

Rethink the way you manage legislative BPO risk: A qualitative approach on mitigating legislative outsource risks

By François Zielemans, Protiviti Manager

“Two of the main reasons respondents cited for the lack of enthusiasm [for Finance and Administration Outsourcing¹] were the loss of control and the loss of know-how. What with Sarbanes-Oxley heightening the awareness of internal controls and governance, many CFOs say the risk of missteps are unjustifiably high when processes are handed over to a third party” CFO Europe, May 2007.

The globalisation and rapid advances in technology have changed the basis of competition. The time when companies owned the whole value chain has gone forever. Depending on which research firm one believes, the Business Process Outsource (BPO) market has a value of USD 175 to USD 200 billion in 2007 and double-digit growth potential.

It's about control capabilities

Today, the key capabilities of a company increasingly evolve around constant optimisation of the sourcing of the value chain and controlling third-party suppliers. As Gottfredson et al state it:¹ “It’s no longer a company’s ownership of capabilities that matter but rather a company’s ability to control and make the most of critical capabilities, whether or not they reside on the company’s balance sheet.”

This drive to leverage business processes in shared service centres, outsource them to third parties or operate them under a Build-Operate-Transfer (BOT) model requires a different control approach compared to managing them in-house. Additionally, the design of an effective control framework to manage these relationships is becoming ever more challenging in the face of the growing forest of legislation with which companies must comply.

The reservation that senior decision-makers feel towards outsourcing is therefore understandable, but in the long term, is not sustainable given the relentless market pressures. The combination of not wanting to be left behind and lack of experience with managing third parties often results in a company managing the third party as an in-house department; relying solely on a SAS 70 report; or creating an administrative monster that requires the third party to report on every conceivable parameter.

All three solutions are ineffective and inefficient. The third party does not want the company to manage its internal functions, a SAS 70 limited is in its use², and reporting on hundreds of metrics creates only the illusion of control.

Based on insights and best practices gained during various shared service and outsource assignments, Protiviti developed a methodology to create a fit-for-the-job outsource risk management process. Therefore, the aim of this white paper is to provide you with a ‘fourth’ solution:

Creating an effective and efficient outsource control framework that aligns with the risk appetite of your company.

¹ This paper uses the following definition for ‘outsourcing’: an arrangement of any form between a Financial Institution and a service provider by which that service provider performs a process, a service or an activity which would otherwise be undertaken by the Financial Institution itself (based on the MiFID, Level 2 Directive draft of June 2006 definition).

² See frame one for a brief explanation of the pros and cons of a SAS 70 report.

Before presenting the methodology to manage (legislative) risks, a few legislations and their requirements regarding outsourcing are discussed below:

Regulations and Outsourcing

As early as 1987 the Treadway Commission, formally known as the Commission on Fraudulent Financial Reporting, made the following recommendation:

“For the top management of a public company to discharge its obligations to oversee the financial reporting process, it must identify, understand, and assess the factors that may cause the financial statements to be fraudulently misstated.”

This recommendation resulted in a proposal by the Security Exchange Commission (SEC) in 1988 for additional rules that bore striking resemblance to some sections of the Sarbanes-Oxley Act. However, aggressive lobbying by interest groups prevented actual implementation of these rules. Until July 2002 when, as a result of fraudulent acting by several U.S. listed companies, the Sarbanes-Oxley Act (SOX) of 2002 was passedⁱⁱ.

SOX is only one of the many regulations that companies need to comply with these days. Financial Institutions and insurers are especially hard hit with regulations like the Gramm-Leach-Bliley Act, Solvency II, the New Basel Capital Accord, and MiFID. Some of these regulations make explicit statements about dealing with outsourcing risks while others are implicit. The following paragraphs briefly discuss outsourcing as mentioned in the Basel II and MiFID regulations.

Second Capital Accord by the Basel Committee (Basel II)

The Second Capital Accord defined by the Basel Committee on Banking Supervision, is colloquially known as “Basel II.” While the original Capital Accord of 1988 already addressed market and credit risks, Basel II substantially changes the treatment of credit risk and links the way operational risks are managed to capital exposure. It is composed of three pillars (see figure 1).

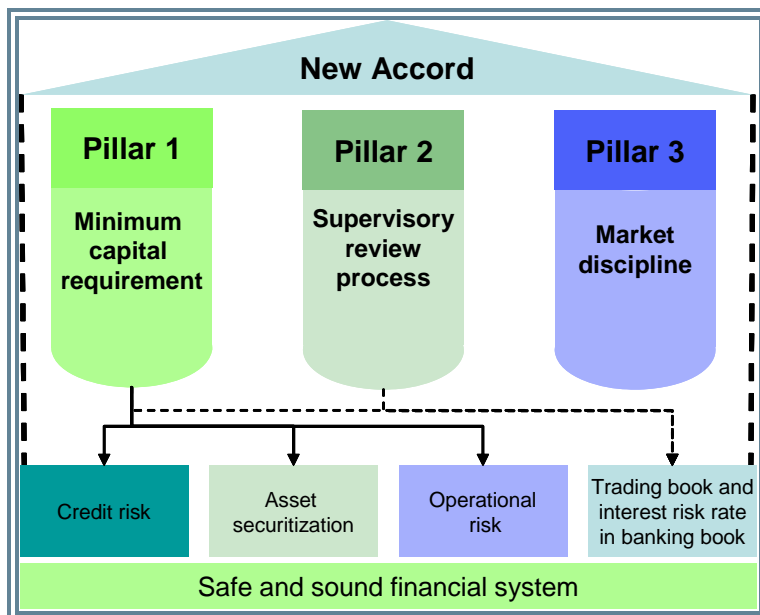


Figure 1: Overview of Basel II (Source: Protiviti 2007)

