

Qtier-Rapor: Spreadsheets in Compliance with the Sarbanes-Oxley Act

ABSTRACT

Qtier-Rapor is a framework that enables a business to control, automate and manage spreadsheet processes. This paper is a discussion document on the key features within Qtier-Rapor that correspond to the requirements of a Sarbanes-Oxley audit, in order to demonstrate that compliance and the use of Spreadsheets are not mutually exclusive.

There is a widely held view that business information systems are secure, but that once data is extracted into spreadsheets to consolidate a corporate view, then most of the security evaporates and, if that data is business critical, then compliance evaporates with it.

Whilst no single product can be a complete compliance solution, Qtier-Rapor provides a methodology that, when combined with appropriate procedures, enables Excel spreadsheets to be integrated with corporate data with all of the security, integrity and auditability necessary for compliance with the Sarbanes-Oxley Act.

1 INTRODUCTION

The Qtier-Rapor software framework oversees the security and flow of data through integrated spreadsheet systems. Spreadsheet templates are held in a secure repository, and spreadsheet derived data, can be held in secure, structured, databases to which access can be controlled using formal IT methods. Processes to control data access, input, validation, consolidation, and reporting are all designed in simple steps.

The control of spreadsheets and data, along with control of Excel functions such as 'Save' & 'Print', enable spreadsheet systems to be designed for compliance, and to remain compliant during use.

This document discusses the key features of Qtier-Rapor and the way in which they relate to the requirements of a Sarbanes-Oxley 404 audit.

2 IN A SARBOX ENVIRONMENT, IS IT MANAGEMENT VS USERS?

Section 404 of the Sarbanes-Oxley Act requires management of SEC registered companies to report on the effectiveness of internal controls over financial reporting.

Section 404 also requires the company's independent Auditors to attest to and report on management's assessment of the effectiveness of these internal controls.

"Sarbanes-Oxley implies managers can't ignore un-controlled spreadsheets" [Pettifor B, Eusprig Conference 2003]

"The presence of a spreadsheet application in an accounting system can subvert all the controls in all other parts of that system" [Butler R. 2000]

'End users are putting their companies at risk by setting up spreadsheets without realising that this demands the discipline of traditional programming. Our [KPMG] findings are disturbing, but they are not really surprising, as 78% of models had no formal quality assurance to ensure they were built to specified requirements and were fit for purpose' [Kavanagh J. 1997]

"In order to comply with the Sarbanes-Oxley Act we can no longer use spreadsheets within our business" [Many CFO's and CIO's. 30 July 2002 onwards]

"You can take my spreadsheets from me when you prise them from the fingers of my cold, dead, hands !" [Most Excel users. 2005]

3 SARBANES-OXLEY AUDIT CONSIDERATIONS

A Sarbanes-Oxley Audit Plan should deal specifically with the auditing and control of spreadsheets. The PriceWaterhouseCoopers document *'The Use of Spreadsheets: Considerations for section 404 of the Sarbanes Oxley Act'* illustrates the considerations that auditors must give to spreadsheets.

It says that spreadsheets may be very complex, relying heavily on macros, input from linked supporting spreadsheets, and complicated calculations. 'In these instances such spreadsheets should be treated as software applications in their own right.'

The Audit Plan should address the following key areas:

Access control – limiting access at the file level to spreadsheets on a central server and assigning appropriate rights. Spreadsheets can also be password protected to restrict access.

Change control – maintaining a controlled process for requesting changes to a spreadsheet, making changes and then testing the spreadsheet and obtaining formal sign off from an independent individual that the change is functioning as intended.

Version management – ensuring only current and approved versions of spreadsheets are being used, by creating naming conventions and directory structures.

Segregation of duties / Roles and procedures – defining and implementing roles, authorities, responsibilities and procedures for issues such as ownership, sign off, segregation of duties and usage.

Input data – ensuring that reconciliations occur to make sure that data is inputted completely and accurately. Data may be inputted into spreadsheets manually or systematically through downloads.

Security and integrity of data – implementing a process to ensure that data embedded in spreadsheets is current and secure. This can be done by locking or protecting cells to prevent inadvertent or intentional changes to standing data. In addition, the spreadsheets themselves should be stored in protected directories.

