

Making sense of internal control:
How to align vision, organisation and technology to lower
your compliance costs and improve business efficiency.



© 2010 PricewaterhouseCoopers. All rights reserved. PricewaterhouseCoopers refers to the network of member firms of PricewaterhouseCoopers International Limited, each of which is a separate and independent legal entity.

PricewaterhouseCoopers (www.pwc.com) provides industry-focused assurance, tax & legal and advisory services to build public trust and enhance value for our clients and their stakeholders. More than 163,000 people in 151 countries across our network share their thinking, experience and solutions to develop fresh perspectives and practical advice.

PricewaterhouseCoopers and PwC refer to the network of member firms of PricewaterhouseCoopers International Limited (PwCIL). Each member firm is a separate legal entity and does not act as agent of PwCIL or any other member firm. PwCIL does not provide any services to clients. PwCIL is not responsible or liable for the acts or omissions of any of its member firms nor can it control the exercise of their professional judgement or bind them in any way. No member firm is responsible or liable for the acts or omissions of any other member firm nor can it control the exercise of another member firm's professional judgement or bind another member firm or PwCIL in any way.

Introduction

In September 2009, PricewaterhouseCoopers hosted a two-day event entitled “Reliable systems and processes: Secure enough to succeed?” The aim of the event was to increase transparency in the Swiss marketplace for next-generation control solutions. This white paper documents and communicates the findings of the event for the benefit of the internal controls community.

At the event, internal control officers from leading Swiss companies participated in round table sessions to discuss and understand each other’s challenges and planned developments in internal controls systems. They also talked about the expectations these raise in terms of next-generation control solutions and their vendors. Most of the companies that participated are listed on the Swiss stock exchange, and many are also listed on one or more foreign stock exchanges.

To provide insight into the current and future capabilities of next-generation control solutions, leading vendors were invited to showcase a customer project where they had implemented their control solution. Most presentations were done by, or together with, the customer.¹

An open discussion took place among vendors, participating companies and PwC’s internal control specialists to compare customer cases with the key expectations expressed by the internal controls officers in the round table sessions.

This white paper reflects on the results of the event and seeks to answer some of the open questions that remained at the end of the event. It is structured in three parts:

- Part I: The internal control system that you want – How Swiss companies want to further develop their internal control systems and the key strategies to achieve this.
- Part II: Smart use of internal control technology – The expectations in the market, current capabilities of control solutions, and how to leverage internal control technology.
- Part III: Next generation control solutions – The views of control solution vendors on how their control solutions fulfil the expectations of internal control officers.

On behalf of my colleagues at PricewaterhouseCoopers who helped make this event happen, I would like to thank the participants, vendors, their customers and the keynote speakers for their contributions. This was a unique event, and we look forward to creating further opportunities for the Swiss internal controls community to share and collaborate in a similar manner.

Yours sincerely,

Paul de Jong
Partner PricewaterhouseCoopers AG

¹ The following vendors participated in the event (in alphabetical order):

■ Approva ■ Bwise ■ Conteliga ■ Oracle ■ Runbook ■ Security Weaver

Vendors were selected based on our observations of current market developments and on their willingness to participate at our event. The presence of these vendors at the event should not be understood as a recommendation. Any software selection should be based on a thorough selection process, considering all relevant client specific requirements. The contents of this white paper are based on the outcome of the event, and not on any further research, e.g. to substantiate any statements of the participating software vendors.

Contents

Executive summary	5
Part I: How to get the internal control system that you want	6
Development goals and challenges in internal control systems	6
Control vision and a “back to basics” organisation	7
The people factor: Are your key stakeholders “pigs” or “chickens”?	11
Part II: Smart use of internal control technology	14
Expectations placed on control solutions	14
Which control solution for what purpose?	15
Use the technology that best fits your control vision	15
Implementing next-generation control solutions	19
Part III: Next-generation control solutions	22
Acknowledgments	30

Executive summary

Many companies want to transform their control activities from a burdensome requirement to measures that contribute to process efficiency and cost reduction. There is a strong tendency in the marketplace to look to software solutions to drive the optimisation of internal control systems. However, there are also reservations as to the maturity and ability of such solutions to fully enable a company's internal control strategy.

Several vendors offer what we will refer to as next-generation control solutions. These solutions are commonly marketed as governance risk and compliance (GRC) automation, GRC management, enterprise risk management, and continuous (controls) monitoring solutions. As evidenced by successful implementations at various companies, software solutions can support the optimisation of internal control systems. At the same time, however, failed implementations at other companies are evidence that software solutions alone cannot drive the optimisation of internal control systems.

The conditions for successfully developing internal control systems are:

- A clear vision of internal control: Automating an intelligently designed internal control system will lead to a highly effective and efficient internal control system. Automating an inefficiently designed internal control system will lead to an automated, but inefficient, internal control system. An intelligent design incorporates a top-down approach enabled by technology.
- Commitment supported by clear roles and responsibilities at all organisational levels: Only with the appropriate commitment on the part of senior decision makers and appropriate involvement of crucial influencers and experts within the business can a change to the internal control system be effected.

The question of which software solution fits best is best answered with the company's control vision in mind. The breadth and depth of functionality provided differs considerably from one software solution to the next. Each has strengths and weaknesses that need to be understood to fully appreciate the applicability of each solution in a specific company context.

“Key to developing internal control systems are a clear vision, commitment from the business, and clear roles and responsibilities.”

The implementation of the selected software solution can only be fully successful if it is driven as a change initiative, with all the right people committed and involved appropriately. The software solution needs to be integrated into the business in such a way that it makes people's jobs easier.

The implementation should not be allowed to become a burden in itself. This requires a structured implementation approach and a good sense of awareness of the common pitfalls in projects of this type.

A well thought-through control vision, committed to and supported by the business and based on the right technologies properly implemented, make for a best-in-class control solution that ensures compliance with control requirements and contributes to process efficiency and cost reduction.

Part I: How to get the internal control system that you want

Development goals and challenges in internal control systems

Since 2008, larger Swiss companies have been required to implement an internal control system over financial reporting. Many organisations found their first implementation unsatisfactory and requiring subsequent optimisation. Their experience has also been that an internal control system is dynamic and needs to be continuously maintained in alignment with market, organisational, legal, and technological developments.

The PwC maturity model for internal control systems, as shown in Figure 1, provides high-level directions for the development of an organisation's internal control system.

This maturity model provides a high-level overview, however, developing internal control systems requires more detailed considerations. Internal control systems have many dimensions, each with options to be considered to provide the best fit within the given context and strategy. These dimensions must fit together in conformance with the company culture and management structure. In addition, the resulting internal control system must be adaptable to accommodate a dynamic business environment.

For illustrative purposes, some dimensions and related options are shown below in Figure 2.

For instance, companies could consider extending the scope of their internal control system to go beyond Internal Control

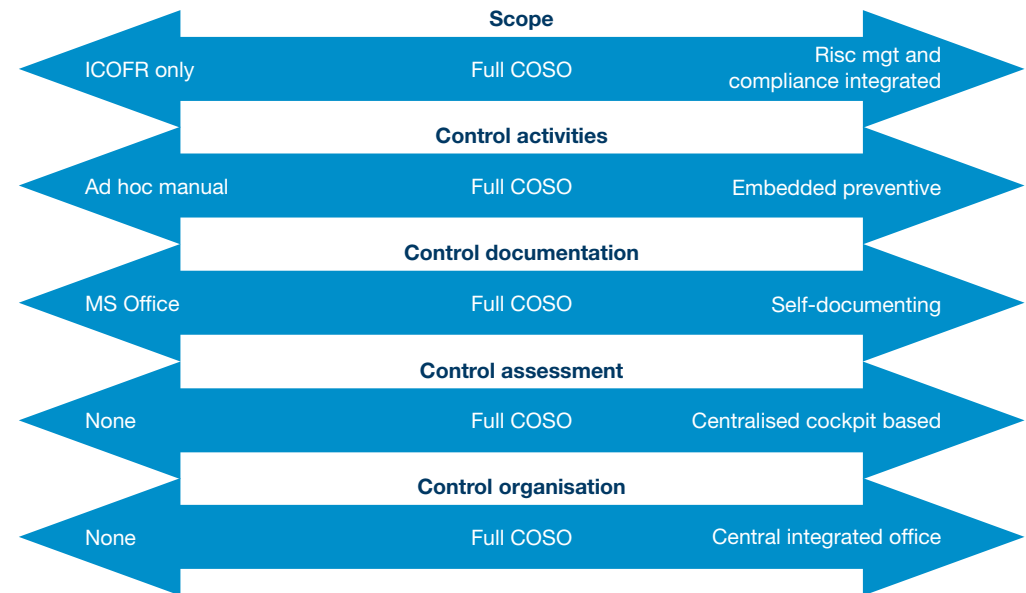


Figure 2: Some dimensions of an internal control system



Figure 1: Maturity model for internal control systems

over Financial Reporting (ICOFR) to also address operational control objectives such as preventing revenue leakages or ensuring the best supplier conditions. They could enhance their control activities from predominantly manual and detective to more automated and preventive. In control documentation and control assessment, organisations could consider using technologies that offer new possibilities in terms of increasing efficiency.

