevent a successful A&M situation. But often, companies proceed on the basis that they both "run the same ERP system". This may be so, and the systems may even be at the same vendor release level.
>
> However, what if the two companies are running different transactions within the vendor system? What if they have written custom code for completely different transactions? What if one has implemented a specific vendor module, but the other has chosen to use only a sub-set? Based on the West Trax data, this is the most likely situation. In which case, the two companies are running two completely incompatible ERP systems.
>
> Do they know? Who can tell them?

- Many of the custom programmes were seldom or never used. Unless deleted, these redundant programmes continue to incur support costs, over and above standard vendor maintenance charges.

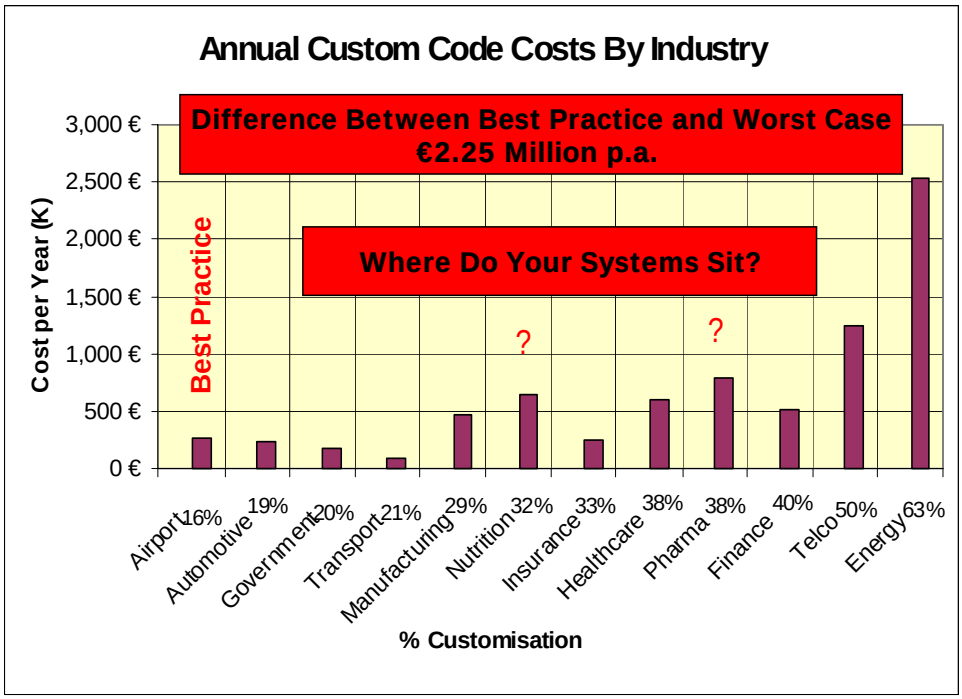
  This finding implies that custom software has been written without a clear requirement (or approval?). This might include temporary software to enable migration from one system to another, or short-term requirements for one-off projects. A more dangerous cause would be code written to work-around standard transactions, or introduce data from off-line spreadsheets. All of these are potential exposures for internal control.

  As well as the internal control risks, custom code collects ongoing support costs whether it is used or not. For example, all transactions must be tested when implementing a vendor software release, or consolidating systems. A rigorous spring clean of this software on a regular basis will reduce the problem.

- In the systems analysed, the annual costs associated with custom software ranged from circa €250,000 to over €2 million. In the enterprises benchmarked, ERP vendor maintenance costs (based on a fixed percentage of the licence fee) were more than twice the level justified simply because less than 50% of the software was actually used.

  The compliance legislation calls for a focus on value management as well as risk management. The systems analysed in the benchmark are not large systems (measured by numbers of users), yet the overhead associated with custom code carried by the enterprises is significant. There is clearly a wide range between "best practice" and enterprises at the wrong end of the scale. It would also appear that some sectors are better than others.

Chart 2 Annual Custom Code Costs



- The interfaces between vendor code and custom code showed major internal control exposures. They may be poorly documented and lack audit approval. Cross-functional processes are rarely understood and monitored because IT organisations and skills are commonly focused on vertical applications e.g. manufacturing, finance, sales.

This is a key compliance issue. As soon as an enterprise introduces custom code either in place of or in addition to vendor code, there is an internal control risk at the point of interface.

Documentation is an issue. The vendor documentation should be reliable; the custom code itself may be documented; but the interfaces are a problem. The ERP vendor is, of course, completely unaware of the existence of the custom code, and the custom code writers will move on to other work (or employers) in due course, and will not be available to constantly monitor these interfaces.