Documentation – ensuring that the appropriate level of spreadsheet documentation is maintained and kept up to date to understand the business objective and specific functions of the spreadsheet.

Development lifecycle – applying a standard Software Development Life Cycle to the development process of the more critical and complex spreadsheets covering standard phases: requirements specification, design, building, testing and maintenance. Testing is a critical control to ensure that the spreadsheet is producing accurate and complete results.

Back-ups – implementing a process to back up spreadsheets on a regular basis so that complete and accurate information is available for financial reporting.

Archiving – maintaining historical files no longer available for update in a segregated drive and locking them as “read only”.

Logic inspection – inspecting the logic in critical spreadsheets by someone other than the user or developer of the spreadsheet. This review should be formally documented.

It is immediately evident that, even if such controls are imposed, normal spreadsheets can be made to fail in almost every area during use; particularly by a user with malicious intent. It should be noted that Sarbanes-Oxley was enacted in the wake of a number of financial reporting scandals where key business data was in error or was manipulated at the very top level of the Corporation.

3.1 Access Control

It is quite possible for a person with malicious intent to find a spreadsheet on a server, and software is readily available across the internet to decrypt spreadsheet protection passwords.

Qtier-Rapor controls access through roles which define common authority for groups of similar users. Individual users are allocated to one or more roles (Figure 1).

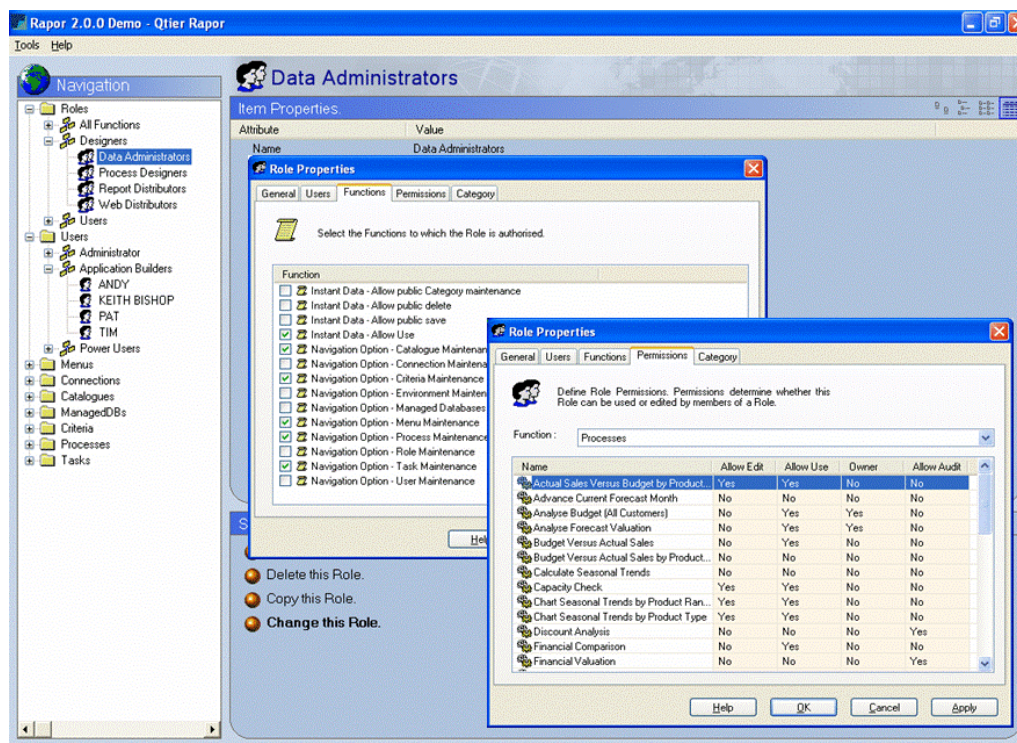


Figure 1

Spreadsheets are accessed by end users through menu structures, system security ensuring that only those spreadsheets to which the user has authorisation will appear on the menu (Figure 2).