To gain a better understanding of current developments in internal control systems at leading Swiss companies and the implications for next-generation control solutions, we asked the internal control officers who participated at our round table sessions the following questions:

“Leveraging the opportunities offered by technology requires a clear vision and an adequate organisational structure”

- In what dimensions do you want to develop your internal control system?
- What are your main challenges (with regard to your internal control system)?
- What do you expect of solution providers (vendors of next-generation control solutions) in terms of helping you achieve your goals?

The responses to the first two questions are summarised in the table on page 8. The responses to the third question are summarised in Part II of this white paper.

In the table on page 8, we summarise the responses relating to the direction which participating companies aspire to take in further developing their internal control systems and the challenges they are faced with. This table contains the common themes of the discussion, and does not reflect individual company-specific round table input.

In summary, internal control officers currently face the challenge of numerous and complex regulations, risks, cultural factors and business dynamics. While the need to functionally integrate internal controls, risk management and compliance is apparent, internal control officers are struggling for attention as senior management’s focus shifts away from controls.

There is significant anticipated value in further developing the internal control system by optimising controls (more risk-based, increased consistency across countries and territories, KPI focused, increased automation), increasing monitoring efficiency, and integration across businesses, territories and functions. This value may not be realised because of the difficulty of quantifying it in a convincing business case. Lack of transparency on current solutions for streamlining controls and concerns about how to move forward are also hindering companies from acting on this potential.

Control vision and a “back to basics” organisation

Technology is only one part of the internal controls puzzle. To fully leverage the opportunities offered by technology, companies first must have a clear vision and an adequate organisational structure with regard to internal controls.

A clear vision of internal controls

Sarbanes-Oxley and the Swiss legislation both focus on internal controls over financial reporting. Only controls that can be linked to relevant financial reporting risks are necessary in the formal internal control system. Ownership and responsibility for these controls systems have been assigned to chief financial officers (CFO). CFOs have, in many cases, asked internal audit and internal controls experts to support them in this task.

We have observed that in most cases the number of controls implemented and documented in the year of implementation, especially for Sarbanes-Oxley, greatly exceeded what was necessary. Companies picked controls from templates and knowledge containers and implemented them without reasoning and questioning their real worth. The trend was clear: the more controls put in place, the safer and better for the CFO and the financial organisation. Operational business owners were left out and forced to perform and document additional new controls with little or no value to their processes and existing controls.

Although Switzerland could have benefited from this experience, we have seen many Swiss companies apply the same approach described above: implementing financial reporting controls into business processes without duly involving the operational business people with their specific knowledge. This has again increased the number of controls which are not applicable to the business environment concerned. Many companies today have a sense of being over-controlled.

Dimension	Summarised developments and challenges
Control culture	Participating internal control officers see a challenge in ensuring continued commitment in the organisation to sustain and improve the level of controls that has been achieved over the last few years. Generally, it is difficult to maintain discipline in control execution. Participants struggle with creating quantified competitive business cases to justify investments (time and money) in the internal control system.
Control organisation	<p>Aligning a centrally driven and organised control view with the needs of individual business units remains a challenge. Given the size and complexity of the organisation of international enterprises, and the mix of cultures, an effective management structure and supporting internal control system is required for adequate governance. Size, complexity and cultural mix also make it difficult to design and implement effective governance instruments.</p> <p>Ownership of controls, and the related roles and responsibilities, need to be considered and communicated carefully in such an environment. Internal control officers face a shortage of staff with the required skills and experience to ensure that people fully understand and execute their roles and responsibilities with regard to controls in a sustainable way.</p>
Scope	Internal control officers consider the convergence of internal control systems, risk management and the compliance function as beneficial to an organisation. This convergence also enables the integration of different local compliance needs and cultures.
Control management	<p>Internal control officers find it challenging to control costs while meeting the regulatory requirements and specific local business needs. In response, more reliance is placed on key performance indicators and closely linking controls to key process risks instead of control activities. Any investment in controls beyond regulatory compliance requires monetary justification included in a business case.</p> <p>Change management (adapting controls to a rapidly changing business environment) and reporting (providing senior management with a straightforward global overview of the state of controls) across diverse or complex entities can be difficult to manage. Companies are looking to achieve consistency of controls between worldwide entities to manage this more effectively.</p>
Control activities	Internal control officers want to move forward from a predominantly detective internal control system based on periodic controls towards a more preventive system based on highly automated controls embedded in processes and day-to-day operations. They see a reduction in the cost of controls as a strong business driver for putting more reliance on automated controls. However, the complexity of implementing the segregation of duties and managing access rights across different systems, as well as the availability of required systems and interface know-how poses a clear challenge when it comes to implementing more automated controls. The centralisation of business systems and the transparency of available controls in complex business systems is critical to further development.
Controls assessment and remediation	<p>Companies that perform a management assessment of controls are challenged by the cumbersome administrative procedures involved. The number and diversity of controls throughout the company make it difficult to centrally assess the appropriateness and adequacy of controls and evaluate the impact of locally identified control weaknesses (i.e. to planning for efficient site visits, and not overreacting to control failures).</p> <p>To address these challenges and establish a more efficient and effective monitoring process, companies are creating central dashboards and continuous monitoring mechanisms, and performing more frequent risk assessments.</p>
Control documentation	The participants did not express any intent to improve on control documentation.
Control infrastructure	<p>Internal control officers are looking to improve the technical infrastructure of their internal control systems. For instance, control data exists in various different systems at numerous locations and can currently only be collected with great effort. To get a central view of controls, data collection needs to be made easier.</p> <p>Participants would like to have a centralised software solution that links financial systems with analysed risks and controls. However, finding the right solution is seen as a challenge as, the capabilities of the available solutions in this area are not widely understood.</p>

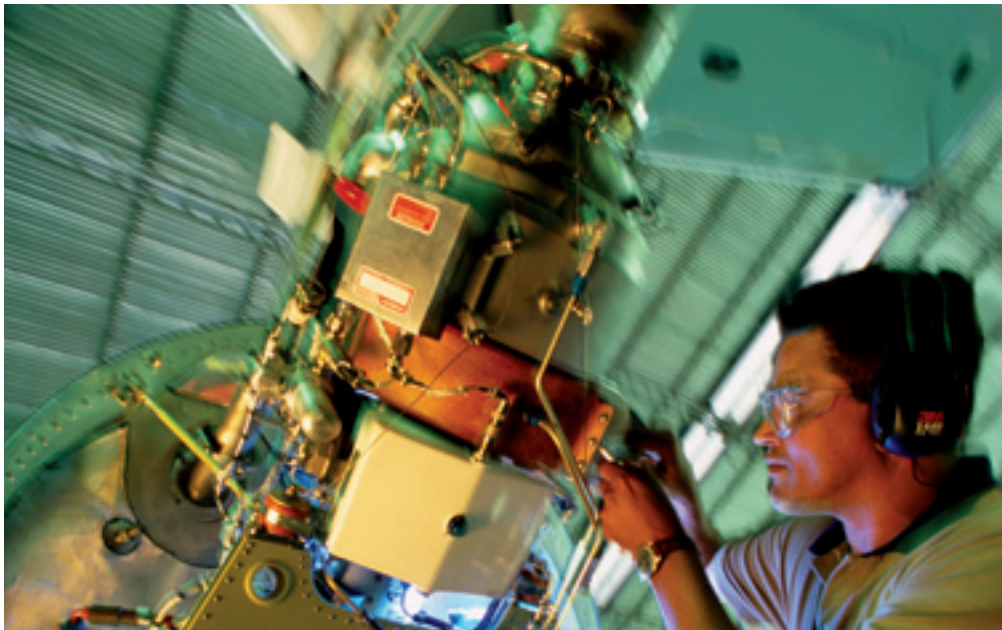
We see two strategies that could be used to rationalise the internal control system in a way that reduces the number of strictly formal control activities and at the same time drives operational excellence and efficiency.

a. *Apply a top-down risk-based approach to internal controls over financial reporting*

A company wanting to focus only on internal controls over financial reporting can achieve efficient results by applying a top-down, risk-based approach. Using so-called direct entity level controls at group, country or divisional level can be a good opportunity to reduce both financial reporting risks and the need for controls at the business process level:

“It is important to give responsibility for controls in business processes back to the business.”

- A good process and controls around critical accounting policies and estimates (such as the impairment test of goodwill or a revenue recognition policy for new products or services) are key elements. These ensure that events and issues in these specific areas, which are sometimes highly subjective are identified early, related accounting policies are researched and applied consistently, and matters are documented appropriately.
 - Monthly senior management business reviews normally include many aspects of financial reporting and are a source of untapped opportunities for leveraging existing controls more effectively. These reviews often include relevant comparisons with prior years, and budget deviations are subject to scrutiny and are reported back for next month’s review or earlier. Reviews are based on reports from financial controlling units with a good granularity of details, below the typical materiality level used for financial reporting.
 - In many companies we find that monthly closing procedures are well standardised and controlled. The closing process includes routine checks, such as reconciliation between general and subledgers, validating intercompany transactions, foreign exchange rates validation, and much more.
 - Information technology general controls (ITGCs) should also be part of the entity level controls. In today’s business reality, a controlled IT environment (organising and controlling access and changes to application and data) is a fundamental prerequisite for reliable financial reporting.
- Depending on the size and complexity of the company, the controls mentioned above on their own provide a solid foundation for internal controls over financial reporting. We recommend that the finance organisation re-evaluate the added value of financial reporting controls that are implemented in their business processes. In practice we see:



“Many companies should go back to basics in terms of the structure of their internal controls organisation.”

