BWise
BUSINESS IN CONTROL

The Role of Continuous Monitoring and Auditing in GRC

The role of Continuous Monitoring and Auditing in GRC

A business in control is the starting point for most people in business. Without being in control, it becomes impossible to achieve long term ambitions and execute on strategy. Senior management, employees, shareholders, suppliers are looking for means to achieve long term prosperity. Recent market developments have clearly shown this can only be achieved by businesses in control. Despite regulations and corporate governance codes, many businesses find themselves in the undesirable situation of not being in control. Regulations are often focused narrowly and codes are at best non-descript or even vague. This will result in significant efforts and initiatives or high level management reports that do not add value; ultimately, not achieving the goal of bringing the business in control.

In this white paper, we discuss means to gain control, with modern techniques. We will demonstrate how the world of Governance, Risk Management and Compliance is now integrated with the world of Continuous Monitoring and Continuous Auditing. Rather than testing every potentially irrelevant control, this integrated approach ensures a focus on things that matter. Rather than focusing on compliance, we help to focus on business performance, with compliance as the end result, including required reporting and evidence.

Throughout this paper, we will give you real, live business cases to demonstrate how your enterprise can improve business, manage risks and demonstrate compliance. Effectively, we will show you how to get in control once again.

Continuous Control

Traditionally, in order to ensure compliance, the focus of internal and external auditors has been on the effective design and operating effectiveness of controls. Given the size and complexity of the modern organization, the need for structure and automation emerged decades ago. Current market nervousness and regulatory initiatives are driving the need for immediate compliance insights even further. Rather than waiting for scheduled audits in the distant future, companies want to monitor the pulse of their organization continuously, but , they do not want to spend more to accomplish this, they want to spend less.

In addition, keeping in mind what regulators will allow, more mature companies are taking a risk based approach. This implies they adopt risk management standards like ISO 31.000, the OCEG framework, the AS/NZ 4360 standard or COSO ERM. Adopting a risk management approach helps to focus on what really matters, and what the real threats and opportunities are. It helps to identify key risks, to define appropriate risk responses with correct measures where needed, and ways to monitor. This is where risk management and compliance meet. Risk management is a management tool, that when properly implemented helps to steer the company.

Ideally, compliance is an element of risk management that not only is used to demonstrate adherence to external and internal rules and regulations, but in addition helps to manage the key risks in the company. These efforts will also result in asking the question of whether or not the business is in control.

Many worlds

With this in mind, it is interesting to see that many organizations have different departments implementing their own approach to Governance, Risk Management and Compliance (GRC).

The IT department monitors IT controls, and digs for information from a multitude of sources to manage data security, business continuity, data privacy and more. Internal audit has its own independent view; implementing the third line of defense. Risk management is defining risk templates and appropriate

measures to manage corporate risks. The compliance department is keeping track of regulatory requirements and defines policies and procedures for the organization to adhere to. The finance department manages compliance with financial standards such as IFRS, US GAAP, tax regulations and if a publicly listed company, compliance to Sarbanes-Oxley, Bill 198, IKS, Tabaksblat, J-Sox, C-Sox and more.

Three main trends are visible today:

1. Convergence of all these efforts into one integrated approach

2. Reduction of the costs of compliance

3. Improving the relevance and accuracy of the risk and compliance information

These three trends are strongly related. When properly converging different initiatives into one integrated approach, costs reduce substantially and the quality of information increases dramatically. In another BWise white paper on “The Value of Process Management”, the value of convergence to organizations is discussed.

The second trend, that of cost reduction, is clearly driven by the current market conditions. Keeping that in mind, most organizations still spend far too much on risk management and compliance for what they get from it. Reduction of costs should be on every manager’s agenda, regardless of economical conditions, certainly given the current low quality of information that organizations are using.

The third trend that is observed, is that organizations must try to improve the quality and relevance of its risk and compliance information, not the quantity. Increasing the amount of information in most cases is not needed, due to the mind boggling amount of manually maintained spreadsheets that some enterprises already maintain. Organizations also spend a great amount of effort to ensure the audit trail is maintained, data is correct and reports are generated. As a result, external auditors, board members and senior management then need other means to be in control of their business, which renders the entire spreadsheet approach utterly useless and expensive. Companies are now looking for other ways of getting in control of all the diverse activities in this area at a lower cost than they already spend today.