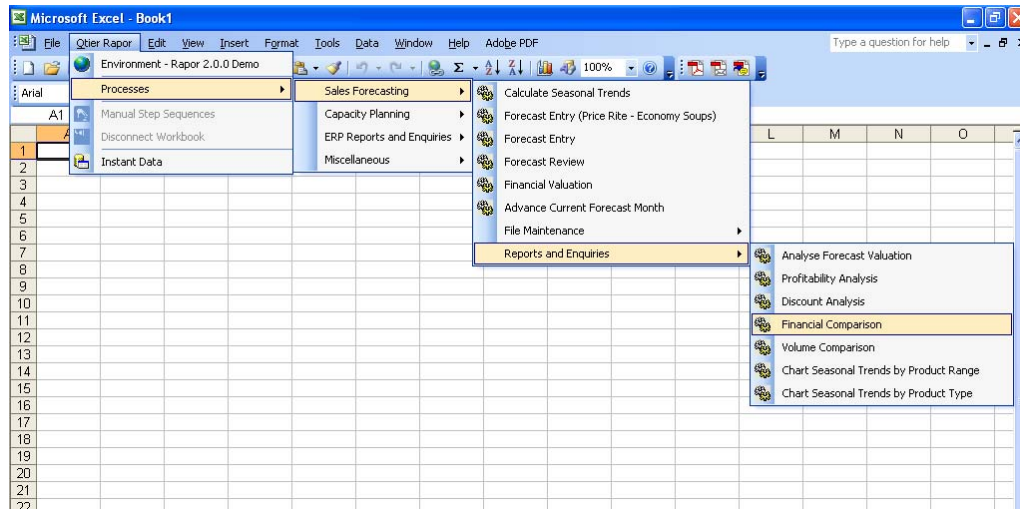


Figure 2

If a user finds a spreadsheet on the server and tries to open it, the template 'knows' that it is controlled by the Qtier-Rapor framework (Figure 3) and still validates access against the user's logon. The spreadsheet is also password protected by a varying, system allocated, encrypted password. Even if the password is decrypted in one instance, and the logic changed, it cannot then overwrite the original template repository without authority.

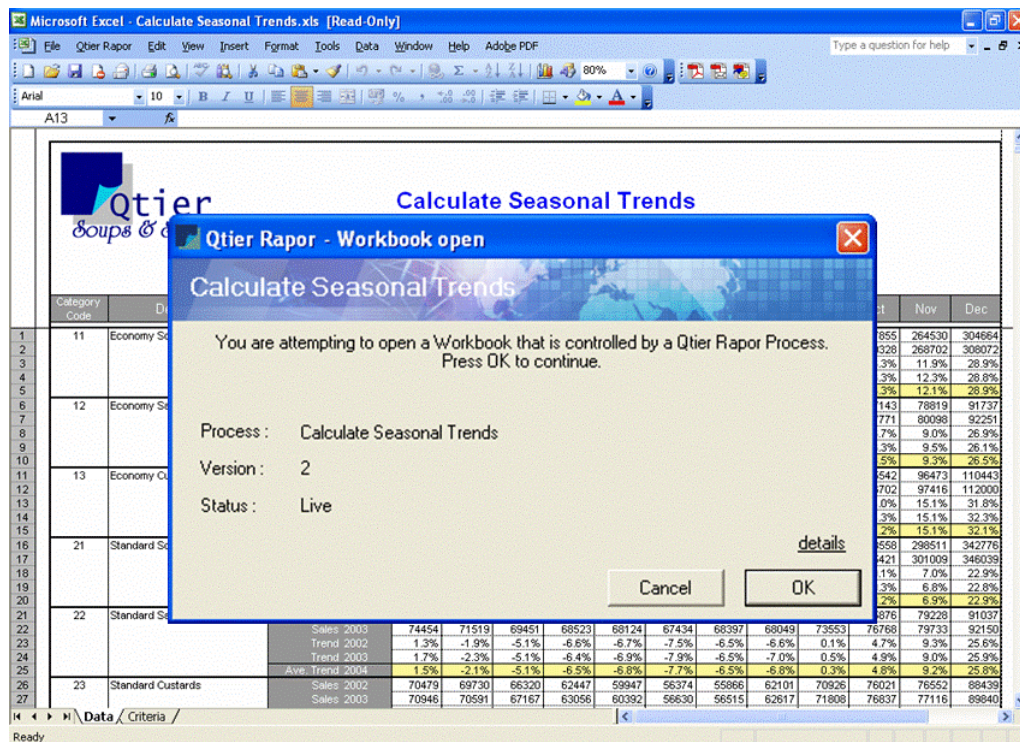


Figure 3

3.2 Change Control

Change controls are circumvented if a spreadsheet can just be amended and resaved under the old name. Within the Qtier-Rapor framework, spreadsheet templates are held in a secure repository. Only authorised spreadsheet ‘owners’ or ‘modifiers’ can access the spreadsheet to modify the design or embedded logic.