- Controls that do not have the right granularity level: too detailed or too superficial
- Redundant controls
- Controls to check situations that cannot occur anyway
- Controls to check on controls that have low or no added value.

Companies should consider which of these business process level controls can be safely removed (without jeopardising compliance with internal controls legislation) in the light of the comfort provided by the direct entity level controls.

b. Combine controls over financial reporting with operational controls to drive operational excellence and effectiveness

Before controls over financial reporting became the focus of legislation, companies needed to run their businesses in a controlled way to reach their business objectives. For example, companies worked

with standard sales prices as one means to ensure their products were sold at an acceptable margin. Standard sales prices were controlled to avoid unwanted changes and deviations to increase revenues at the cost of margin.

The question of how to control these standard sales prices was basically up to the management of the sales department. There were several options, such as using functionality in the underlying application to prevent any changes at sales transaction level, segregating of duties in the organisational set-up with manual controls only, through access rights in the system, periodic monitoring of exception reports, or by doing monthly margin analysis. In short, controls that were also relevant for financial reporting purposes already existed before formal internal control projects were implemented, but were often neglected or overruled in such projects.

By shifting the focus back to operational controls (and taking comfort from these for financial reporting purposes), financial reporting controls with no added value can

be minimised. In addition, time and effort can be dedicated to further developing the added value of operational controls (for instance with new technologies) to drive operational excellence.

That is why it is important to give responsibility for controls in business processes back to the business. Financial management knows financial reporting risks best and knows which controls are most effective to reduce these risks. Operational management knows its business best and knows how to ensure that business objectives are met through KPIs and controls.

Clear roles and responsibilities for all people at all organisational levels

Legislation in the controls domain, including Sarbanes-Oxley and the Swiss law on internal controls, have created several new positions. Chief risk officers, heads of internal controls, heads of compliance and chief security officers are good examples of new roles that have been created. In other cases, existing roles have been charged with increased responsibilities. Typically, the head of internal audit has been asked to take on more responsibilities related to internal controls and risk management. The audit committee is also a relatively new organisational unit, and at US companies could be supplemented by a risk management committee if the so-called Schumer Bill of 19 May 2009 is passed.

These roles are generally top management positions. A similar tendency has been observed at middle management level, especially when companies have to take account of regional and/or divisional set-ups.

The description of the responsibilities of these new positions may not always clearly reflect the expectations placed on the new position. Often only limited diligence was exercised in cases where the new responsibilities would overlap with existing positions in the organisation. While many companies have been very good at addressing the tone at the top regarding the importance of internal controls, we have observed that the unclear and inconsistent allocation of responsibilities related to these new roles in many organisations makes it difficult to realise organisational change with internal controls.

We strongly recommend clarifying all the roles and responsibilities, including a clear allocation of responsibility for governing, designing and executing controls on the one hand, and assessing and auditing controls on the other. Central governance and direction and regional implementation and execution should also be taken into account. In general, we believe that many companies should go back to the basics in terms of the structure of their internal controls organisation.

“Ownership is a critical component of an automated control solution.”

The old fable of the Chicken and the Pig² reminds us about the level of commitment to a project or cause. “Pigs”, who are completely committed to the project and accountable for its outcome, and “chickens”, who consult on the project and are informed of its progress. Successfully imple-

menting a next-generation control solution requires leadership behaviour resembling that of the pig in the fable.

The critical success factor in implementing any technology solution is dissecting the problem and being able to translate and

The people factor: Are your key stakeholders “pigs” or “chickens”?

As mentioned previously, employees feel over-controlled in this highly regulated environment, and burdened with administrative control tasks that they see add little value. At the same time, any next-generation automated controls project is a challenge to sell internally, let alone implement, because employees find it hard to believe that the technology will solve that underlying problem. How can a company find its way out of this apparent deadlock?



² A chicken and a pig were thinking of opening a restaurant. The chicken came up with the idea of calling the restaurant “Ham and Eggs.” The pig responded by saying: “No thanks, I’d be committed, but you’d only be involved!”

blend business requirements into business applications. Next-generation control solutions are not just about a computerised index of potentially low value rules. They are about implementing controls which make business sense, and for many companies this means a change in thinking and behaviour.

A successful control environment enables a company to operate within defined rules while allowing the spirit of the company's culture to flourish. Ideally, the behaviours and processes become a part of the company's culture and of the work ethic of its employees.

Based on our experience with implementation of next-generation control solutions, we have found the following steps to be critical controlling risk, driving corporate performance and inspiring greater confidence among people:

1. Define and endorse a business case that clearly demonstrates the benefits

An endorsed business case assists in determining the strengths and weaknesses of a project in a systematic and objective manner. Corporations need to be rigorous, objective and honest in applying and estimating the cost and effort involved in a next-generation control solution. An excellent business case would contain an estimate of the planned business benefits and indicate

how they will be monitored and realised. The business case drawn up for a next-generation control solution needs to pay specific attention to the fact that a number of working days used to operate and audit manual controls would be replaced with automated controls.

2. Include compliance as part of the company strategy and consider the supporting organisation

During 2009, PwC carried out research on 20 global projects to determine what the defining characteristics of successful change projects were. Projects that were driven by regulatory requirements ultimately did not meet their objectives. Projects where the nature of the organisation's strategic business need was clearly stated as the reason for the implementation produced a more successful outcome.

Depending on the industry in which a company operates, obtaining compliance certification is part of the licence to operate. These compliance aspects are non-negotiable. Despite regulations that apply to the top level of an organisation, the control environment should not be imposed from the top down. Rather, it must be driven and managed from above but carried out by the individual departments whose responsibility it is to know and understand what they must do. Management should convey the idea to the departments that they need to see the new-

generation controls project as a reason to change – an opportunity. They need to understand why they are required to do things differently, and have to have the necessary support to make the required changes. By cleaning up the control environment on a business process level as described above and moving controls towards supporting operating efficiency, a positive environment can be created to approach the change.

3. Move control ownership into the business

Ownership is a critical component of any automated control solution. Without ownership, a company will not be able to define the workflow items and will not be able to manage exceptions.

The majority of the financial controls lie within the finance function. However, having the entire control ownership lie with the finance function, or a dedicated control function, does not allow for clear ownership of and accountability for risks and controls. Top management should consider how to ensure accountability for the business and include the outcome in the next-generation control solution during implementation. To gain commitment, extend the team responsibilities beyond internal controls and finance, and include other business functions such as procurement and sales.

4. Do a fair assessment of what you have, and implement only what you need

When modifying rule sets, it is crucial to link the business objectives, often provided in the form of KPIs, with the controls. Consider conducting a risk assessment applying the "back to basics" principle, as described in the previous chapter, to ensure full insight into all of the risks, while remaining focused on those that are relevant. This may mean moving away from industry best practice controls and controls knowledge containers to the organisation's unique business reality. If the level of working capital is an important KPI, then controls must help achieve this objective. This approach enables prioritisation of the most important risks to leverage implementation efforts most effectively.

Only after this stage should the automation and technology aspects be addressed. Companies should constantly evaluate the value their controls. Non-valuable controls trigger exceptions that need to be addressed, moving resources away from the organisation's true priorities.

5. *Build change initiatives to align culture for maximum business impact*

Next-generation controls projects affect all people and functions in an organisation to some degree. The project's success depends upon its impact on employees' day-to-day work, and whether that impact is enabling or debilitating. One of the most crucial, yet often underestimated, aspects of an implementation is proper change management that motivates the people involved. Typically the solution is training courses, but these alone are not effective in terms of modifying behaviour.

To return to the fable, a successful project needs both chickens and pigs. However, it is difficult to find enough pigs, given the sacrifice required, including forswearing other projects and opportunities. Buy-in is required anytime significant change is enacted. Educating employees about the benefits of simplifying of the control environment and assessment process will likely lead to a greater degree of buy-in. The chance to get rid of labour-intensive manual controls makes it even more tempting. By moving control ownership to the business and setting up a reward system linked to business performance (of which controls are then an inherent factor), companies can create an attractive culture of change management.

6. *From change initiative to project approach*

Implementing a next-generation control solution is an innovative undertaking and needs an appropriate project structure. In companies with a global span over many regions and divisions, the underlying complexity needs to be addressed adequately.

Companies should approach the implementation of a next-generation control solution like a small business system implementation. None of the control solutions come with plug-and-play implementation functionality, and controls are always very specific to the company's business reality. We have found it useful to define specific

complex and challenging areas as priority tasks and solve them first, ensuring rapid progress throughout the rest of the project. The implementation of control solutions is discussed in more detail later in this white paper.



Part II: Smart use of internal control technology

“Vendors should help build a business case. Without this, it will prove difficult to find senior management willing to make investments in control solutions.”