The first pillar defines minimum regulatory capital requirements, based on its risk profile with a minimum of eight percent of capital-to-risk weighted-assets. The second pillar defines guidelines for supervisory review and the implementation of enterprise risk management (ERM). It defines specific responsibilities for executives and principles for internal control and governance. The third pillar aims to bolster market discipline through enhanced disclosure by banks. From an outsourcing perspective, the second pillar is most relevant.

The Basel Committee on Banking Supervision makes several specific statements regarding outsourcing in its *Sound Practices for the Management and Supervision of Operational Risk* (February 2003). Among these statements there are two requirements and some hints on how they can be addressedⁱⁱⁱ.

“Outsourcing arrangements should be based on robust contracts and/or service level agreements that ensure a clear allocation of responsibilities between external service providers and the outsourcing bank.”

Translated into practice the quote requires an adequate contract and that the bank and service provider create an organisational entity to manage the relationship. Within a financial institution this function would be called the Retained Organisation or Service Management Organisation³. [See the second frame](#) for more information on this subject.

Customer loss needs to be reflected in contract

Another interesting requirement is:

“...banks should understand the potential impact on their operations and their customers of any potential deficiencies in services provided by vendors...”

This implies that the bank is required to assess the whole service chain and translate the financial impact of non-performance somewhere downstream in the chain into upstream contract clauses and controls.

This is not a simple requirement to fulfil as banks often do not know their service chains well enough to determine the downstream impact of upstream non-performance by third parties. It is also difficult to mitigate the potential loss by liability and credit clauses as the damage might not be in proportion with the total contract value.

European Union’s Markets in Financial Instruments Directive (MiFID)

The European Union seeks to create a single market for financial services and part of its action plan is the Markets in Financial Instruments Directive (MiFID). MiFID replaces the Investment Services Directive (ISD) which was adopted in 1993. MiFID basically allows an investment firm, established and authorised in an EU member state, to provide services and/or establish branches in other member states without further authorisation.

In essence MiFID will greatly simplify cross-border commerce by harmonising the rules of conducting business. Other organisations within the scope of this so-called ‘passporting’ regime are commodity and credit derivatives, underwriting services, safekeeping and administration of financial instruments and investment advisory.

³ This paper uses the following definition for ‘Retained Organisation’: An intelligent management and purchasing function used to govern one or more service provider(s) providing a process, a service or an activity for the Financial Institution. Other terms commonly used for Retained Organisation are Service Management Organisation or Demand-Supply Organisation.

The consequences for outsourcing initiatives discussed below are based on the Level 2 Regulation and Directive dated August 2006^{iv}. The key phases revolve, like in Basel II, around ‘avoiding operation risk’ and ‘control’ capabilities. The following is an excerpt from Article 13:

“... firm shall ensure, when relying on a third party for the performance of operational functions which are critical for the provision of continuous and satisfactory service to clients ... that it takes reasonable steps to avoid undue operational risk.”

“Outsourcing of important operational functions may not be undertaken in such a way as to impair materially the quality of its internal control and the ability of the supervisor to monitor the firm’s compliance with all obligations.”

The previous quote refers to ‘critical operational functions’ which is defined as:

“...an operational function shall be regarded as critical or important if a defect or failure in its performance would materially impair the continuing compliance of an investment firm with the conditions and obligations of its authorisation or its financial performance, or the soundness or the continuity of its investment services and activities.”

Put simply, the maturity of the contract and capabilities of the Retained Organisation need to be at a higher level when outsourcing ‘critical operational functions’ compared to what is required when outsourcing a less-than-critical function.

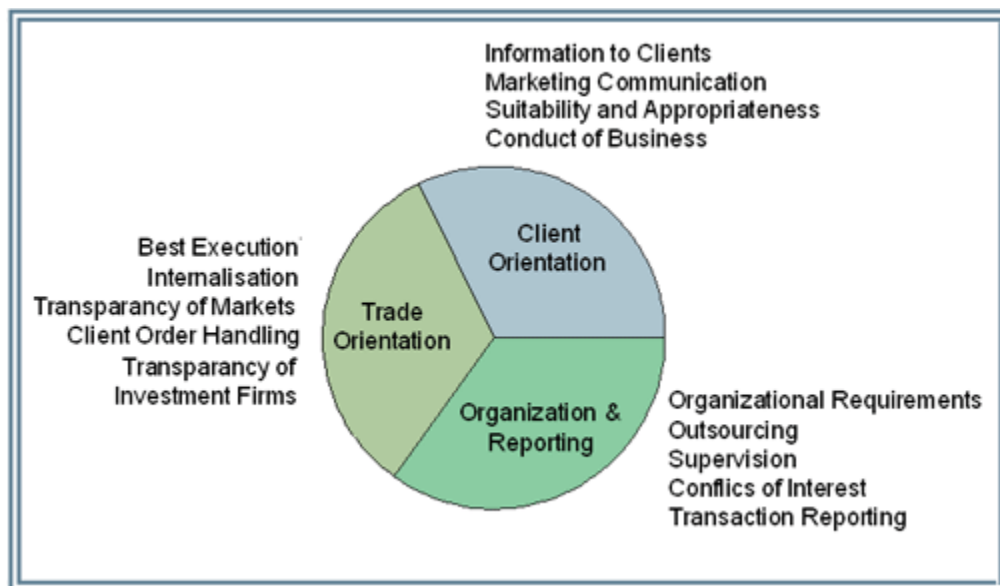


Figure 2: Overview of MiFID (Source: Protiviti, based on Level 2 Directive, August 2006)