Access is security logged automatically, and the new version is quarantined as “work in progress” until tested, audited and authorised for release (Figure 4).

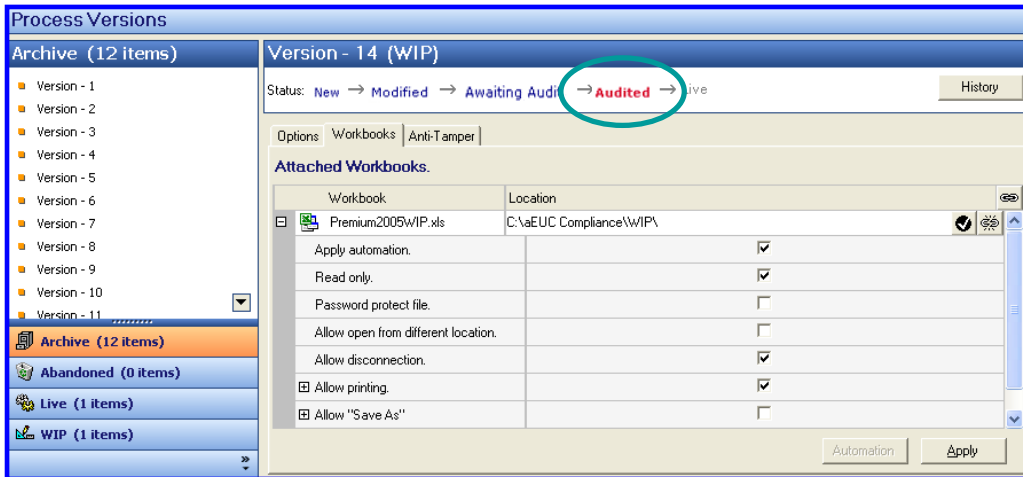


Figure 4

3.3 Version Management

Many versions of a spreadsheet, all with the same name, can exist within a business. As can be seen in Figure 4, old versions are withdrawn and version numbers are incremented when processes are modified. Only the latest approved version of a process is available to users, and previous versions are archived so that the functional logic in use at any time in the past can be examined.

3.4 Segregation of duties / Roles and procedures

Normally, spreadsheets do not know or care who uses them. The corporation can design an authority matrix, but that will not ensure that the procedures are followed. With Qtier-Rapor, every spreadsheet process knows and cares who is (trying to) run it.

Roles are maintained which give authority to spreadsheet processes (Figure 5) and to which Users can be allocated. This extends not only to use of processes, but also to the ownership ‘Owner’, design ‘Editor’ and audit release ‘Auditor’ functions. All of the above is subordinate to security policies implemented on the corporate servers.

Consequently, a defined procedure can be implemented that clearly states, and controls, the authority of individual users, ensuring (for example) that an editor cannot be responsible for audit release of a spreadsheet process.