Governance, Risk Management and Compliance

The first step in an integrated approach is to understand how the organization is structured and how business is done. For many, this feels like a huge documentation task, possibly because of past experiences like Sarbanes-Oxley or large ERP implementations. This perception is incorrect, you only need the important stuff. Using a risk-based approach, only the relevant subjects are captured.

An enterprise should continuously ask itself the question, “What could go wrong if this information was not properly documented?” It is surprising to see what happens to the amount of documentation if this question is asked continuously. Starting with key objectives and key risks, and opportunities related to these risks, an initial risk assessment will show the most important areas of risk (and opportunity). From there, measures can be taken to mitigate risks, to design processes and controls, but most importantly, only for those things that really matter.

***Figure 1**. Risk – based approach*

Other BWise white papers delve deeper into the methodology of managing risks and compliance projects in an integrated fashion. The value of genuinely understanding business processes at the right level is also presented.

Continuous Monitoring and Auditing

In this white paper, the focus is on Continuous Monitoring and auditing. Once it is clear what the key risks are and the risk response is, it is necessary to monitor them. For the sake of clarity, it can be relevant to differentiate between various types of risks, see table 1 below.

	Financial Example	Safety, Environment, Health Example
Risk of non-performance	Long lead times of Order to Cash process potentially causes cash issues	Safety incidents cause absence reporting to increase
Risk of non-compliance:		
Internal non-compliance	Sending incorrect invoices causes extra costs and damage to reputation	The use of paper is minimal and only environmentally friendly paper is used
External non-compliance	Lacking sign-off of contracts potentially causes incomplete revenue statements	Spillage of oil causes non-compliance with applicable laws

Note that the risk of internal non-compliance in some cases will have a relation of risk of non-performance.

Normally, management will have defined policies and procedures to increase their performance, and reduce the likelihood of damage to reputation. Today, most Continuous Monitoring projects focus on just financial non-compliance (the green cell in the table above). It is clear that a lot more can be accomplished and as aresult much business benefit can be achieved.

Real Business Examples

Consider the following examples of how Continuous Monitoring can help to improve or sustain the level of 'in control' within your organization:

Managing Customer Credit
Inappropriate maintenance and monitoring of customer credit, combined with the incentives of sales personnel to maximize sales can lead to significant risks in revenue. Systems can help to reduce that risk by providing Application or IT dependent controls. To control customer credit, usually a mix of controls is present in a system that consists of the following types:

- Customizations (system settings that prevent misuse, inappropriate data-entry, checks etc.),
- Authorizations (system function usage is limited to the appropriate personnel) and Reports (system generated lists of exceptions/alerts that need manual follow-up).

In the example of customer credit management, the following controls with considerations, can be setup in most ERP systems:

- (Customization) For each customer in the system, a credit limit can be assigned. If no credit limit is setup for a customer, no system check will be applied. If the credit limit is set too high, it will be ineffective.
- (Customization) When creating a sales order, the total amount of outstanding sales (goods issued but not yet paid) and the newly created order can exceed the customer credit limit, results in the created order will be blocked for delivery.
- (Authorizations) A limited number of people can change credit limits, release blocked sales orders, create new sales orders, create goods issued etc. Certain critical segregation of duties conflicts such as creating sales orders vs. releasing blocked sales orders should be resolved.

- (Reporting) There might be cases where releasing sales orders in excess of the credit limit is desirable (e.g. customer provides bank guarantees). There should be system generated reports that help to identify the current outstanding sales against the customer credit limit (credit exposure) for periodic review of over exposure.

Being 'in control' is only one aspect of Continuous Monitoring. In many cases controls in any system also provide a means to improve the effectiveness of your operation while reducing risks. Consider the following example:

Days Sales Outstanding (DSO)
Non-timely invoicing and inappropriate follow-up on long outstanding sales by dunning results in a loss of interest, limitation of cash in hand and eventually an increased risk of non-collectibles.