Below are two quotes, the first of which needs to be addressed in the exit clauses of the contract:

“..the investment firm must be able to terminate the arrangement for outsourcing where necessary without detriment to the continuity and quality of its provision of services to clients..”

This requires the investment firm to think in terms of regularly updated exit plans that incorporate overviews of key personnel, assets, tools, procedures, disentanglement arrangements, and contracts with other third parties used by the service provider to deliver its services.

The second MiFID quote reads:

“..appropriate action must be taken if it appears that the service provider may not be carrying out the functions effectively and in compliance with applicable laws and regulatory requirements.”

In other words, if the service provider is underperforming, the investment firm needs to have adequate mechanisms embedded in the contract to influence the behaviour of the service provider. Consider stick-and-carrot mechanisms, contract change procedures, and liability clauses.

These excerpts provide two key messages: a) outsourcing does not relieve a Financial Institution from its responsibilities and liabilities, and b) the Financial Institution outsourcing a business process should ensure the same degree of control as it would when performing the activities in-house.

The next section briefly outlines the lifecycle of a BPO initiative and then describes the creation of a fit-for-the-job outsource risk management framework.

The sourcing lifecycle and its risks

The lifecycle of any sourcing initiative consists of four segments: implementation, transfer and transformation, delivery, and termination. Implementation begins with defining the sourcing strategy and ends with a signed contract (see figure 3). During the implementation project, the Financial Institution is in the lead and the controls are aimed at not being ‘out negotiated’ by the service provider. With the second project, transfer and transformation⁴, the lead shifts to the service provider; the employees, assets and accompanying responsibilities are transferred from the Financial Institution to the service provider⁵.

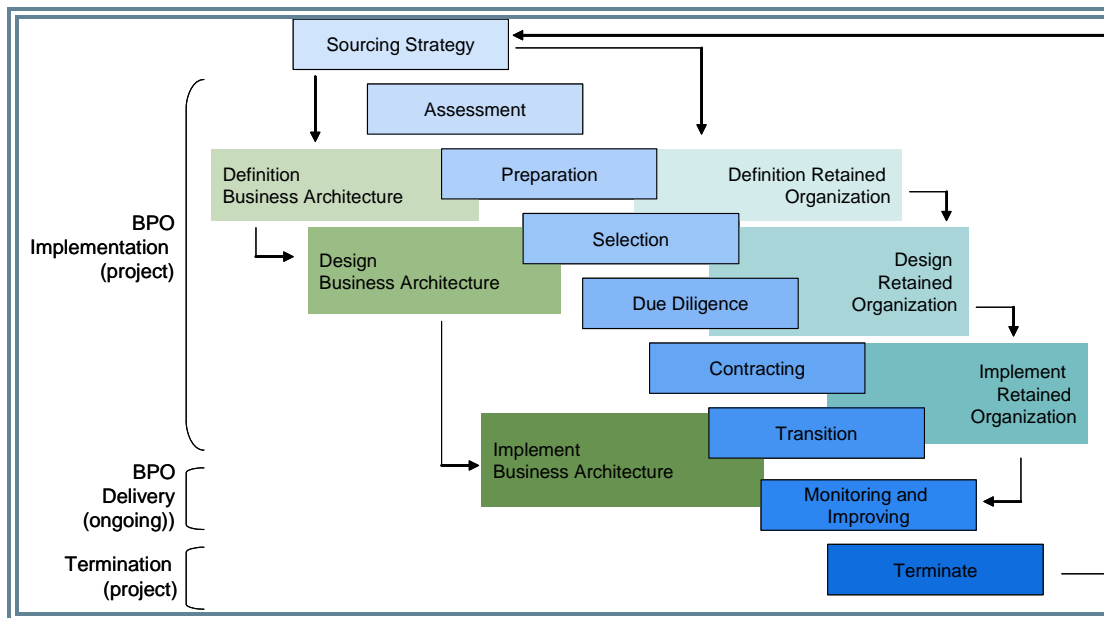


Figure 3: The BPO outsourcing lifecycle (Source: Protiviti 2007)

⁴ The objectives of the Transfer are shifting the responsibility for service delivery and the legal ownership of the assets to the service provider. During this phase the present mode of operation (e.g. service levels, procedures, technology) is typically maintained at the same level. During Transformation, various properties of the services are adjusted; the services migrate from Present Mode of Operation (PMO) to Future Mode of Operation (FMO).

⁵ The Financial Institution remains in all cases accountable for the performance of the service provider. Transferring responsibilities is meant, in this context, the day-to-day responsibility of the service provider to perform according to the contract and any additional mutually agreed addendums.