There is also another key issue here. As mentioned previously, efficient ERP systems will integrate processes that span across functional modules. For example the process to approve a supplier's invoice for payment could span purchasing, warehousing and financial modules. In this example, the contract price features in two of the modules, as does the quantity received and the receipt date. Approval to pay a supplier's invoice relies on the agreement of certain information in line with a company's procedures. If one piece of this data is introduced from a custom source, internal controls are exposed, and the system is open to mistakes, incorrect payments, and even fraud.

The compliance legislation expects managements to test and document internal controls. This is one area where those tests are vital.

- The most revealing information from these benchmarks was that, in most cases, the CEO and CFO did not know they had a problem. The results came as a surprise, and the lack of previous visibility a serious concern – and a real compliance issue.

  Why is this a compliance issue? Because the CEO and CFO are required to personally attest (by signature on reporting schedules) to meeting the various legal requirements. Therefore, if much of the risk management and value management information in their ERP system is hidden from them, their attestation is worthless.

  The CEO and his team should be able to ask –

  - Is the system actually supporting the business operations as intended?
  - Is the system delivering the strategic business benefits anticipated in the original business case?
  - Do the benefits justify the investments to be made throughout the ERP implementation's life cycle?

  The failure to conduct post-implementation reviews and track actual versus planned benefits is frequently put down to

conflicting priorities and a lack of tools to gather appropriate management data. In fact, sources of data are available, but they are often not used, for a variety of reasons -

- The “C” level executives may not be aware of the importance and availability of system optimisation data and its potential to help them manage ROI, business alignment and compliance issues.
- IT management may not be aware of the available compliance data or its value to corporate executives.
- They may be too busy supporting and updating current systems to analyse historical performance.
- There may be a reluctance to expose historical governance and performance issues.

Whilst some ERP vendors are now offering software tools to tackle compliance issues, these can only apply to the vendor’s own software. If the enterprise is not using 50% of the vendor software, then these tools are a questionable investment. And, the custom built software is not included in the support, training and documentation provided by the ERP vendor, plus the original implementation team has moved on to other projects – another compliance exposure.

> *“What is possibly more surprising than this habit of customising more than half the application is the fact that in most instances the CFO knows nothing about it – revelling in the warm glow created by the certain knowledge that his or her organisation is using a standard set of processes and that this has done no harm at all to their CV. What is particularly worrying is that much of this custom code is undocumented and involves the use of private spreadsheets. Most CFOs and CIOs think their organisations just have one version of the truth – held in ERP data files. Nothing could be further from the truth.*
> *All of this should be ringing alarm bells for those with any responsibility for compliance. Undocumented, multiple versions of the truth are exactly what the regulatory authorities are keen to unearth.” Martin Butler, Butler Group.*

There used to be a saying in IT organisations that you couldn’t be fired for buying from IBM. That may no longer be true, but perhaps the ERP system vendors (who are huge global enterprises) may now be in the same situation. Within the IT function, the safe option is to stick with major players that are already endorsed by peers, and can provide excellent support. In most cases, the ERP system will have been implemented with the help of a specialised ERP consulting (or outsourcing) company that also enjoys wide acclaim and approval. The potential risks to be faced by challenging this well-trodden path are unwelcome by IT managers.

It is clearly difficult to persuade CEO’s and CFO’s to recognise the risks to the business and their own positions by not challenging the status quo. Enterprises are not making decisions or looking at their ERP system deficiencies based on objective information – they are

typically provided with subjective opinions influenced by career concerns, compensation, personal motivation, and the desire to avoid change and being the bearer of bad news.

Perhaps a recent survey by the National Computing Centre will help to focus attention on the problem –

> *"Nearly half of IT executives claim they aren't fully aware of the standards and legal requirements that apply to them.*
> *In a survey of 300 IT decision-makers conducted by the National Computing Centre (NCC), 44 per cent admitted to not being fully aware of IT standards and legal requirements - and 22 per cent admitted to not having any awareness of the issue at all.*
> *Sarbanes-Oxley Act and Financial Services Authority regulations, as well as legislation such as the Data Protection Act, can all have a bearing on the IT department. Other standards such as BS7799 and the e-government interoperability framework can also apply.*
> *Stefan Foster, managing director of NCC, said: "This is an alarming figure, indicating significant lapses in compliance and poor adoption of best practice."*

In the meantime, what are the practical measures that can be taken, and how can these be achieved within the organisation?

Actions for Management Accountants

One of the most common reasons for these worrying results is the failure of organisations to conduct ongoing post-implementation reviews, to track realised benefits versus the original goals, and to do this throughout the life cycle of the ERP system. Evaluating the strategic benefits and legal compliance provided by ERP systems cannot be made on purely technical grounds. If the task of assessing attainment of these goals is delegated downwards within an organisation, the focus will be on tactical or technical measurements.

