

Extract from Jim Lee's 'midrange matters' column in iSeries365 and iSeries News UK

COLUMN: Midrange Matters with Jim Lee: COMPLIANCE AND CONTROL

When it comes to compliance, watch out for gullibility, reasonability and liability.

Setting aside the dictionary definition of compliance, I am going to define it in a corporate IT idiom, as "the art of balancing gullibility, reasonability and liability".

My fascination, from a position of overseeing so many aspects of IT, is that compliance is required or demanded, for the most part, to standards that are outside of the sphere of IT per se. We in IT can assist. We can measure. We can deliver statistical data. Whatever else, compliance to the great majority of emerging standards is not a responsibility of IT, and non-compliance is not IT's fault. Even where IT may adopt responsibility for, say, warning of possible non-compliance, the essential fact is that most compliance is about business process, not about the support mechanisms for these processes.

Before going any further, the first thing that you need in the compliance world is a degree in acronyms. This is because the legislatures have long ago overtaken everybody else in evolving code-speak. In order to avoid using brackets and explaining each acronym I have supplied the translations at the end of this article. Here are a few of the current compliance issues:

- Companies in the UK who think that SOX does not apply to them need to recognise that OFR has appended the UK Companies Act and audits will change in future and statements will be required to be made and to be supported in year-end accounts.
- The FSA demands compliance to PAS56 and other emerging standards for business continuity. Public sector and fire, police, ambulance also adopt this.
- If you are going to process payments, the PCI regulations and standards are a must.
- US companies under the regulation of SEC must be aware of SORPs and will be subject to PCAOB review. More detail within COSO statements and the HIPAA

regulations. Again, as GAAPs become internationally agreed, all of these rules will appear in the UK in like form.

- Help for IT in these non-IT subjects is available from ITCi (UK) and ITTATC (USA).
- IT is not entirely immune but is not legislated. If you are a designer/developer then COBIT awareness and reference to ITIL help keep you right.

Of course, there are hundreds of examples of compliance requirements of which the above are just a few. This brings me to my first balance requirement; gullibility. When somebody storms through your door demanding urgent compliance, first translate statements, then determine legislation and jurisdiction, then decide if, how and when the requirement becomes an IT issue.

There is one other form of gullibility. In terms of the OFR-type stuff, directors and auditors are going to have to make statements that the business is a going concern and that identified risks are under control. Of course, the easy way out is to have IT make the latter statement with their blood. In that circumstance, ask for a seat on the board. Only the directors can assume this responsibility. As I have pointed out, you may report the cheque for a million pounds. You did not requisition it nor did you cash it. IT-enabled warnings are not compliance. The business process to stop that cheque involves humans.

When the gullibility tests have been passed and you believe that IT can help and should help then you have to move through "reasonability". Is it reasonable that imposing some rule or measure from IT will inhibit, reduce or remove risk? By the same token, can extension of the IT disaster recovery plan toward a full-blown business continuity plan be upheld as reasonable?

The two most important aspects of business continuity are communications with the outside world, including press and media, and between and amongst staff and management and people, ie, the company's reliance on them and their reliability in a crisis. Is it reasonable to expect IT to assume responsibility for PR (public relations) and HR (human resources)? What is needed is a balance between what can be done



and what needs to be done -- always modified by an awareness by senior management that none of what can be done by IT is a sinecure.

At the end of the day "liability" is the measure that clears the smog. In every example of a requirement for compliance you can work through the applicability of the requirement to your company. If compliance is required then answer who is liable for non-compliance. What is the exposure? With answers, preferably documented, the IT component can be reviewed and tabled. The IT component will never change the liability. You in IT may well provide control mechanisms, inhibitors, workflow reporting and alerts. You may provide assurances on your security and reliability as delivered by hardware and software. At the end of the day, only board directors are liable. They get your assurance but you don't get on the board. Speaks for itself.

So, juggle gullibility, reasonability, and liability. Do what you can, willingly. Simply be assured that either you become a board director or the worst that can happen is that you lose your job. Those actually liable can lose their house.

Finally, preparation. If you are an ERP user get on to your applications vendor's site and search "Sarbanes Oxley". Hits here tell you what is available mostly on risk management at transaction level. Have a look at products like Qtier that help you subscribe to assurance for extracts. Remember, the database may be accurate but there are users who cannot be taught that OR means start again, and AND means only that and only within the last OR -- (have them draw a flowchart for "I will see you on Tuesday or Wednesday if it is raining"). Get hip to business continuity; your disaster recovery plan is actually the easy part. As ever, the rest of the company assumes that if you can move computers all will be well. Not!

Be a Boy Scout, be prepared.

GLOSSARY

CoBIT: Control Objectives for Information and Related Technology (international).

COSO: Committee of Sponsoring Organisations -- Treadway Commission findings (USA).

GAAP: Generally Accepted Accounting Standard (international).



Midrange Matters

www.campbell-lee.co.uk

HIPAA: Health Insurance Portability and Accountability Act (USA).

ITCi: IT Compliance Institute -- "Compliance is a hidden Opportunity" (UK).

ITIL: IT Infrastructure Library (international).

ITTATC: Information Technology Technical Assistance & Training Centre.

FSA: Financial Services Authority (UK)

Insurance brokers/advisors

Mortgage brokers/advisors

Stock brokers/advisors

Property managers and surveyors.

OFR: Operating Financial Review -- audit guideline (UK).

PAS56: Publicly Available Specification 56 -- Guide to BC Management (UK).

PCAOB: Public Companies Accounting Oversight Board (oversees audits, not accounts, and standards -- not public companies) (USA).

PCI: Payment Card Industry -- data card security (international).

SAS 55 / 78 Statements of Auditing Standards (USA).

SEC: Securities and Exchange Commission -- oversees PCAOB (USA).

SORP: Statement of Recommended Practice (USA).

SOX: Sarbanes Oxley (USA).

Ends.