Upon transfer, the Financial Institutions' Retained Organisation starts managing the service provider on contract compliance. This ushers in the delivery phase that has a typical lifespan of three to seven years. The final project is termination which occurs upon contract-expiration; the contract can now be renewed, handed over to another third party or insourced.

Each segment of a BPO initiative has specific risks that must be mitigated however, there are also risks that are common throughout the lifecycle.

In order to create a manageable risk⁶ portfolio, Financial Institutions typically categorise risks in: credit risk, market risk, operational risk, liquidity risk, interest rate risk, legal risk, strategic risk and reputational risk. When outsourcing, the following risk categories are relevant:

- **Operational Risk.** The Basel Committee defines operational risk as follows: "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events." BPO Operational risk drill down is provided in figure 4.
- **Legal Risk** is the risk of loss resulting from legal penalties, such as the penalties arising from non-compliance with privacy laws like the Gramm-Leach-Bliley Act (GLBA) or Notification of Risk to Personal Data Act (NORPDA).
- **Strategic Risk** is the risk of loss due to dwindling capabilities necessary to achieve long-term, above-average growth in shareholder value. Examples of strategic outsourcing risks are losing capabilities and knowledge required to perform functions in-house, Intellectual Property Rights (IPR), and misalignment between sourcing strategy and the Financial Institutions overall strategy.
- **Reputational Risk** is the risk of loss due to negative press coverage to the BPO initiative. The term 'offshoring' is especially unlikely to receive a warm welcome by all stakeholders. In the United States negative national sentiment on offshoring jobs has already led to proposals for legislation on both national and state level^v. While in Europe, the discussion about the pros and cons of protectionism and market capitalism also regularly make it into the newspapers.

Of the categories mentioned, operational risk is the most likely to have a negative influence on the value of the BPO initiative. Losses due to legal, strategic and reputational risk are often a result of failing to mitigate operational risks. The remainder of the paper will therefore focus on identifying and mitigating operational BPO risks.

Managing operational BPO risks

Black box and white box risk

Not all BPO risks should be managed the same way by the Financial Institution. Mitigation of some risks can be done using a 'black box' while others cannot. Looking at risks from a 'black box' perspective means the Financial Institution defines requirements or controls that the service provider must adhere to and report on, but with no need to know the internal means of operation.

⁶ This paper uses the following definition for 'risk': the threat or uncertainty related to the Financial Institution not achieving its objectives.

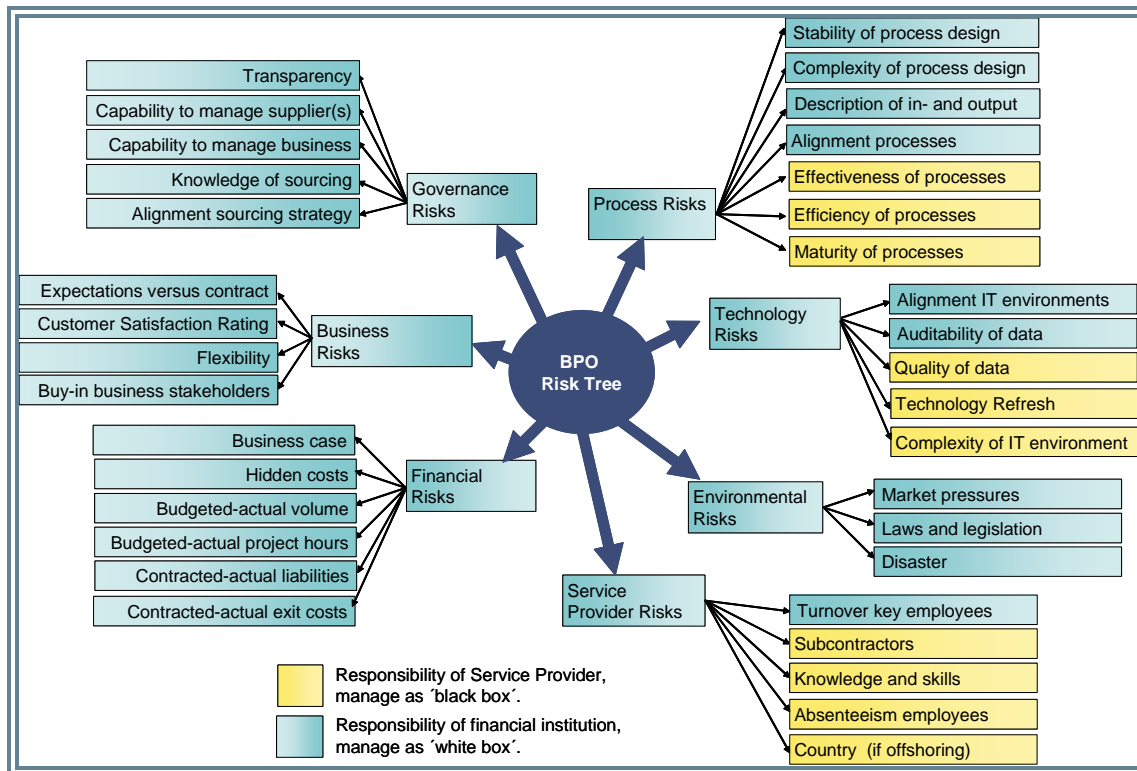


Figure 4: Typical BPO risk tree during the Sourcing Delivery phase (Source: Protiviti 2007)

However, not all risks can be managed this way. Certain risks require in-depth knowledge of the internal structure and workings of the service provider to ensure an acceptable risk level for the Financial Institution. This is known as a 'white box' or 'glass box' approach. Activities in figure 4 that have been performed within the Financial Institution itself are also considered to be 'white box.' The two examples below make it more tangible.