> *"Regardless of the technology used or the efforts of IS, the formal system and the actual business processes will have a widening gap over time. A periodic review of this gap will help focus attention on the problem." Olin Thompson, a principal of Process ERP Partners.*

Martin Butler and Olin Thompson are just two of the many consultants calling for constant vigilance and monitoring of ERP systems during their life cycle.

The methodologies and tools for conducting management reviews are normally to be found in the CFO's area, and suit the skills and experience of Management Accountants.

So, here are three key questions for Management Accountants to ask their IT colleagues, with a request for objective answers based on real data, and in straightforward business language.

1. What percentage of the ERP vendor software licensed is actually being used? What are the plans to optimise the current applications, or to conduct a cost/benefit analysis of lightly used modules?

2. What percentage of the custom code is essential, what percentage can be replaced with vendor code, and what percentage is unused? What are the plans to delete unused code before the next software release, or request for more server capacity?

3. Which processes and transactions contain interfaces between vendor and custom code? Are they documented, and approved by Internal Audit?

   The key objective here is to get real objective data, which can be analysed, and then used, confidently for decision-making. The raw data required lies in the system log files. In its raw state, it is of no use, but using automated analysis tools the raw data can be turned into valuable information.

   Often, IT management is aware of the data, but not aware of its importance or usefulness. The West Trax experience strongly suggests that CEO's and CFO's are not aware that the data exists, nor aware of how valuable it could be.

   The analysis tools can provide much more information than simple percentages of unused vendor code or custom code. For example, the transaction-level information shows how many times a file is changed after its first creation. This information is invaluable in looking for internal control weaknesses. A purchase order that is changed several times after its first creation may point to poor purchasing processes, but could also point to fraud. A customer order that is changed several times may point to poor order management that in turn could lead to customer dissatisfaction.

   The system log files are just that – a log of how the ERP system is being used. There is no need to analyse sensitive commercial data, so the analysis process itself is not a compliance threat.

The next step would be to use a combination of System Benchmarking and Activity Based Costing to express the problem in financial terms. First, all planned costs associated with the four system components (or "activities") would be established by using Zero Based Budgeting (Used Vendor Code, Unused Vendor Code, Used Custom Code, Unused Custom Code). The process would then be repeated to reveal and review the actual costs for appropriate time periods. A management analysis of activities not delivering targeted benefits would result in their elimination or revised targets and costs

based on ZBB. This analysis process could also be employed when reviewing and approving new projects, software upgrades, server consolidations, and particularly outsourcing.

The system benchmarks would produce a comprehensive list of all transactions in the ERP system, separated not only by the four “activities”, but also by functional module and sub system. The major costs elements for the ABC analysis are (1) people (2) software licences (3) ongoing support and (4) capital equipment.

Since most IT departments assign ERP modules by functional skills, this helps to identify people to activities. The people costs of any new implementation can be directly attributed to relevant activities i.e. they should only be working on implementing vendor code or custom code. In practice, we know that much of the custom code will not be used, so this analysis will pose some interesting questions!

Vendor software licensing is typically based on the vendor’s own module structure – users pay for whole modules no matter how much of a module is actually implemented. The system benchmarks will show how much code is used or unused, so that the costs can be allocated to both areas. It can be argued that the vendor’s licence fee for a particular module should be assigned 100% to the actual transactions implemented, with no cost assigned to the unused code. However, this may not show the real cost of unused software, and therefore the motivation for looking for opportunities to use this code in the future.

The vendors will also charge maintenance in addition to the licence fee, and this would normally be allocated with the licence costs. However, since the vendor will only be responding to maintenance requests on the used software, perhaps this again could be assigned 100% to the used code. Note that failure to implement new vendor releases within a given timeframe often results in cost penalties from increased vendor maintenance charges.

Ongoing support costs cover a range of activities – training, documentation, help desk – each of which can be assigned to vendor or custom code.

ERP systems typically have a programme of vendor upgrade releases, maintenance releases, consolidations, de-mergers, etc. These can be major events in the calendar with people and other costs specifically budgeted for the purpose. All should be allocated to the function and vendor/custom code areas. This will inevitably lead to valuable debate about people assigned to work on software that is no longer or rarely used! Why document this software, why test it, why not just delete it?

Capital budgets will consist of both core infrastructure spend as well as client equipment for new ERP implementations. In assessing ROI, it is essential to assign both existing IT assets and new planned expenditures across the various areas. Of equal significance is the ability to consider the potential to defer capital spend as a result of deleting software not used.