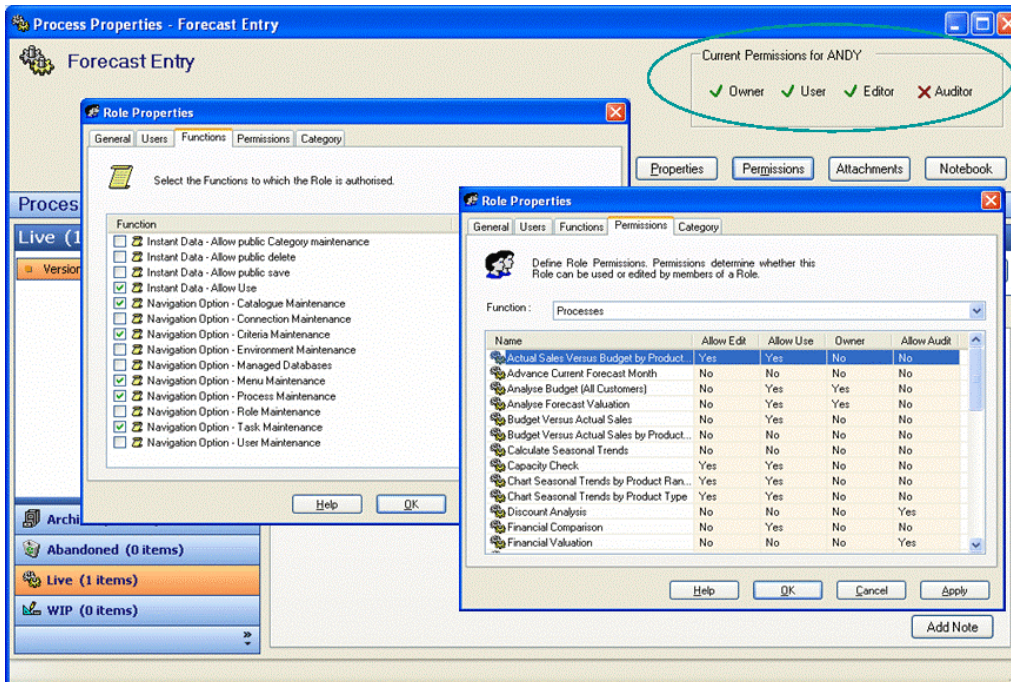


Figure 5

3.5 Input Data

Any system is only as good as the data that is input. Qtier-Rapor ensures that any data that can be obtained automatically from corporate data files is made available to any spreadsheet process without user intervention. This ensures that all users access the same data and that there is ‘only one version of the truth’.

Data derived from a process can be written to Qtier-Rapor’s User Defined Database (UDD) for retrieval by subsequent processes. Dependency checking ensures that processes reliant on the completion of previous operations (such as consolidation) cannot progress until those operations are completed.

All spreadsheets can contain validation ranges on input cells, but sometimes entries can be individually valid, but give rise to a combination of circumstances that are invalid. Qtier-Rapor can maintain global ‘reasonable ranges’ of expected results against key indicators within the UDD. Spreadsheet processes can then perform a reasonability validation against those key indicators and take appropriate action. These global validation checks can be absolute, or allow values to fall within a range, with appropriate logic embedded in the step design to respond to out-of-range results (Figure 6).

This test of reasonableness has been previously identified by EuSprIG as a key factor in validation of data entry in spreadsheets.