1. A technology risk is the quality of data that is sent from the service provider to the Financial Institution. The Financial Institution cannot handle the quality of data purely as the service providers' problem as that would lead to a 'garbage-in/garbage-out' scenario. The Financial Institution, however, should look at the quality of data in functional terms (e.g. accuracy, integrity, availability, completeness, and timeliness) and define thresholds or service levels for them. It should be left up to the service provider to operationalise the requirements. In this case, manage this risk as a black box.
2. A specific supplier risk is the turnover of key employees. Key employees possess skills, knowledge or expertise that are so valuable to the Financial Institution that it wants to influence the decision making process of the service provider when it comes to replacing them. Influencing the internal decision-making process of the service provider on this point means treating the risk as a white box.

Managing a risk as a black or white box needs to be reflected in a) the way it is translated into contract clauses and b) the way the service provider is controlled by the Retained Organisation. Benefits of this differentiation are more focused management attention, less ballast and thus ultimately lower cost—lower cost due to a smaller Retained Organisation and lower charges from the service provider for reporting and compliance services.

Taking the operational BPO risks that have been discussed so far, the following recommendations can be taken into account:

Recommendation 1: Create a holistic overview of all risks that might affect the value of a BPO initiative.

Recommendation 2: Wherever possible, manage outsourcing risks as a black box.

Determining whether a risk should be categorised black or white box is part of the Outsource Risk Management (ORM) methodology that is used by Protiviti to manage outsource risks effectively and at minimal cost.

Maturity-based Approach of Managing BPO Risk

Figure 5 provides a graphical representation of Protiviti’s ORM process. It is an ongoing, closed-loop process. As a one-off project it cannot ensure effective and efficient risk management over the whole life cycle of the BPO. Securing that continuous improvement is an integral part of the process—activities have been aligned with the Plan-Do-Check-Act cycle from Deming⁷.

eSCM-CL to enhance management capabilities

Ease of adoptability has been further increased by incorporating elements from the eSCM-CL standard⁸. This ‘best practise’ aims to gradually increase the capabilities of Retained Organisations to manage their service providers and outsource initiatives. However, as eSCM-CL is designed primarily to manage outsourced IT services it is only useful if replenished with specific vertical and business process focused additions.

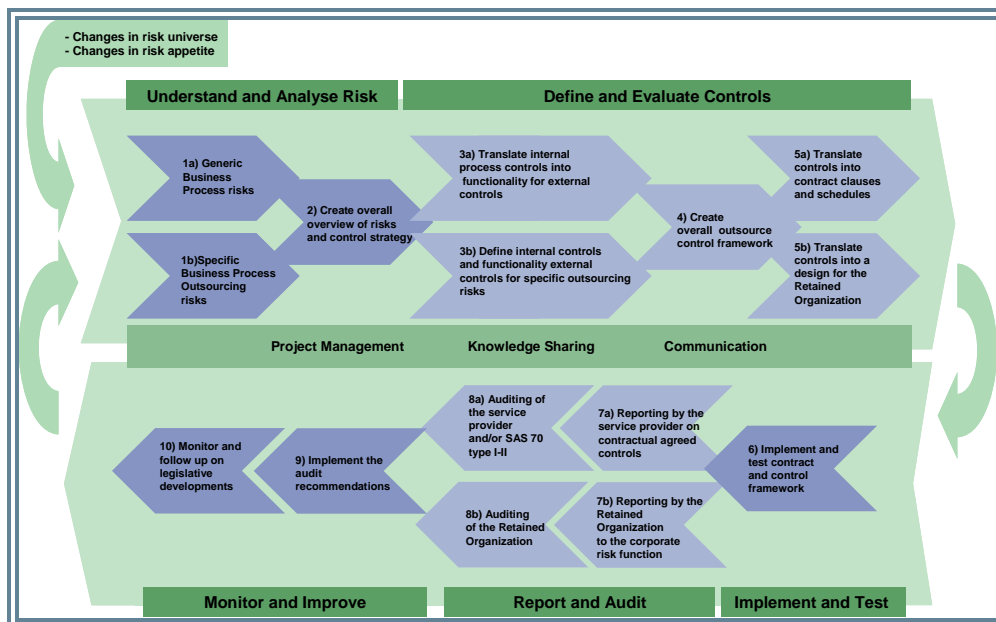


Figure 5: ORM process at eSCM-CL level 2+ (Source: Protiviti 2007)

⁷ Deming (1900 – 1993) proposed in the 1950's that business processes should be analyzed and measured to identify sources of variations that cause products to deviate from customer requirements. He recommended that business processes be placed in a continuous feedback loop so that parts of the process needing improvement could be identified. Based on the work by Walter Shewhart, Deming created for his students the Plan-Do-Check-Act cycle as a simplified version of his methodology.