Appropriate monitoring of outstanding sales will limit these risks and inefficiencies:

- (Customization) In the system, each customer has a base payment term. The system is automatically setup to apply this payment term to any invoices sent to the customer. If the invoice is still outstanding a certain number of days after the due date has passed, it will automatically be positioned on the dunning list.

- (Authorizations) A limited number of people can change customer master data (including payment terms), create credit memo/invoice cancellations.

- (Reporting) There is a periodic review of a system generated report that provides acceptable insight into the DSO, upon which the invoicing department can act if inappropriate payment terms are used by customers.

During manual system checks/audits some of these controls can be checked without the use of tools (although taking more time). There are however, situations in which the analysis of large amounts of data provides more accurate assurance than manual checks will. Consider the following example (SAP specific, but some apply to other systems as well):

Three-Way-Matching
When receiving an invoice, it is automatically matched against a goods receipt. The quantities and prices are verified. If differences occur larger than the set tolerance limits, the invoice will not be released for payment, if with acceptable limits it will automatically be released for further processing.

- (Customizing) Three-way-matching is only performed if the correct system settings (tolerance limits) are set within the system.

- (Customizing) The three-way-match applies only to suppliers that have the GR-based-IR value set correctly on their master data record.

- (Authorizations) A limited number of people can release blocked invoices for payment if tolerance limits are exceeded.

- (Reporting) Three-way-match is only applied if the goods receipt is booked with a reference to a purchase order. If not, no three-way-match is applied. There is a periodic report that gives an overview of all goods receipt without a reference to a purchase order(movement-type 501).

- (Authorizations) A limited number of people can post/release goods receipt without a reference to a purchase order.

To provide a reasonable level of assurance you would have to check all of these settings/reports/authorizations manually and periodically, which can take a significant amount of time and because of the elaborate number of steps, can be prone to errors.

BWise Continuous Monitoring

The BWise Continuous Monitoring (CM) solution has been engineered as an open solution capable of capturing and analyzing data from any open application and data source. This includes all major ERP systems such as SAP, Oracle, JD Edwards, PeopleSoft and others. The high level structure of the BWise solution for GRC with CCM is shown in figure 2.