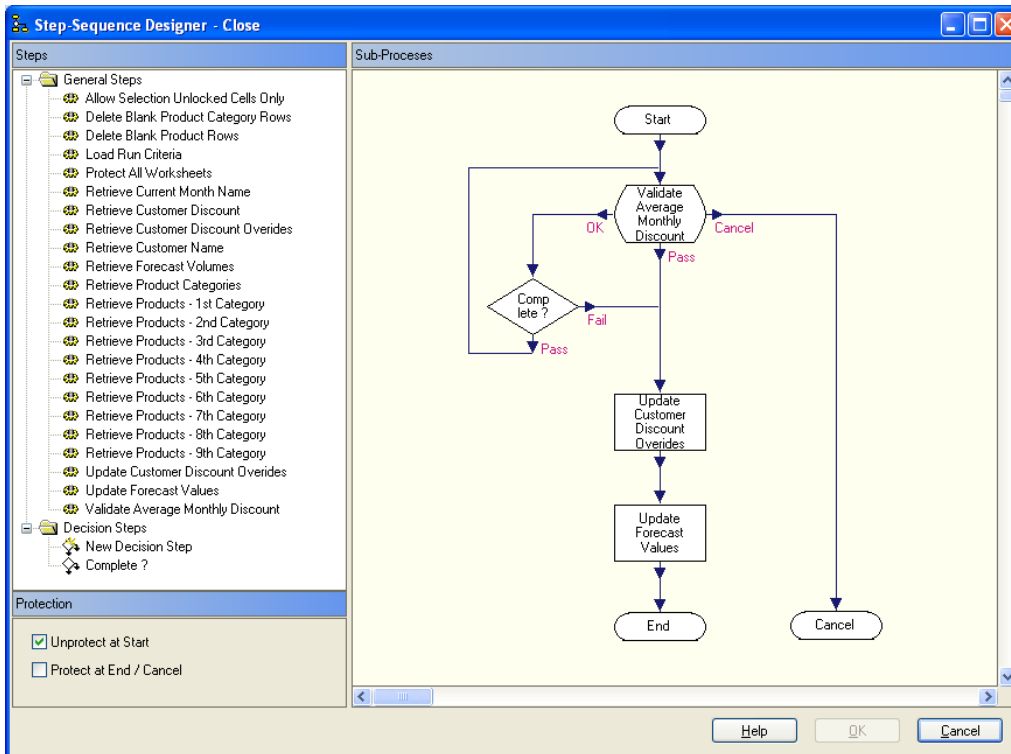


Figure 6

3.6 Security and integrity of data

Only one current spreadsheet template can exist at any one time for any one process, and it is secured against tampering by locking with a system generated encrypted password. This ensures that the process logic is unchanged since it was audited and released.

Each template can access data direct from the corporate database, or from the User Defined Database (UDD), using formal IT methods through a Connections and Catalogues system. This ensures that the data is absolutely current. The spreadsheet templates are themselves stored in a secure repository.

All actions are audit logged showing the process used, criteria selected at the time, user, computer ID and timestamp (Figure 7).

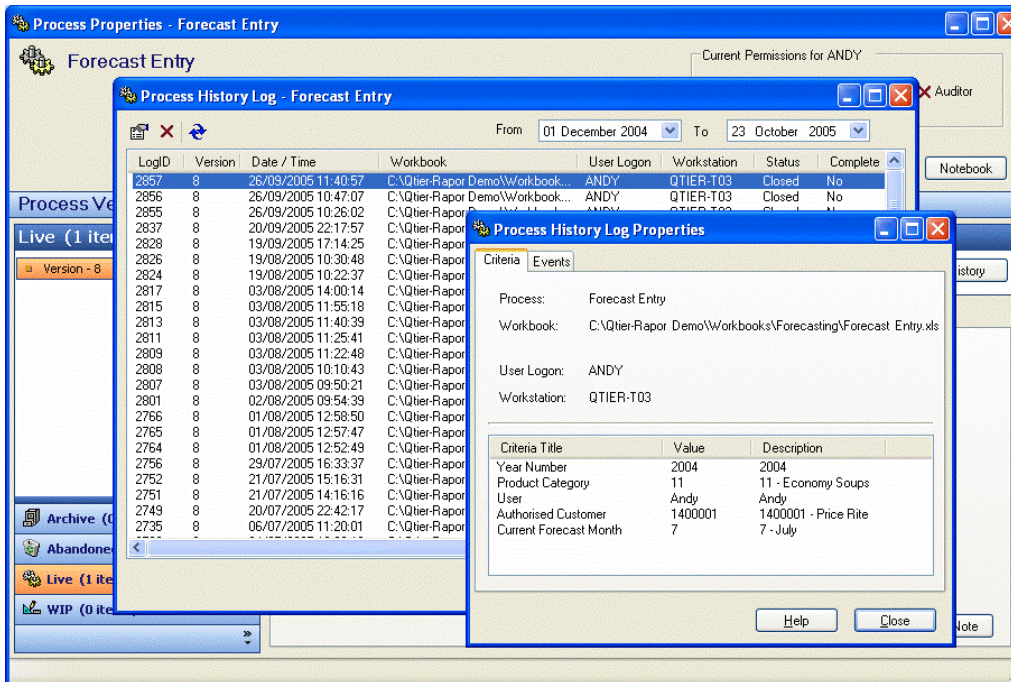


Figure 7

3.7 Authentication

Rigorous authentication of printed output from spreadsheets is not normally possible. It is easy to save a copy of a locked spreadsheet or even copy and paste it onto a new sheet, then amend the formulae, change the data and re-type any timestamp information to make it look exactly like the original version.

Qtier-Rapor can disable the Save, SaveAs, and Cut&Paste options in Excel. A special feature can embed a unique, non-reproducible, authentication stamp that corresponds to the security log entry into any printed material.

This means that spreadsheets cannot be duplicated (other than by complete re-typing), and any screen-prints or cut & pasted 'copies' cannot have the authentication stamp. The management, and auditor, can be assured that the report being examined is a validated output of the system.