⁸ The eSourcing Capability Model for Client Organisations (eSCM-CL) is a “best practise” capability model developed to give clients of IT-enabled services guidance toward improving their capability across the sourcing life-cycle. Additionally, it provides client organisations with an objective means of evaluating their sourcing capabilities (Source: The eSourcing Capability Model for Client Organisations (eSCM-CL): Practise Details V1.1, Carnegie Mellon University, July 2006. Note of author: despite that the model is aimed at managing IT sourcing initiatives it does provide useful input for managing business process sourcing initiatives as well.

This combination of best practises and Protiviti’s hands-on experiences are described in the next paragraphs. It describes the ORM process using the example of mitigating legislative risk to make the theory more tangible.

Understand and Analyse Risk

Creating a BPO control framework is rarely a Greenfield situation. In all cases, except for a start-up, applicable laws and legislation have already been translated into entity objectives and the COSO ERM framework, providing a good foundation for the implementation of ORM.

The first two activities (1a and 1b) of Understanding and Analysing Risk (figure 5) lead, in this case, to an overview of all legislative requirements in-scope of the BPO.

- Generic regulatory requirements with which the business process must comply irrespective of being outsourced or not.
- Specific regulatory outsource requirements that become relevant only when considering outsourcing or creating a shared service centre.

The regulatory risks the Financial Institution is required to address should be incorporated into a holistic risk tree. This tree would look like figure 4, but with one more level of detail.

Based on the risk tree, the impact of the BPO on the overall risk-return profile of the outsourced portfolio can be determined. This, combined with the risk appetite of the Financial Institution, prescribes the extent of the required outsource control framework. Part of such an exercise is represented in table 1.

Objective: Risk factors	Mitigation on specific outsource risk					
	Impact of risk	Probability of risk	Criticality of Risk (Impact x Probability)	Acceptable Risk Level	Mitigation strategy (Treat, Take, Terminate, Transfer)	Projected cost of mitigation
Default of service provider. (Basel II)	€45 [#]	0.1	4.5	€10	Not required, threshold not exceeded	-
Operational breakdown service provider. (Basel II)	€15 [%]	10	150	€40	Treat by continuity plans and Transfer by liability clauses	15% of contract value
Protect any confidential information (MiFID)	€20 ^{&}	5	100	€10	Treat by controls and audits and Transfer by liability clauses.	2% of contract value
Capability to manage the service provider. (Basel II and MiFID)	€12 [!]	5	60	€10	Treat by implementing capable Retained Organisation.	2% of contract value

Table 1: Quantitative approach of creating an outsource control framework (Source: Protiviti 2007)

[#] Base impact on projected project costs to insource or outsource to other third party.
[%] Base impact on historical downtime costs within own organisation.
[&] Base on historical average cost of brand damage and legal fines due to similar events.
[!] Derive impact from historical cost curve versus the expected benefits from outsourcing.

Define and Evaluate Controls

Functional requirements of a control

The third activity (3a and 3b) starts with categorising risks exceeding the acceptable-risk-threshold as a black or white box. This requires an in-depth understanding of the individual risk and potentially matching controls⁹. Based on this understanding the *functional* requirements of the controls can be defined as well as how the Financial Institution wants to implement them within the outsource relationship.

The resulting functional design of the outsource control framework can now be aligned and incorporated into the overall Enterprise Risk Management (ERM) framework. The following Basel II quote shows that this is a good practise:

“In some instances (...of outsourcing), banks may decide to either retain a certain level of operational risk or self-insure against that risk. Where this is the case and the risk is material, the decision to retain or self-insure the risk should be transparent within the organisation and should be consistent with the bank’s overall business strategy and appetite for risk.”^{vi}

After alignment, the outsource control framework is ready to be translated into contract clauses and schedules (5a). For those risks managed via black box, properties like suitable evidence, reporting frequency, SMART key control indicators, trend-lines and auditability requirements have to be defined. Risks labeled white box should be discussed with the service provider resulting in a suitable control design.

- Recommendation 3:** Translate, wherever possible, risk impact into a monetary value and incorporate it and its mitigation cost into the business case.
- Recommendation 4:** Implement a *process* to continuously monitor the alignment between sourcing objectives, sourcing risks, and contractually agreed controls.
- Recommendation 5:** Align outsource risk management with enterprise risk management (ERM).

Executing activity 5b results in two deliverables—the first one is a governance and process design for the Retained Organisation covering subjects like:

- Positioning within Financial Institutions structure.
- Strategic objectives (e.g. lower cost by 15% over three years, increase standardisation with 10%) and strategic Key Performance Indicators (e.g. number of escalations on strategic level, amount of non-standard services).
- Role descriptions capturing responsibilities, mandate and main activities of key persons within the Retained Organisation.
- Design of the governance and control framework (e.g. managing demand, business architecture, risk, cost, projects and quality).
- Description of the interfaces with internal business units and external service provider.
- Overview of meetings on strategic, tactical and operational level, their frequency, participants, duration and basic agenda.
- Reporting structure explaining who is reporting when, what, and to whom.

The second deliverable is derived from the first and is a contract schedule describing in detail the way the Financial Institution and the service provider interact with each other.

⁹ This paper uses the following definition for Control: The policies, procedures, practices and organisational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected (Source: CobiT 3rd Edition Control Objectives, CobiT Steering Committee and the IT Governance Institute, 2000).