Expectations placed on control solutions

Now that we have discussed fundamental pre-requisites for the further development of internal control systems, it is time to present what contribution the participating internal control officers expected from technology. We asked the internal control officers at our event to share their expectations on how control solutions should contribute to the further development of their internal control system. Of the various expectations considered, we extracted the common themes as key expectations. For the purposes of the discussions, we only focused on what functions the software was expected to deliver.

The five expectations are, that the control solutions should:

- Enable the reduction of “over-controlling” by linking business risks with controls
- Enable clear ownership of and accountability for risks and controls (both local and central)

- Provide value information to senior management
- Provide on-time information: continuous monitoring
- Handle and integrate multiple IT systems.

Each key expectation is further explained below.

- **Enable the reduction of “over-controlling” by linking business risks with controls**

Internal control officers expect control solutions to offer support in reducing the number of controls. Control solutions should provide a method for systematically reducing the number of controls by providing transparency on the interdependency of controls. Control solutions should support this objective by providing links to compliance frameworks and process risks (supported by industry templates) and by linking to other types of controls, e.g. KPI-based. Further support is expected in evaluating the

“materiality” of the controls to select key controls, as well as in evaluating the cost-benefit ratio of individual controls.

- **Enable clear ownership of and accountability for risks and controls (both local and central)**

Ownership and accountability are critical to ensure a continuously effective internal control system. This applies to both the implemented controls and to the process for maintaining the internal control system. The control solution should facilitate the allocation of both central and local ownership and roles and responsibilities. In addition, the control solution should support the process of maintaining internal control systems with e-mail notification for control execution and workflows for control assessment and remediation (issue tracking). Flexibility is required to adapt to continuous change in business and organisational structures.

- **Provide valuable information to senior management**

Internal control officers believe that it is important for control solutions to provide effective reporting for every level in the business, for external auditors and for authorities. It is necessary to show the value of the internal control system by reporting tangible benefits to senior

management. Specific reporting such as scenario reporting, KPIs and fraud reporting (Where are people by-passing controls?), is deemed suitable. Dashboards are considered a fitting reporting instrument for senior management. Integrating risk management and compliance in the control solution can make controls information more valuable for senior management.

- **Provide on-time information: continuous monitoring**

Internal control officers see potential in control solutions that make the current process of monitoring, assessing and remediating controls more efficient. A more timely view of the effectiveness of the internal control system and a reduction in the time elapsed in detecting control breakdowns, are important features. Management should be able to monitor controls in such a way that control data can be collected and processed automatically and exceptions are flagged for follow-up. Companies aspire to monitor the controls environment more frequently.

■ Handle and integrate in multiple IT systems

In companies with complex IT landscapes, the participants expect control solutions to be able to link, communicate and integrate with any business platform, including legacy systems and other control solutions.

The participants raised one important point in connection with the expectations placed on vendors in addition to the aforementioned and that is to help build a business case (quantitative and qualitative, e.g. based on industry practices). Without such a business case, it will prove difficult to find senior management willing to make investments in control solutions.

To match the expectations with the capabilities of available control solutions, we asked the vendors of the control solutions presented at our event to explain how and to what extent their solutions meet these key expectations. The answers to these questions, as well as a short introduction to the vendors and their solutions as provided to us by the vendors, are included in the last part of this white paper.

Which control solution for what purpose?

As shown in the previous section it was clear that internal control officers expected a considerable contribution from technology to further the development of the internal control system. However, before detailing the use of technology for internal control purposes, it is first important to outline the different types of control solutions, and why it is important to distinguish between them.

The term “control solution” is broadly defined, and misunderstanding can occur if further definition is not provided. For example, rather than competing against each other, some solutions could be linked and in conjunction provide a more comprehensive solution. To help navigate between the various types of control solutions, we have developed a reference model. The reference model in the table on page 16 identifies the functionality areas we generally see covered by control solutions:

We asked the participating vendors to identify the areas of functionality covered by their solutions. Their answers can be found in Part III of this paper.

If we compare the answers from the six vendors participating, it is clear that the various solutions cover different areas of functionality. It is important for companies to first understand what they want to

“It will be exciting to see how Swiss companies going forward will balance culture and control, and how technology will impact this process.”

achieve with technology, as part of the control vision, before trying to select a control solution.

Use the technology that best fits your control vision

Once a clear control vision is established, consider the developments in controls technology. By smartly using technology, more effective and efficient controls can be implemented while reducing the administrative burden that comes with managing an internal control system. Needless to say, selecting a technology that does not fit the control vision only adds to the burden. A tool with strengths in governance and reporting will not help a company which is looking for the transactional data analysis type of controls. It is essential to have a deep understanding of the fit between company specifics and the control solution to be selected. The cost of implementation

and future adaptation will far outweigh the licence fees. Based on PwC’s experience, if there is one best practice to follow in selecting a control solution, it is to do a proof of concept first, if necessary, with multiple vendors.

Functionality offered by control solutions on the market varies considerably. Solutions range from full scope control solutions to small “niche tools” that may cover only one aspect, for instance, emergency user access. More than one solution may be required to fully implement a company’s control vision. In the remainder of this section, we will explain how control technology can be used smartly.

a) *Use your business system’s functionality to automate control activities*

We see many companies missing opportunities to fully utilise their available control environment. The introduction of formalised internal control systems in recent years has resulted in the implementation of pre-

dominantly manual detective, sample-based controls. The benefit of generating tangible evidence is often outweighed by the effort required to perform these controls and the likelihood that they will not be performed effectively on the full population of transactions. At the same time, modern business systems provide an abundance of functionality to ensure the reliability of financial information, such as automated accounting

procedures, access rights, configurable tolerance levels and check reports. Such automated controls are performed systematically, without any manual effort, for the full population of transactions.

Not all control objectives can be achieved with inherent automated controls. The business system may not provide the functionality required. The size of the organisation may not allow for implementation of adequate segregation of duties and related access rights. This does not mean, however, that a manual control is required. We see companies create successful

automated workarounds by implementing specific data analyses to identify and report unusual transactions, such as manual journal entries outside the finance department or specific purchase transactions with customers. These data analyses are often driven by the audit function, performed with Computer Assisted Audit Tools (CAAT), and then adopted by the controlling function and integrated in business intelligence systems.

Functionality area		Description
Governance	Enterprise risk management	Product to manage risks at enterprise level (strategic, operational and financial risks) for multi-location entities
	Risks and controls cockpit	Product to be created between risks and controls, and allows flagging of which controls are documented, operating effectively and efficiently
	Control management	Product to enable the documentation of the control framework, manages control assessments (surveys), stores evidence, and manages mitigating controls
Processes	Application workflow	Product to assist business users in performing certain activities in a more controlled and efficient manner
	Application access rights	Product to define segregation of duties, sensitive access and monitor for exceptions
	Application configuration	Product to assess business automated controls
	Application master data	Product to identify and control master data integrity risks
	Application transactions	Product to analyse business transactions and identify specific and unusual patterns
Infrastructure	Identity management	Product to ensure that only authorised people can access resources through the IT infrastructure
	Database monitoring	Product monitor databases, including access management, activity log monitoring, configuration and master data integrity
	OS monitoring	Product to monitor operating systems, including access management, activity log monitoring and configuration
	Network monitoring and traffic control	Product to monitor the network (availability and entry) Web, and e-mail traffic
	Operations monitoring	Product to monitor server storage, backups and transport monitoring

More and more, process-level internal control solutions are also starting to offer this functionality. Certain solutions can analyse financial data and require that the control owner follow up on identified exceptions. This releases control owners from the need to check the bulk of data, which is correct, and allows them to focus their attention on the exceptions. This can be applied in numerous areas, such as:

- Overdue accounts receivable
- Assets under construction
- Overdue open purchase orders
- Uncleared suspense accounts
- Inventory differences
- Critical master data changes
- Special transactions, such as write-offs, reversals and credit notes

As we have indicated before, internal control officers are challenged by the complexity and limited availability of required know-how to successfully replace manual controls with automated controls. We also see companies that have overcome this challenge and significantly increased the proportion of automated controls compared to manual controls. The people/skills required to implement automated controls are available in the market, however, the challenge is communication and co-operation between internal control officers, business managers, and IT experts.

b) Use technology to manage controls at process and infrastructure level

The problematic implementation of IT general controls as part of the internal control system may to some extent have caused a lack of trust in business systems for use internal control purposes. IT departments were forced to implement a higher level of formalisation than they were used to or were able to due to “time to market” requirements. In the past, identity and access right management and change management were often highly informal in nature.

In user and access management, IT departments were faced with the challenge of obtaining appropriate input from business, for instance clear requirements with regard to the segregation of duties as a necessity to implement adequate access rights. The complexity and level of detail of access

rights in modern business systems is staggering and places huge demands on skilled resources. On top of this, negligence when it came to the segregation of duties in business systems has resulted in a smorgasbord of access rights tied together with Gordian knots. In some cases it may have seemed that the best way to clean up the mess without interrupting business operations would be re-implementation of the system.