3.8 Documentation & Development Lifecycle

All spreadsheets placed under the control of the Qtier-Rapor software framework become largely self documenting. The Qtier-Rapor database contains all key spreadsheet meta-data, and the detail of each step and logic diagrams for each process. Where additional spreadsheet process control documentation is required this can easily be defined and maintained within the Rapor database by any authorised user. Process documentation is updated along with the spreadsheet design. The framework lends itself to the normal IT disciplines of application development.

3.9 Backups & Archiving

Creating back-ups and archiving old spreadsheets places a heavy reliance on user initiated processes. Qtier-Rapor ensures centralisation and the structured organisation of spreadsheet processes. Once under the control of Qtier-Rapor, the location of all live spreadsheets can be automatically communicated to those responsible for backup procedures.

Where critical data sits in a number of spreadsheets in a variety of locations, it is rarely possible, without extensive effort, to ensure effective back-ups. The Qtier-Rapor framework provides the features to save such data into structured IT databases in known locations. These can be backed up and archived on the server, as in any IT application, without relying on the user.

3.10 Logic Inspection

Qtier-Rapor instils the discipline of best practice programming into 'spreadsheet modifiers'. This is achieved by dividing processes into small steps and assembling them within a visually displayed logic diagram. Peer review is made easier, as is audit.

No claim is made that Qtier-Rapor can validate spreadsheet logic – that is the province of other tools and techniques available. However, once logic processes are embedded they are locked and not subject to amendment unless under change and version control.

4 SUMMARY

Excel spreadsheets are uniquely flexible to meet the demands of modern accounting and reporting, where information is needed quickly, and adaptability is the key to business speed.

However, uncontrolled flexibility and the ability to manipulate data manually, means that no information has provenance – But provenance is what is demanded by legislation that seeks to instil rigid process and control over financial reporting. One of the biggest holes in 404 compliance occurs when business-critical information is held in spreadsheets.

Many corporations that need to demonstrate compliance to the Sarbanes-Oxley Act are giving consideration to banning the use of spreadsheets for critical data areas. They are implementing reporting tools with a rigid pre-defined structure – but where does the data originate? How many companies don't feed their budgets from spreadsheets? How many don't extract their forecasts to spreadsheets?

How to square the circle? Users need to retain flexibility by retaining Excel as their working tool – But management needs to control, authenticate and monitor the logic, inputs and outputs to the same degree as a formal IT system.

The Qtier-Rapor framework wraps itself around the whole spreadsheet process to provide all of the elements necessary to allow users the flexibility of a spreadsheet interface, but to deny them the opportunity of breaking the provenance and integrity of the business-critical data that they produce.

Sarbanes-Oxley compliance is about making executives more accountable for their information.



Sarbanes-Oxley IT audits are about ensuring systems are more secure to support compliance.

Qtier-Rapor is about making Excel spreadsheets as compliant as any other IT system.

5 FUTURE PERSPECTIVE

Use of spreadsheets as a tool is a 'must have' for anyone involved in finance. Imposition of additional workload on any aspect of the use of such a tool will encourage users to look for ways to subvert the process. Qtier will continue to enhance the usability and power of functions, in order to ensure that design of spreadsheet systems is undertaken within the Qtier-Rapor framework as a matter of choice rather than mandate.

Current development includes:

- More advanced automation techniques for the 'batch' disconnection and re-connection of spreadsheets outside of the Qtier-Rapor framework.
- Automated spreadsheet drill-down facility.
- Integration of other Microsoft Office end user computing productivity tools.

6 REFERENCES

'The Use of Spreadsheets: Considerations for section 404 of the Sarbanes Oxley Act'. Available for download from PriceWaterhouseCoopers 'Sarbanes-Oxley Information Centre at <http://www.cfodirect.com> , 14:08 8/03/2005.

Butler R., *'The Subversive Spreadsheet'*, EuSpRIG Website www.eusprig.com 12:30 10/03/2005

Kavanagh J., article in Computer Weekly, July 1997

Pettifor B., The EuSpRIG Conference, 2003

CONTACT:

BvW Technology
310 George Street
GPO Box 311
Sydney NSW 2001
Australia

Tel: +61 (02) 8011 3670
Email: info@bvwglobal.com