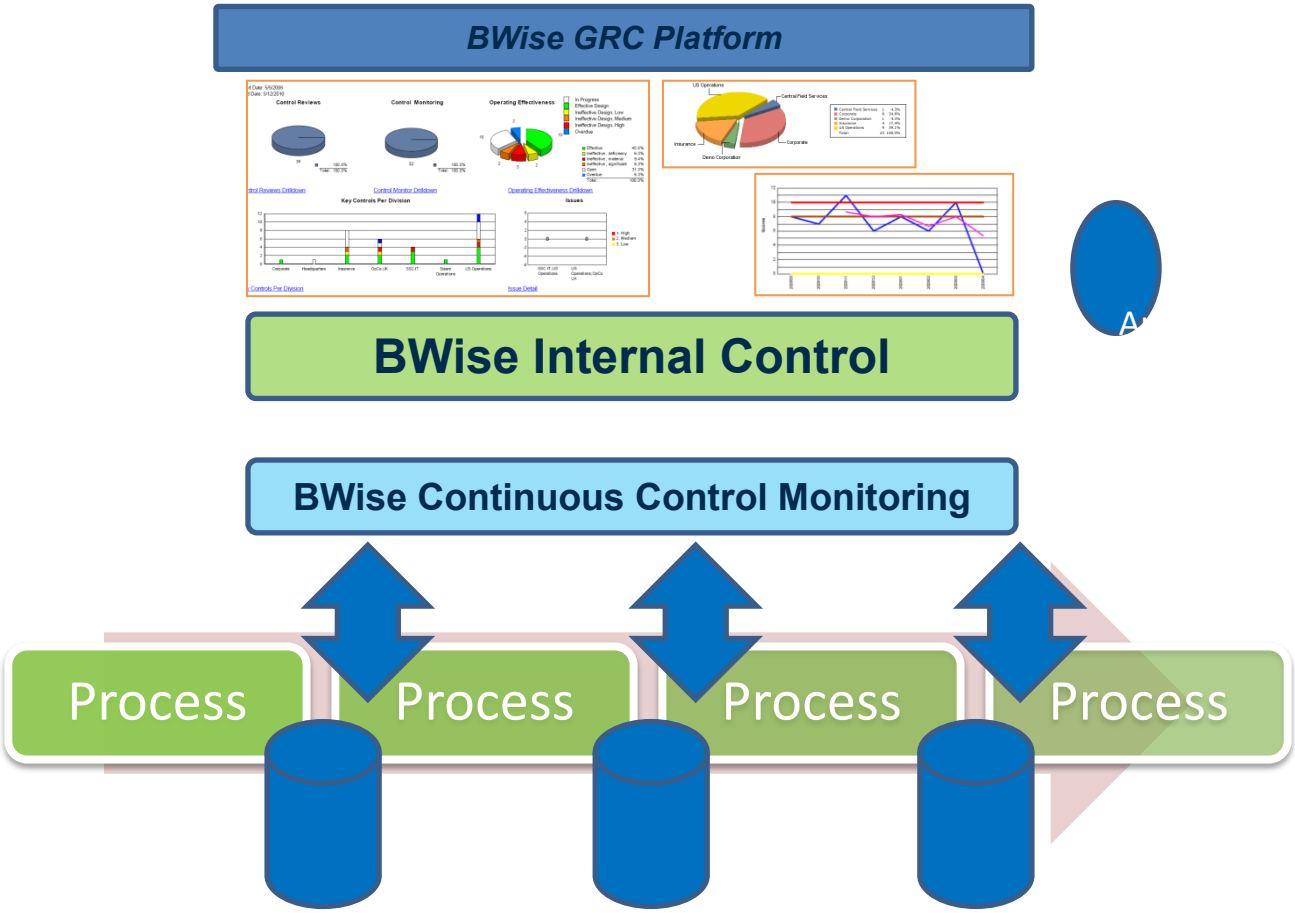

Figure 2. *High level structure of the integrated BWise GRC & CCM solution.*

On a more technical level, the BWise architecture for Continuous Monitoring looks like Figure 3 below.