Implement and Test

The sixth activity requires both the Financial Institution and service provider to implement and test the contract and control framework. It is advisable that the Financial Institution finishes the implementation of its Retained Organisation the moment the Transition phase starts—this is to prevent a management vacuum and reduce the risk of a quality dip.

Recommendation 6: Ensure all in- and output elements marked in the contract as relevant have named owners within the Retained Organisation and service provider.

Recommendation 7: Negotiate not just a single norm for key performance and control indicators but also, where desirable, multi-year trend lines.

Report and Audit

Activities seven and eight create the desired feedback loop providing insight into the effectiveness of the control framework. Potential areas of concern as a result of gaps between desired and actual control effectiveness is shown in figure 6—and of course this risk has not gone unnoticed by regulators:

“Institutions should implement an oversight program to monitor each service provider’s controls, condition, and performance. Responsibility for the administration of the service provider relationship should be assigned to personnel with appropriate expertise to monitor and manage the relationship.”^{vii}

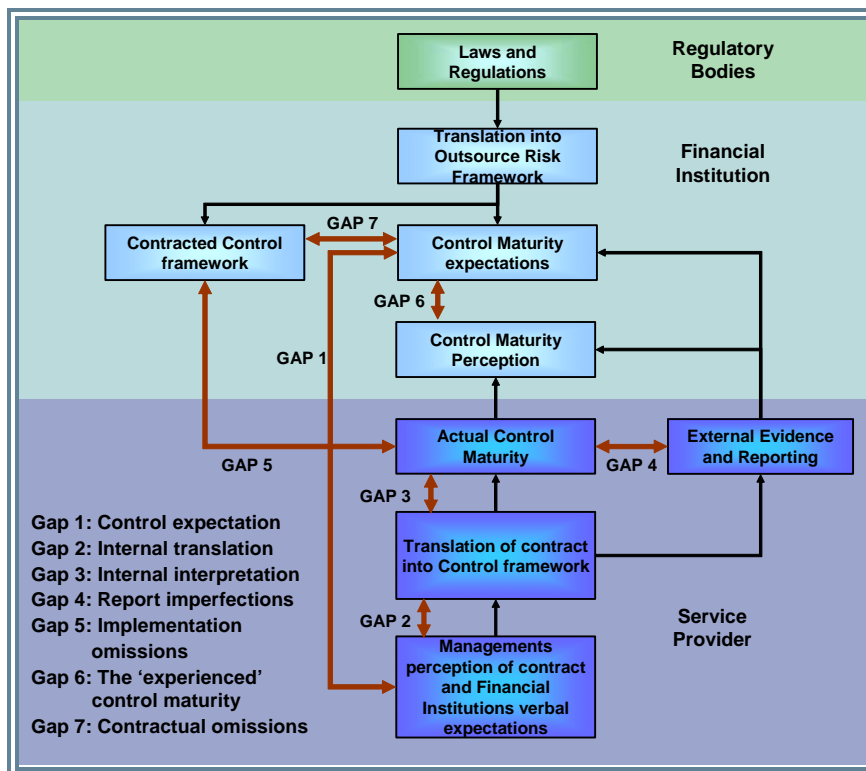


Figure 6: Potential gaps between expected and actual control (Source: Protiviti 2007)

Figure 6 shows the step-by-step translation of a regulatory requirement into a control within the domain of the service provider. This translation is done by people and people make interpretations and have expectations, leading to the depicted 'gaps.'

Implicit expectations are a source of risk

The first gap originates from the Financial Institutions' compliance experts having expectations on how the service provider will design and implement their control framework. The extent of the first gap depends largely on the ability of these experts to translate their implicit expectations into explicit contract clauses, and the capability of the service provider to capture the *actual* demand of the Financial Institution.

The figure shows many more potential gaps, but the messages are a) make implicit expectations explicit and b) include a thorough but flexible control framework in the contract.

Monitor and Improve (... and truly add value)

Auditing by internal and external auditors is one of the means to make control gaps transparent and trigger improvements. Common practise is that improvements recommended by external auditors are implemented at the cost of the service provider, while the cost of executing the internal audit advice is open for negotiation.

Create true audit value by linking controls to financial return

Audit reports providing recommendations to bridge control gaps are valuable, but even more value is created if auditors are capable of selecting controls that mitigate legislative risks *and* improve the financial bottom line of the Financial Institution. Below is a concrete example of how this can be done using the following Basel II requirement^{viii}:

"...banks should understand the potential impact on their operations and their customers of any potential deficiencies in services provided by vendors...(and) the extent of the external party's liability and financial ability to compensate the bank for errors, negligence, and other operational failures should be explicitly considered..."

Such a 'deficiency' could be the inability of the service provider to deliver processed mortgages due to an IT problem within the service providers' data centre. This is an example of a risk becoming increasingly relevant as 'bundling' IT Outsourcing (ITO) and BPO wins in popularity.

The annual direct financial loss the Financial Institution incurs due to this risk can be calculated by multiplying the number of problems, average resolution time, average number of effected users and lost revenue per hour of idle time. Experience shows that companies are often startled when confronted with, even roughly calculated, figures.

The next table describes both the typical standard control objective used to mitigate this risk, complimented by two more business-value oriented control objectives. The standard control objective ensures the service provider creates documentation and that it registers the input of the process, but provides hardly any guarantees to safeguard against a garbage-in garbage-out scenario.