The infrastructure-level and application-level internal control solutions we have featured in this white paper initially focused on dealing with exactly this issue of regaining control over users and access rights in business systems. They offer functionality to monitor, remediate, and even provision users and access rights. In addition, some offer functionality to identify and report any unusual activities at application, database, operating system and network level. This improves both the efficiency and reliability of the user and access right management processes, making it easier to safeguard assets, one of the key objectives of an internal control system. When selecting solutions for control over access rights, it pays to understand for which specific business system the solution was initially developed. In general, solutions developed initially for the company’s own business system will have the best developed rule set for that business system.

“It can be useful to consult with other companies and experienced implementers that have gone through similar internal control projects.”



“Start with easy-to-implement automated controls in high-risk areas.”

In change management, changes to business systems were poorly documented at many companies in the past. This made it very difficult to assess in detail whether business rules, and more specifically accounting and control rules, had been adequately represented in the business system logic. IT departments have made rapid progress in improving change management documentation and strengthening the procedures and access rights around making changes to production environments. But it remains a challenge to ensure that the effectiveness of automated controls is maintained over time. To address this, some process-level control solutions now have functionality to identify and report any changes to the relevant system configuration (for instance tolerance levels in a three-way match), reports and master data. Also, with some solutions attempts to bypass automated controls at the database level can be monitored. However, whilst many business systems in the ERP domain provide high-quality change management functions, current next-generation control solutions lack this ease of tracking function for change management.

An increasingly popular development with potential to make the management of controls more efficient is business process management software. Such solutions enable organisations to enforce the execution of scheduled process activities in the right order and at the right time. For example, by applying this to a monthly closing process, and embedding the control activities in the closing schedule, the execution of these control activities will be automatically ensured and documented for evidence. By securing the controls in the monthly closing in this way, reliance on this key component of the internal control system can be substantially reduced. As this software is integrated into the business system, it can be directly linked with and build on the inherent control functionality of the system. Such business process management software can also be applied in the area of IT general controls, for instance to ensure that changes to application functionality are adequately tested and approved before migration to production.

c) Use technology to ease the controls assessment

The management assessment process and the administration associated with it is a considerable burden and does not contribute to the popularity of internal controls. Automated controls and the automated management of controls may be a solution leading to more efficiency in this area.

For instance, with business process management an audit trail of both the actual control performance (accountant A started the monthly reconciliation in the accounting system between the general ledger and accounts receivable on February 1 at 15:13) and the related control results (the system reconciled general ledger with accounts receivable and reported no differences) becomes digitally available for automated monitoring. An up-to-date overview of control performance and results can be made available at any time, with no need to wait until annual controls testing has taken place.

As techniques change related to how management assesses their controls, current processes will be replaced by new and innovative ways to make control judgements. Controls assessments will be based on automated monitoring and real-time exception reporting instead of on low-frequency periodic testing. This is no longer wishful thinking. For processes with a high level of

automated controls, such as purchase to pay, some companies are already starting to monitor controls and analyse transactions centrally. Control weaknesses and unusual transactions are identified and reported as soon as they occur, and further analysis and remediation is initiated and tracked centrally on a daily basis.

Companies are implementing intelligent dashboards that summarise the results of this monitoring on a group level. This provides up-to-date transparency on and comparability of control effectiveness for processes throughout the whole company. With such continuous controls monitoring in place, annual controls testing no longer makes sense. The burden of creating, checking and annually testing the paper documents disappears. Instead, the dashboard provides controls reliance at a glance and the focus can be placed on the analysis of exceptions and subsequent actions. The assessment could then be limited to validating the monitoring system, with special attention to how it is modified for changes in the business, organisation, processes and business systems.

For companies with standardised businesses and a related system, some control solutions offer a combination of process-level and governance-level functionality that enables such a breakthrough in controls

assessment. There was a long held belief that with a standard business system, companies would achieve standard processes. However, in many cases, only standard user interfaces have been created. Controls solutions help identify where processes are actually still outside of the predefined process map.

Processes, systems and related automated controls do not need to be standardised in order to monitor them centrally in an automated manner. But it does need to be clear which controls cover what control objective, and it has to be possible to derive the relevant data from the systems involved. This is especially applicable for companies that want to create accountability on controls effectiveness without losing local responsibility for controls design. At this time there is no one solution on the market that offers the full functionality required to do this for a company with multiple businesses and related systems. Starting with a proof of concept remains critical. We have seen in practice, however, that it can be done.

A few pioneering companies have gone down this road, with positive results. Given that companies have to live with the controls assessment process, we expect many to follow suit. It will be exciting to see how Swiss companies going forward will balance culture and control, and how technology will impact this process.

Implementing next-generation control solutions

Implementing a next-generation control solution can be compared with a small business system implementation. Most current control solutions are not integrated with the underlying business systems in a way that derives full benefit from the available settings in the business system. Configuration settings as well as master and transactional data must be read and extracted from the business system. As a consequence, implementing a next-generation control solution usually involves nothing less than deeply reflecting on the settings and data of the business system, similar to a business system implementation. In this section we raise some implementation issues that are specific to next-generation control solutions.

An overall implementation plan is usually driven by the implementation of controls for high risks first and low risks last. However, in some situations we recommend that companies could also look at their existing controls environment and choose to start by implementing controls where automation would yield the fastest return on investment or eliminate work-intensive manual controls.



a) *Customise the rule set to fit the business*

Almost all vendors deliver a standard rule set with their solution. Although these rules represent good practice, an as-is implementation of these rules will result in a very high number of exceptions (generally into the millions), and could reduce the credibility of the solution within the organisation. As explained before in this white paper, each company must create and design specific controls covering its unique and specific business risks.

Segregation of duties (SoD) rules have their own challenges and complexities, but there is a great deal of experience to draw on in creating a company specific rule set:

- The first step is to define high-level risks and evaluate whether SoD is a valid response to mitigating these risks. We find that companies dive into the details too quickly and develop expensive solutions that might be practical for a number of entities, but cannot be implemented by smaller entities. The

preventive character of the segregation of duties is important, but there are many other controls possible in a process that covers the same aspects of risks. The discussion of the segregation of duties should be driven by representatives from both IT and business, and from all relevant regions where a company is active. While IT is strong in providing technical information, the business has the ability to define business risks and the type of controls that should be implemented. The discussion should not only include the initiation of transactions where segregation of duties is specifically important, but end-to-end business processes as well.

- The second step is to translate the high-level risks into technical definitions based on the business system being used. For example, when talking about the segregation of duties, if the business defined “create vendor” and “pay vendor” as a high risk, the second step for IT would be to define all possible ways in the business system that someone can create a vendor (and the process would repeat for paying a vendor). It may be particularly important to include custom transactions that are used by the business.

- The third and final step is to translate the technical definitions into the format that the control solution can understand. This is not something that a software vendor can always fully provide. This step is normally performed by people with hands-on experience with the control solution and the business system concerned.

A less explored area is assessing controls based on a combination of transactional data and configuration settings. A well-known example is the three-way match functionality in ERP systems. Monitoring the configuration control aspect in the IMG is only half the work. In addition, the underlying transactions need to be tested to identify purchase orders and goods receipts that are not created in the right order or, for instance, on the same day. There are many situations where only a mix of segregation of duties, monitoring of master data, configuration settings and transactional analysis provides the necessary comfort, again adapted to the specific business process risk of a certain company. Standard rules often do not provide the necessary linkage between the different domains.

Proofs of concept are useful to assess the applicability of rule set customisation. It can be useful to consult with other companies and experienced implementers that have gone through similar projects to ensure that key strategic and technical challenges have been identified.

b) Plan to remediate

After implementing an internal controls monitoring solution, the results produced may not be favourable. Even with a customised rule set, the initial number of exceptions identified could be quite intimidating. In some cases this could be a surprise for the organisation and an eye-opener for senior management. In such a situation, companies should remember that the underlying issues already existed, and the new solution has simply brought them to light. However, we have seen such situations creating significant issues and questions, both internally and externally. It is important to analyse the results and put them into perspective and initiate pragmatic remediation actions.

Project plans should anticipate appropriate effort and availability of resources to allow timely remediation. While, as mentioned above, the results can be surprising, the remediation should follow best practices and tackle areas with potentially significant business impact first. A rigorous process with ownership and accountability needs to be designed for the entire remediation phase.

To be able to do so and to follow up on remediation progress on numerous issues, workflow based tracking has proven to be a good approach. To enable this, it should be clear in advance who owns which issues so that they can be routed to the owner directly. Accountability can be built in by monitoring actual time to remediate versus planned time to remediate.

We also see companies define small packages of rules to be implemented sequentially. Well designed packages allow a company to achieve steady progress in small steps, with a manageable volume of remediation activities.

c) Do not underestimate the data

Translating controls into technical rules can be a complex job, especially for transaction analysis. It requires an understanding of the control solution, business rules, logic of the business system(s) involved and their data models (logical and physical). The required knowledge normally resides with different people who need be brought together through the appropriate project planning.

In some cases significant amounts of data might need to be assessed in a certain timeframe. This can present additional challenges in terms of both disc storage and the processing power required. Dedicated infrastructure may be required to process hundreds of gigabytes of information on a daily basis.