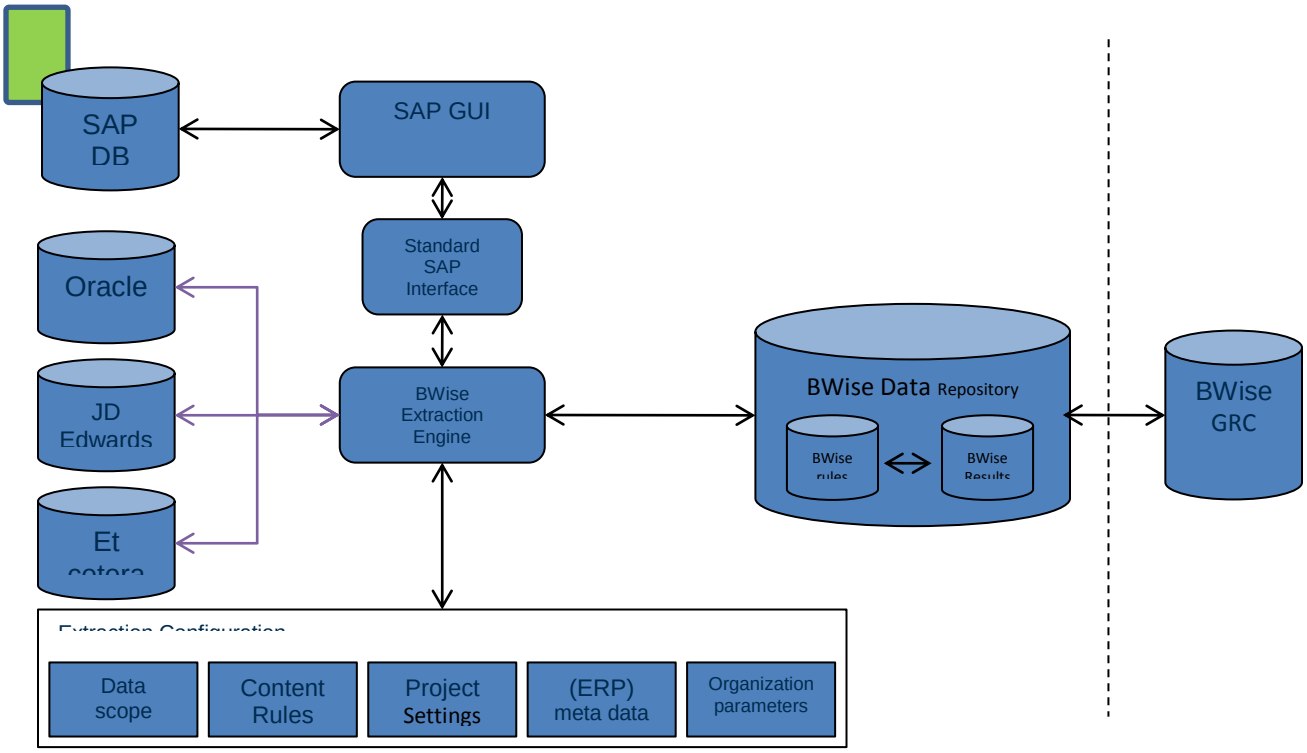

Figure 3. *Architecture of BWise Continuous Monitoring with BWise GRC.*

Figure 3 above shows BWise CCM is purposely built as an open engine, leveraging the strongest data integration engine available, based on Business Objects technology, this also ensures certified and scalable data retrieval. Based on the data retrieved, rules are executed whenever required. Rules may take random samples of the data, but typically look at the full data set and report exceptions to the BWise GRC solution. In the solution assigned users are alerted by for instance an email to take appropriate actions, perform reporting and view evidence. BWise keeps a full historical trail of all exceptions data, while pushing exception reports into BWise GRC for reporting and auditable evidence.

BWise Continuous Monitoring Templates

Based on years of experience in process improvement, audit, ERP implementations and most importantly, risk management and compliance implementations, BWise has also developed templates that help organization to jump start their monitoring efforts. This can dramatically reduce ramp-up time, and will quickly reveal where the biggest pain points are.