Chart 3 – Activity Based Cost Worksheet

(by function, module, organisation unit)

Category	Used ERP Standard Code	Unused ERP Standard Code	Used Custom Code	Unused Custom Code	Total (100%)
Number of Transactions					
Percentage Of Transactions					
Cost Group – People					
Cost Group – Licences					
Cost Group – etc					

If the ERP system is outsourced, or outsourcing is being considered, these questions (and more) should be in the outsourcing contract as essential components of system monitoring and the contractor's continuous improvement programme. Outsourcing does not remove the responsibility for compliance – it just makes the job more complex. Following a decision to outsource, then ZBB is also an effective tool in the process of re-establishing the in-house IT organisation. One of the critical new roles for IT and Finance together is conducting ongoing post-implementation reviews – benchmarking at quarterly intervals would make this an objective exercise, based on real system data. These reviews can also be the forum for developing system efficiencies and, hence, driving down outsourcing contractor fees.

Much has been written about outsourcing, and it is not the purpose of this document to add to that particular debate. However, it is essential to fully understand the legal responsibilities for compliance when planning to outsource an ERP system. The bottom line is that an enterprise cannot outsource compliance of the system. Therefore, the outsource contract must include all the necessary processes for both

parties to adhere to the relevant legislation, and apply continuous monitoring to maintain compliance management.

A regime of regular post implementation reviews is an ideal basis for such monitoring. It is recommended that IT and Finance together manage this process, with the support and advice from Internal Audit.

These reviews will serve several purposes –

- Monitoring outsource compliance issues
- Demonstrating compliance to external auditors as required by the legislation
- Advising the CEO and CFO on opportunities to cut costs, improve productivity, cut risks and really *measure* ERP operations
- Comparing the performance of the enterprise with others, particularly peers in the same industry sector, and using this information to direct improvements

The final area for consideration in this white paper concerns the internal control exposures created by over-dependence on custom code – issues like documentation, training, and skill retention have a direct impact; but also the interfaces within and between custom applications and vendor software are fraught with dangers. To identify and tackle these exposures requires accurate benchmarking data throughout the various layers of the system, and across the vertical or functional applications. Two actions required – first, to scope and tackle the problems with existing systems which requires the co-operation of IT, Management Accounting and Internal Audit; second, to establish the management process for the review and approval of all future proposals to implement custom code rather than vendor code in new systems or modules.

This is a complex area. It is both a challenge for enterprises to understand the issues involved, and therefore a significant area of risk where breakdowns in internal controls are most likely.

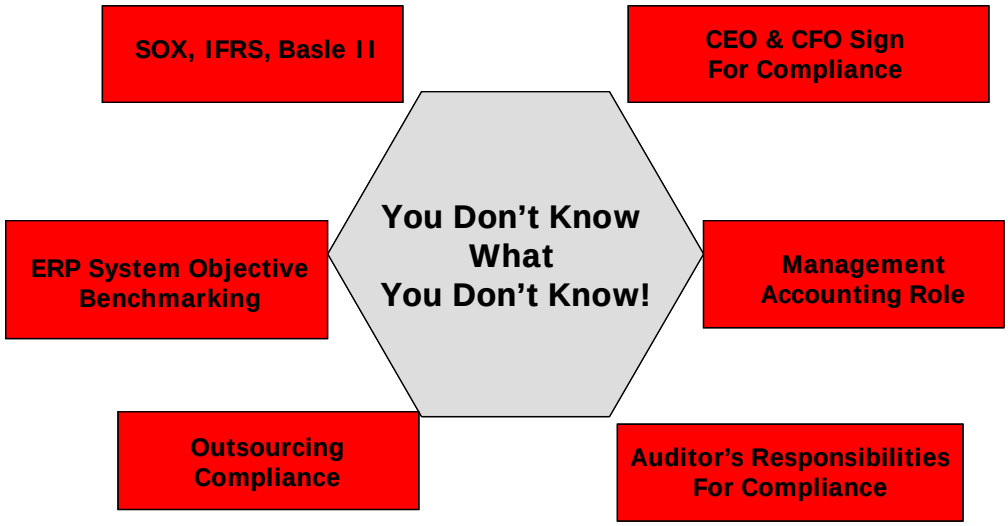
It cannot be avoided. As external audit firms become more familiar with the requirements of compliance legislation, they will demand detailed assurances from management about the workings of their ERP systems.

As well as carrying out the benchmarking analyses described earlier, the enterprise compliance management process should ensure that lessons are learned from past problems. A strong recommendation would be to formally review and approve all ERP implementation plans from the compliance perspective. Certainly this would include any proposals to develop custom

software instead of using vendor code. It should also include the reverse situation – a cost/benefit analysis of using only a small part of any particular vendor module compared to writing some small transaction for the purpose.

Compliance exposures in ERP systems are a reality today, yet a key responsibility of CEO's and CFO's. Technology is now available to identify problem areas and corrective action, and this is also an opportunity for Management Accountants to take the lead in tackling the problem.

Chart 4 Compliance Issues Summary



Ken Gorf is Chief Financial Officer of West Trax Applications LLC, a software and services company with operations in the UK, Germany, and the USA. Ken is a Fellow of the Chartered Institute of Management Accountants.