Extracting and processing global data in a single controls repository can create data security issues. In an international environment, data cannot be collected across all borders. Data security regulations differ from country to country, and this can mean that data from one country cannot be transferred to another country.

d) Design security to allow for easy remediation

As already mentioned above, the number of exceptions identified can be significant, especially in the area of access rights and segregation of duties. Design problems in underlying security concepts can make remediation a painful exercise. For example, when fixing one problem, many new violations and exceptions may be created in other domains. In some cases a redesign of the underlying security concepts is a more effective approach to remediate exceptions.

e) Be smart

It can be very tempting to strive for a high level of automation in the internal control system. An intelligent approach always considers the short term feasibility and cost of implementation of an automated control compared to that of a mitigating manual control. With the current speed of technological development, some automated controls might be easier to realise in one or two years' time. Start with easy-to-implement automated controls in high-risk areas.

An intelligently implemented control solution will not only contribute to compliance with control requirements. It will also help make processes more efficient and, ideally, help change behaviours in the company to create a culture where internal control is no longer seen as a burden, but as an integrated part of business.



Part III: Next-generation control solutions

The vendors that participated provided the following information as a short introduction to their company and/or solution as well as

a self-assessment of how their solutions meet the key expectations of the internal control officers.

Short introduction to the vendors that participated in our event

Approva/Consider Solutions	<p>“Consider Solutions operates as the European business for Approva Corporation providing the industry’s leading Continuous Controls Monitoring (CCM) technology. Approva Bizrights supports all aspects of CCM, including User Access Controls (such as Segregation of Duties [SoD] and Sensitive Access) and uniquely, Business Process Controls Monitoring (such as Configuration settings, Master Data and Transactions) in key systems.</p> <p>Consider Solutions supports organisations looking to understand the potential business value of CCM, explore the key requirements and business case, perform evaluations and proof of concept projects, implement specific automated controls or deploy CCM across the enterprise from a business and technology perspective.”</p>
BWise	<p>“BWise is a global leader in compliance and enterprise risk management software, with a strong heritage in business process management. Established in 1994, BWise delivers proven solutions to help organisations become ‘in control’ by increasing corporate accountability, strengthening financial, strategic and operational efficiencies, and maximising performance and ROI. With more than 1,200 customers in more than 80 countries worldwide and 300,000 users in virtually all markets, BWise has developed a strong and sustainable presence in the compliance and risk management sectors. Utilising templates and a best-practice implementation approach, BWise enables management to measure and manage risks and to comply with rules and legislation, such as Sarbanes-Oxley, European Corporate Governance Codes, IFRS, Basel II, ISO standards and more. BWise has offices in the Netherlands, United States, United Kingdom, Germany and India.”</p>
Conteliga GmbH	<p>“Conteliga is a Swiss based company specialising in innovative risk intelligence solutions. Conteliga is built up of a team of experienced professionals who have been inspired to bundle their knowledge and develop an inventive enterprise risk management solution focusing on control and process automation, usability and risk prevention strategies. Conteliga is providing immediate control results without any cost for hardware, operations or user training - and therefore the ideal internal control system for small and medium sized companies. The automation of administrative processes (e.g. user provisioning or password reset) as well as the optimization of the SAP license model ensures a maximal the ROI. ”</p>
Oracle	<p>“Oracle is organised into two businesses, software and services, which are further divided into five operating segments. Our software business is comprised of two operating segments: (1) new software licenses and (2) software license updates and product support. Our services business is comprised of three operating segments: (1) consulting, (2) On Demand and (3) education. As of October 31, 2009, we employed 73,502 full-time employees. In EMEA, Oracle is present in 25 EU countries, and in 16 countries in Middle East and Africa.”</p>
Runbook Company International	<p>“Runbook Company International is a certified SAP development partner for solutions for Financial Close, Internal Control Automation and Compliance Documentation in SAP. Companies using Runbook save costs and improve quality through automation of recurring financial processes.”</p>
Security Weaver	<p>“Security Weaver is a best-of-breed compliance application suite that integrates with any SAP environment to help users quickly and easily control enterprise cross-application compliance risk without consulting expense.”</p>

Vendors were selected based on our observations of current market developments and on their willingness to participate at our event. The presence of these vendors at the event should not be understood as a recommendation. Any software selection should be based on a thorough selection process, considering all relevant client specific requirements. The contents of this white paper are based on the outcome of the event, and not on any further research, e.g. to substantiate any statements of the participating software vendors..

The vendors mapped their solutions to our reference model for control solutions (see table below). If we compare the answers from the six vendors that participated, it is clear that there are different types of control solutions, which appear to cover different

functionality areas. In the vendor presentations at our event the customer cases did not demonstrate the full scope of functionality as expressed by the vendors in the table below.

As part of their control vision, companies should have a clear understanding from the outset of what they want to achieve with technology before evaluating a control solution. In this context, the existing IT landscape of an organisation is a leading factor for the selection of a control solution.

It is important to understand that the control solutions presented by Conteliga, Runbook and Security Weaver are mainly specialised for SAP, whereas the control solutions from Approva, BWISE and Oracle are positioned as business system-independent solutions.

Functionality area		Approva	Bwise	Conteliga	Oracle	Runbook	Security Weaver
Governance	Enterprise risk management		✓	✓	✓		✓
	Risks and controls cockpit		✓	✓	✓	✓	✓
	Control management	✓	✓	✓	✓	✓	✓
Processes	Application workflow	✓	✓	✓	✓	✓	
	Application access rights	✓	✓	✓	✓		✓
	Application configuration	✓	✓	✓	✓	✓	✓
	Application master data	✓	✓	✓	✓	✓	✓
	Application transactions	✓	✓	✓	✓	✓	✓
Infrastructure	Identity management	✓		✓	✓		
	Database monitoring		✓		✓	✓	
	OS monitoring				✓		
	Network monitoring and traffic control						
	Operations monitoring				✓		

In any case, we recommend assessing the fit for purpose through a proof of concept in what the company sees as the key functionality area(s). Also note that the best fit for purpose could also be offered by a combination of control solutions, each used for what it does best.

The vendors provided us with their self-assessment of control solutions against the key expectations of internal control officers who participated.

Enable reduction of “over-controlling” by linking business risks with controls		
Approva	“The main task in reducing ‘over-controlling’ is to limit and focus the number of controls to only those that represent a genuine business risk or performance improvement opportunity that management can take action on. We address this by linking the controls to be monitored with the business risk or performance improvement opportunity they relate to, and by asking the question ‘what action will management take to specific exceptions to the control test?’ If there are no clear actions, there is no value in the control. This first approach is independent of technology and should be applied universally. The specific Bizrights CCM approach relates to the fact that much ‘over-controlling’ is necessary as a form of ‘checks and balances’ for multiple controls that are tested manually, typically through small samples. When using continuous and complete monitoring of controls, the organisation is able to reduce the set of controls to a smaller set of tests that are continuous and completely covered across activity, avoiding the need for extra, redundant control tests.”	<p>PwC view:</p> <p>We believe “being over-controlled” is related to a lack of focus on risks that are really relevant. Standard risk libraries should not be used without further customising. This requires a sound risk assessment, performed with people from the business, from finance and from IT who have the right knowledge and competence.</p> <p>“Back to basics” is our vision to reduce over-controlling. Control solutions will not be able to drive this, but can be an instrument to support the implementation of such a vision.</p>
BWise	“A recent customer survey revealed that the BWise customer base was able to significantly reduce control testing, remediation, and reporting effort after implementing the BWise GRC solution. BWise GRC has been designed to support integration of governance, risk and compliance management initiatives into one converged approach in contributing a risk-based, business process oriented strategy.”	
Conteliga	“Conteliga provides an innovative risk/control framework covering the process, application and system level related risks. The Conteliga methodology is a risk-based approach, which supports the intelligent re-use of active controls, avoidance of ‘false positives’ and easy adaptation to individual processes and organisations. In order to reduce the cost of controls Conteliga provides effective risk prevention strategies and functionalities to allow the automation of control execution and control execution monitoring.”	
Oracle	“Oracle GRC provides an automated approach to manage and enforce user access policies (including segregation of duties), configuration management and prevention of unusual transactions. The solution offers a best-practice library of controls developed in conjunction with Oracle’s industry leading partners. Risk and compliance activities are streamlined – including risk assessment, policy documentation, controls testing, and organisational certification – with Oracle GRC Manager being the orchestration hub for all GRC initiatives. Risk and compliance activities are thus unified with fragmented GRC activities across multiple business units, geographies, and information systems, brought together. In addition to an integrated portfolio of business applications, Oracle GRC includes a best-in-class set of solutions for infrastructure control. The infrastructure control solutions provide the cornerstone for information protection and privacy.”	
Runbook	“Runbook Company provides software that enables automatic execution of controls as part of the business process. By embedding the controls in the process the risk are covered automatically. We see that many companies are not efficient and also not effective in their controls and that they build way too many controls that generate a lot of work. Reduction of control work can only be achieved by automation and management by exception. A lean and well designed business control framework will help, benchmarking against other companies does too.”	
Security Weaver	“Security Weaver proposes an out of the package standard analytic package for SoD matrixes (230 rules) and transaction monitoring (60 rules). Based on the requirements of the customer, the customer himself can choose the amount of controls he requires.”	