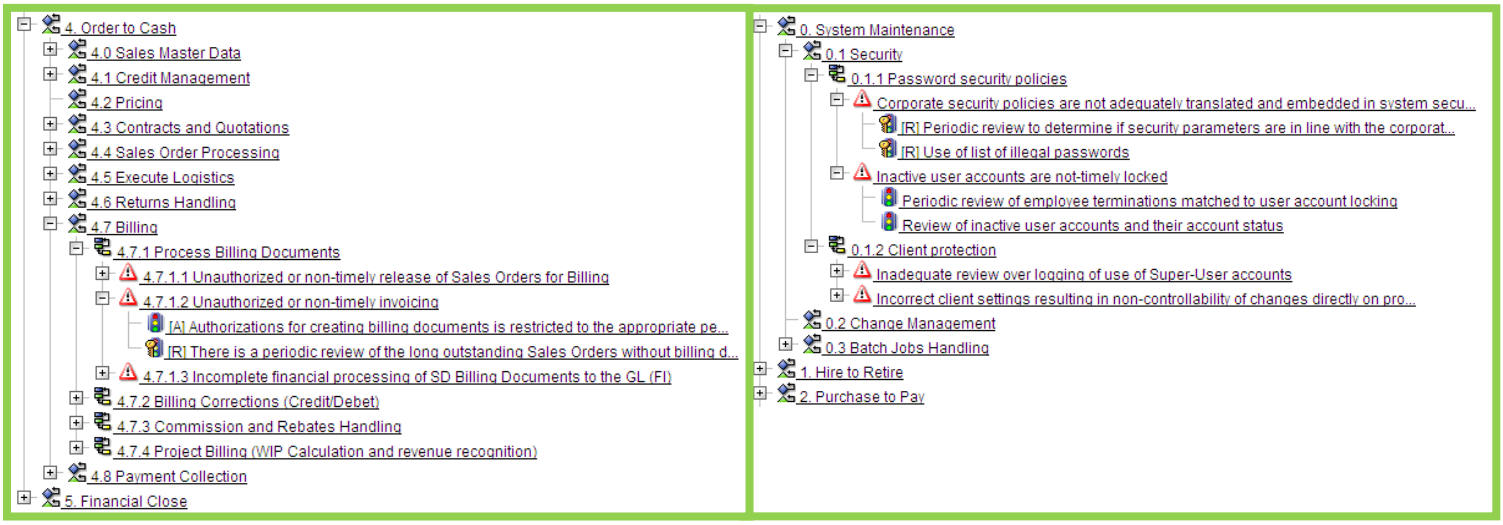

Figure 4. *Sample template in BWise GRC for Continuous Monitoring*

The screenshot above shows a part of the template that BWise offers. This template not only names the controls, but also includes the relevant rules to retrieve and analyze the data from an ERP system, such as SAP, and reports exceptions to the BWise GRC solution. This is a unique capability that will help companies to quickly reap benefits from BWise CCM. No other GRC platform offers this level of integration between high level risk & control frameworks and actual data analysis and evidencing.

Rules

A lot has been said about rules engines, and many very advanced engines have been developed. Most of these solutions require extensive training, expert knowledge and very specific programming skills. This makes a roll-out very expensive and highly dependent on external experts. BWise takes a different approach, as BWise believes the data is the starting point. In other words, the correct data needs to be retrieved. This means the raw data, not the standard reports that SAP and other ERP systems provide. Any auditor will tell you that these standard reports are not necessarily correct or complete. This implies we need world class data retrieval capabilities.

Once we have the raw data, it needs to be organized and presented in an orderly fashion. This is done by the BWise CCM solution. And once data is organized, analysis is quite forward; rules are very basic and can be stacked, allowing auditors to clearly see and understand what the rule is. Most other CCM solutions retrieve data and perform all sorts of data cleansing and data transformation actions, making it very hard to track down what really has happened. BWise believes this needs to be done in one clear step. Next, by using standard MS Excel capabilities, the definition and maintenance of rules becomes especially simple. All exception data is safely kept for future reference and trend analysis, ensuring ease for audit in the future. Moreover, any business analyst can build and understand rules, BWise finally brings Continuous Monitoring to business owners. Continuous Monitoring and GRC together become Business Optimization and assist an enterprise to get in control.

About BWise

BWise, established in 1994, is the global leader in Enterprise Governance, Risk Management and Compliance (GRC) software. Based on a strong heritage in business process management, BWise delivers a truly integrated and proven GRC platform. With this platform, BWise supports an organization to track, measure and manage key organizational risk in one integrated system. By doing so, BWise helps customers to be truly in control by sustainably balancing their performance and risks. BWise also enables it customers to increase corporate accountability; strengthen financial, strategic and operational efficiencies; and maximize performance, while understanding risks. Using BWise, organizations are able to comply with regulations such as Sarbanes-Oxley, ISAE3402/SAS-70, PCI, Solvency II, Basel II and III, Dodd-Frank, ISO-standards, European Corporate Governance Codes and many more.

BWise provides for the GRC needs of hundreds of customers, worldwide, across all industries. Customers include AEGON, AngloGold Ashanti, Connexxion, Health Alliance Plan (HAP) of Michigan, LeapFrog, Liebherr, Marathon Oil, Southern Company, Swiss Life, TNT and Transcontinental. BWise has offices in the Netherlands, United States, Germany, France and the United Kingdom. For more information, visit www.bwise.com.

BWise offices

BWise Headquarters
Rietbeemdenborch14-18
5241 LG Rosmalen
P.O. Box 321
5201 AH Den Bosch
The Netherlands

Tel: +31 (0)73 – 6464911
Fax: +31 (0)73 - 6464910

BWise
"The Gherkin"
30 St. Mary Axe, 28th – 29th Floor
London, EC3A 8BF
United Kingdom

Tel: +44 (0)20 7469 4049
Fax: +44(0)20 7469 4001

BWise Germany GmbH
Kaiserswerther Strasse 115
40880 Ratingen
Germany

Tel: +49 (0)2102 420 663
Fax: +49 (0)2102 420 62

BWise Inc.
1450 Broadway, 38th Floor
New York, NY 10018
USA

Tel: +1 212-584-2260
Fax:+1 212-730-6918

BWise
19, boulevard Malesherbes
75008 Paris
France

Tel: +33 (0) 1 55 27 37 28
Fax:+33 (0) 1 55 27 37 00

www.bwise.com

Disclaimer