Enable clear ownership and accountability for risks and controls (both local and central)		
Approva	<p>“This is largely a controls governance issue that needs to be explored, agreed and consistently executed with management. However, ownership and accountability become much clearer and more effective when management and stakeholders realise that ownership and accountability are associated with specific required actions. In the CCM world with Bizrights, control exceptions are routed directly to the responsible individuals who have agreed on their ownership. Ownership thus becomes clear and practical, and the remediation actions are equally clear as an audit trail. The continuous and immediate nature of CCM eliminates the risk that management sees old or out of date business exceptions which reduces the risk of the sense of ownership and accountability becoming diluted over time. With Bizrights both central and local controls, with information routed to the correct stakeholders, are managed effectively.”</p>	<p>PwC view:</p> <p>Most control solutions are able to represent ownership of controls and/or risks. We see, however, that many organisations first need to clean up ownership, responsibilities and accountability for internal controls. Control solutions will not be able to drive this.</p> <p>It is important to consider risk versus control ownership, for instance when a risk is covered by multiple (even interdependent) controls or by varying controls per country. Also, responsibility and accountability should be clearly defined for automated controls as well as for remediation.</p>
BWise	<p>“A central risk library or localisation of risk and control frameworks per entity with dedicated risk and control owners and accountable, the BWise GRC solution provides both options with according workflows for top-down or bottom-up risk and control identification and assessment, as well as comprehensive steering, remediation and monitoring capabilities to be able to stay in control at any time.”</p>	
Conteliga	<p>”The Conteliga solution delivers an ‘out-of-the-box ownership model’, customisable to individual organisations. The concept focuses on process-related accountabilities, such as the ownership of risks, controls or business processes and on organisation-related accountabilities, such as country manager or cost centre owner. Conteliga provides best practice solutions to automate notification, alerting and deputisation management.”</p>	
Oracle	<p>“GRC Manager provides a default set of authorisation roles that can be assigned to users by a GRC Administrator. Each role has a pre-defined set of permissions for accessing and using GRC Manager functions. Users can be assigned one or more GRC Manager roles and a role can have modified permissions, depending on each user’s need for access to GRC Manager content and for tracking activity for compliance. Roles can be customised according to an organisation’s requirements. Security features control which users can view, edit, and manage documentation in GRC Manager. Security is provided in Oracle Content Server for the documentation created with GRC Manager and for the user accounts set up to create, use, and manage information with GRC Manager. Security is also implemented through the assignment of specific GRC Manager roles and permissions to users. The administration tool enables authorised users to customise the GRC Manager Interface for organisations by configuring the user interface for lists, fiscal periods, display text, and user defined fields (adding or hiding fields).”</p>	
Runbook	<p>“Runbook has build in clear ownership and accountability for execution, rating and documentation, monitoring and remediation of controls. Business operations are responsible for financial risk management and compliance. However, a trend in many large companies is a central design. Most IT systems that have a central design are designed by IT staff and have pre-sets mandatory for operations to work with. In that case it is not always transparent who is responsible and accountable.”</p>	
Security Weaver	<p>“Security Weaver mainly focuses on local (decentralised) system environments. This avoids complicated data extraction and does not require additional hardware infrastructure and secures a high performance in performing the analytics. As Security Weaver is SAP embedded there is also the possibility of providing the analytic data to a central approach too.”</p>	

Provide value information for senior management		
Approva	“Information provided to senior management is of a high value because it is specific to the agreed priority risks and controls, the right information is targeted and routed to the agreed stakeholders and the control exceptions are complete, precise and timely for business operations. The information is high value because it is a ‘full 360 degree’ view of risks to the business, not just access control or master data for example. Information is typically filtered according to stakeholder, such that senior management get control exception summary information, in a dashboard for example, for the processes or risks under their responsibility. Detailed business control exception alerts are routed to the stakeholders who have agreed to be the owners that take action on specific control exceptions. Detailed technical information is routed to the relevant IT specialists where required. This makes for a valuable, efficient and effective controls management process. Obviously, governance is an issue here also, in that the stakeholders need to agree what ‘value’ means to the specific business in this context and thus the priority controls and ownership.”	PwC view: The question is what constitutes “value” for senior management with regard to controls. We believe senior management needs to be informed about the nature and size of significant control exposure as soon as it occurs, and needs to be able to monitor timely remediation of the related weaknesses. For that purpose it is essential that the control solution can aggregate control exceptions and remedial activities across processes, entities or regions. Companies should specifically focus on control solutions that operate in the governance functionality area.
BWise	The fully integrated BWise GRC solution ensures that sound reports and relevant information on all business units involved can be provided at the right place and time. Comprehensive (ad-hoc) reporting and interactive off-line dashboards support senior management in analysing trends of past loss occurrences, present risk assessments and future development of risk scenarios in one single tool.	
Conteliga	“Despite other solutions Conteliga provides a full SAP integrated management dashboard with real-time data. No supplement hardware, file import/export routines or extensive user training is required. The dashboard is KPI based and can be used for operational monitoring such as batch file execution as well as for risk/control status and business process monitoring. KPIs can be easily customised for individual reporting requirements.”	
Oracle	“The Oracle GRC platform provides unparalleled visibility, with role-based intelligence for risk and control performance. It aligns GRC initiatives with the achievement of strategic organisational objectives by concretely linking key risk and control metrics to strategy formulation and planning, actively monitoring day-today operations, and providing a single, accurate view of enterprise-wide GRC activities to promote business transparency, actionable analysis, and rapid execution. Oracle GRC empowers you to stay on top of critical organisational compliance and risk management activities. Fusion GRC Intelligence offers enhanced visibility into your organisation’s compliance readiness and responsiveness by providing risk, control, and performance analytics and dashboarding. Robust reporting capabilities help validate control design and operating effectiveness against access policies and segregation of duties conflicts. The interactive solution enables GRC professionals to effectively plan, model, report and analyse GRC activities so that potential issues are identified earlier and corrective actions are more timely and informed. Senior management gain transparency to control status, and can thus accelerate risk responsiveness with user-tailored intelligence. The standard dashboards can be augmented with data from operational and planning systems.”	
Runbook	“Runbook is a user and operational based solution. Managers can drill down to problems and intercept errors. Value based information is available through extracts.”	
Security Weaver	“Security Weaver solution suite has a built in reporting functionality. Currently there is no central reporting considered but will be available soon.”	

Provide on-time information or continuous monitoring		
Approva	“Timely, accurate and complete exception information provided to management and stakeholders is a core value of the Bizrights CCM solution. Whether for user access, system configuration or process and data monitoring, the timely information provided is complete and precise and targets all instances of the required control exception in the business, not just from a small sample. This is the essence of continuous monitoring.”	PwC view: In our opinion, on-time information with regard to controls means that control breakdowns are identified and reported as soon as they occur. This cannot be accomplished through a periodic assessment of controls, but requires an infrastructure to monitor controls directly or through transaction analysis on a high-frequency basis. Especially in a global environment with multiple business systems, the collection and processing of control and transaction data requires the right infrastructure in addition to that which current control solutions offer.
BWise	“The BWise solution provides a unique integration of GRC and CCM with workflow support for automatic transaction monitoring functions, periodical imports of transaction data from ERP and financial applications, identification of control exceptions, notifications and alerts as well as exception and remediation management with comprehensive reporting and analytics capabilities.”	
Conteliga	“Conteliga delivers real-time analysis on risk status and control failures. Automatic risk review processes are available; document and evidence management can be activated. The monitoring of historic data allows trend analysis and ongoing improvements of the risk and control framework to focus on critical business risks and to reduce over-controlling. Outstanding is the Conteliga product ‘Process Controller’, which is an automation engine for implementing controls on critical business processes without impacting the business performance.”	
Oracle	<p>“Oracle’s GRC Controls Suite (GRCC) provides governance controls that can be embedded into an enterprise resource planning (ERP) system. Embedding helps companies set controls for real-time monitoring of access to and changes in inventory items, general ledger accounts, order-to-cash and procure-to-pay cycles, payroll, and other items. Compliance becomes easier and as a result it becomes more effective. Business units can incorporate compliance into their workflow instead of resisting yet another request for information.”</p> <p>“GRCC allows companies to collect useful compliance information through continuous monitoring and enforcement. It protects operations so that compliance activities add value rather than layers of costs and tasks. In addition, the system creates a tamper-proof audit trail designed with multi-agency and multinational reporting needs in mind.</p> <p>“The GRC applications are embedded into the Oracle system to make GRC controls work for the organisation; the controls ensure business process integrity. This technology enables customers to automate GRC activities, such as enforcing proper segregation of duties in enterprise applications, reducing fraud with continuous monitoring of business transactions, and providing defensible evidence of a proper control environment. With Oracle GRC Controls, organisations are better able to enforce corporate policies in real time by embedding granular controls and monitors into their business applications. GRC becomes part of the business, not an afterthought.”</p>	
Runbook	“Runbook monitoring is real time and includes on demand handover messaging by regular e-mails and other forms of text messaging. The execution of controls, both automated and manual, is based on management by exception thus applying continuous performance monitoring.”	
Security Weaver	“Security Weaver technology provides real-time information as the solution is completely embedded into SAP.”	

Handle and integrate multiple IT systems		
Approva	“Bizrights is architected to be a controls management platform for business. This means that whilst it is highly tuned for specific common applications, such as SAP, it is configured to handle multiple system and data formats. One company has a single instance of Bizrights monitoring 57 different production SAP instances in its global business, and another monitors 18 non-SAP systems together with 2 SAP production instances. However powerful this may be, effectiveness in addressing multiple IT systems is not just about systems to be monitored, it is also important to integrate the application into the customer’s overall IT and process landscape, so we integrate into Single Sign-on, Active Directory, Intranets such as Sharepoint, risk management reporting systems, corporate dashboards and identity management systems at many customers.”	PwC view: Most tools mainly focus on one type of ERP, although some claim to accommodate and cover any other legacy application. This is generally true, but the effort to reach that objective should not be underestimated. Developing interfaces or connectors for non-standard applications may not necessarily be on the vendor’s development roadmap, does not provide any library of risks for the non-standard application, and generally triggers additional costs that are sometimes difficult to estimate. It is also very important to clarify with vendors whether their control solution will be able to cover controls within and across non-standard applications.
BWise	“BWise is capable of capturing and analysing data from any open application and data source, including all major ERP systems. An out-of-the-box SAP process and access controls template is available. Additionally, various integrations to third party applications have been established.”	
Conteliga	“Conteliga is a SAP add on, which can also integrate legacy systems into the control framework. The product ‘Conteliga Adapter’ allows this integration of legacy systems, enabling cross application processing during processes, such as, user provisioning, analysis/simulation of segregation of duties or cross application general computing controls analysis (GC-IT controls). No supplement hardware is required.”	
Oracle	<p>“Oracle delivers a comprehensive GRC platform that works across heterogeneous environments. Oracle combines risk intelligence and analytics, end-to-end support for cross-industry and industry-specific GRC processes, and best-in-class controls enforcement and data security, so clients can do the following:</p> <ul style="list-style-type: none"> ■ Leverage a centralised repository of GRC information. Built on the industry’s leading content management solution, only Oracle unifies disparate silos of GRC data across multiple mandates, frameworks, systems, and lines of business to deliver insight into risk-adjusted performance. ■ Manage GRC processes across the enterprise. Mitigate risk across areas, such as financial assurance, workforce training, and IT governance, and in industry-specific areas such as credit risk management, anti-money laundering, and pharmaceutical quality assurance. ■ Protect critical information assets at all levels. Core security and privacy controls, along with automated enforcement of proper user access and authorisation policies, keep information safe across all IT resources – applications, middleware, and databases.” 	
Runbook	“Multiple SAP systems can be integrated in one comprehensive overview. As long as it is SAP we can handle it.”	
Security Weaver	“Security Weaver focuses on audit automation within the SAP environment. It is also possible with Security Weaver Secure Enterprise to take account of compliance controls out of non-SAP systems. Secure Enterprise extracts data from non-SAP systems into SAP and takes account of the imported data while the analytic is running.”	

Which of the key expectations will be addressed by your current main development/solution enhancement and how?		
Approva	“The core values of Approva Bizrights continue to strengthen with our new releases, together with improved capabilities for delivering controls monitoring as a Web-based service using the SaaS model and enhanced ‘controls intelligence’ to further increase the value of controls monitoring information to senior management, which further drives greater ownership and accountability and continual focus on ‘just enough’ and ‘just in time’ controls monitoring.”	<p>PwC view:</p> <p>We believe that for companies to be happy with their investment, they should first have a clear control vision and a back to basics set-up for their internal controls organisation.</p> <p>It is also important to understand what the different control solutions can do now, and what they will be able to do in the future.</p> <p>It is our aim, for instance through this white paper, to support companies in the further development of their internal control system by helping them use the best technology in the best way possible.</p>
BWise	“BWise is currently developing additional templates, such as Oracle authorisation or templates for fraud and anti-money-laundering. MS Outlook integration for monitoring results will further improve user-friendliness. Enhanced enterprise risk management and internal audit support as well as full Web-based process portal integration will further strengthen the global leadership of BWise in the GRC market.”	
Conteliga	“The Conteliga strategy is based on 3 pillars: the automation of control, risk reporting and continuous monitoring of business processes. The focus on preventive control strategies and the integration of other standard platforms allows cross-application risk and process monitoring. The Conteliga generic concept enables a very quick response to individual customer requirements. This approach ensures that we are able to continuously optimise our services and capabilities.”	
Oracle	<p>“The convergence of global standards and accelerating corporate performance expectations mean that organisations are seeking a better way – a sustainable platform that improves the quality and effectiveness of compliance programmes and provides the mechanisms to understand, manage, and treat risk. From an applications perspective, Oracle continues to integrate our planning and risk assessment products to provide true cross-enterprise support for real-world requirements. The newly released Enterprise GRC Manager (EGRCM) creates a common foundation facilitating shared practices, reuse of work, efficiency, and cost savings, while individually supporting the unique focus, processes, information and security requirements of each group. With a platform and natively-built modules for specific initiatives, Enterprise GRC Manager allows each group to configure modules to their needs. This approach addresses the problem of siloed GRC responses, without imposing a one-size-fits-all solution. Oracle will continue to enhance the best practice library of controls and build integration points for our GRC Controls Suite to work with major ERP systems to better enable customers manage conflicts within and across ERP systems.</p> <p>“On the technology side, Oracle will continue its practice of expanding our security offerings built on open standards.”</p>	
Runbook	“Web-based Runbook solution independent of SAP and compliance documentation organiser; one single point of entry for all compliance documentation.”	
Security Weaver	“Flexibility in setting up additional controls, central reporting, risk calibration, more flexibility in considering non-SAP systems.”	

Acknowledgments

White paper

**Making sense of internal control:
How to align vision, organisation
and technology to lower your
compliance costs and improve
business efficiency.**

Published by
PricewaterhouseCoopers AG

Sponsor

Jürgen Müller

Partner-in-Charge

Paul de Jong

Managing editor

Raymond Mastre

Editors

Antoine Wüthrich

Christine Gora

Jürgen Müller

Paul de Jong

Raymond Mastre

Reviewers

Aaron Werth

Alexander Fleischer

Bryan Lutz

David Ingen Housz

Joe Walsh

Jürgen Elbel

Richard Thomas

Robert Diggle

Special thanks to

Audrey Burro, Barry Franck, Giovanni Perone, Hans-Hermann Gröger, Rainer van Alphen, Robert Borja, Roger Ellecosta, Sandra Scheffmann, Tanja Schmitz, Yves Luetolf

www.pwc.ch/spa

To have a deeper conversation about how this subject may affect your business, please contact:

Jürgen Müller
Partner

Leader Systems and Process Assurance –
Internal Audit Services Switzerland,
PricewaterhouseCoopers

+41 58 792 8141
juergen.t.mueller@ch.pwc.com

Paul de Jong
Partner

Systems and Process Assurance –
Internal Audit Services,
PricewaterhouseCoopers

+41 58 792 7658
paul.l.de.jong@ch.pwc.com

Comments or requests?
Please visit www.pwc.ch/spa.

Aarau
Bleichemattstrasse 43, 5000 Aarau
Tel. 058 792 61 00, Fax 058 792 61 10

Basel
St. Jakobs-Strasse 25,
P.O. Box, 4002 Basel
Tel. 058 792 51 00, Fax 058 792 51 10

Bern
Bahnhofplatz 10, P.O. Box, 3001 Bern
Tel. 058 792 75 00, Fax 058 792 75 10

Chur
Gartenstrasse 3, P.O. Box, 7001 Chur
Tel. 058 792 66 00, Fax 058 792 66 10

Genève
avenue Giuseppe-Motta 50,
P.O. Box, 1211 Genève 2
Tel. 058 792 91 00, Fax 058 792 91 10

Lausanne
avenue C.-F.-Ramuz 45,
P.O. Box, 1001 Lausanne
Tel. 058 792 81 00, Fax 058 792 81 10

Lugano
Via della Posta 7, P.O. Box, 6901 Lugano
Tel. 058 792 65 00, Fax 058 792 65 10

Luzern
Werftstrasse 3, P.O. Box, 6005 Luzern
Tel. 058 792 62 00, Fax 058 792 62 10

Neuchâtel
place Pury 13, P.O. Box, 2001 Neuchâtel 1
Tel. 058 792 67 00, Fax 058 792 67 10

Sion
place du Midi 40, P.O. Box, 1951 Sion
Tel. 058 792 60 00, Fax 058 792 60 10

St. Gallen
Neumarkt 4/Kornhausstrasse 26,
P.O. Box, 9001 St. Gallen
Tel. 058 792 72 00, Fax 058 792 72 10

Thun
Bälliz 64, P.O. Box, 3601 Thun
Tel. 058 792 64 00, Fax 058 792 64 10

Winterthur
Zürcherstrasse 46,
P.O. Box, 8401 Winterthur
Tel. 058 792 71 00, Fax 058 792 71 10

Zug
Grafenauweg 8, P.O. Box, 6304 Zug
Tel. 058 792 68 00, Fax 058 792 68 10

Zürich
Birchstrasse 160, P.O. Box, 8050 Zürich
Tel. 058 792 44 00, Fax 058 792 44 10