Risk	Control Objective	Control Objective
Managing operations addresses how an organisation maintains reliable application systems in support of the business to initiate, record, process and report financial information. (Source: General IT Control Framework).	IT management has defined and implemented problem management controls to ensure that all operational events that are not part of the standard operation (incidents, problems and errors) are recorded and analysed in a timely manner to minimize re-occurrence of the problem. Service level (e.g. in service level agreements) are to be defined and managed to support the monitoring of financial reporting system requirements (Source: General IT Control Framework).	Typical implementation of this <u>white box</u> control results in backups being made, procedures created to manage incidents and problems and calls being registered and managed. The control however does <u>not</u> ensure less downtime, it just allows for downtime being properly documented and signed-off.
	IT management has defined and implemented management controls to ensure the average number of all operational events that are not part of the standard operation (incidents, problems and errors) are reduced with an in the SLA predefined yearly percentage (Source: Protiviti).	Steering on these <u>black box</u> control objectives force the IT function (regardless internal or external) to reduce the loss due to IT outages annually. The control implicitly forces the service provider to implement a problem management process, record and analyse problems and active manage service levels because it will otherwise not be able to achieve the control objective.
	IT management has defined and implemented management controls to ensure the average resolution time of all operational events that are not part of the standard operation (incidents, problems and errors) are reduced with an in the SLA predefined yearly percentage (Source: Protiviti).	Value is high as it combines the requirement for a controlled and documented process with annually declining financial loss due to this risk.

Table 4: Combining standard and value adding controls (Source: Protiviti 2007)

Value-based Outsource Risk Management

The second and third control objectives approach the risk from the view point that the service provider is held accountable to reduce the loss incurred by the Financial Institution due to this specific risk annually. It focuses on the desired *end result* from a business perspective. One could describe this approach as Value-based Outsource Risk Management and can be applied on both BPO and ITO.

Value-based outsource risk management is, however, not achievable from day one. It requires a maturity-based approach (e.g. CMM of eSCM) structuring the growing capabilities of both Retained Organisation and service provider.

This approach requires specific arrangements to be made to the legal contract and underpinning schedules. Key success factors of this approach are trust and flexibility as the initial contract can only contain a detailed description for the first two years and objectives for subsequent years.

- Recommendation 9:** Invest in thorough transcription of compliance expectations into contract clauses plus a ‘honeymoon’ period with mechanisms for re-negotiation.
- Recommendation 10:** Distil the essence and overlap out of the forest of regulations and buckets of controls and compile a framework of *true* key control indicators.
- Recommendation 11:** Merge wherever possible legislative controls with controls that improve the financial bottom line.
- Recommendation 12:** Allow in the contract a maturity-based control framework that requires both the Financial Institution and service provider to enhance its capabilities over time.

By quantifying risk, it becomes even possible to add it as a value driver in the outsource dashboard, depicted in figure 7. The outsource dashboard provides management with valuable steering information at a glance by displaying a set of key metrics consolidating underlying data provided by both service provider and Retained Organisation.

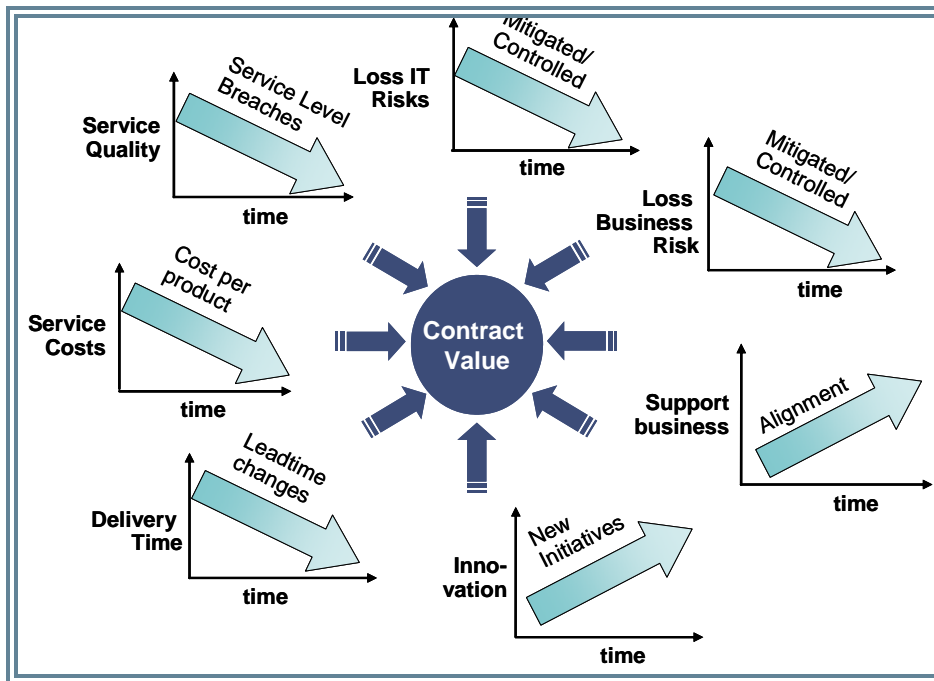


Figure 7: Outsource Value Dashboard (Source: Protiviti 2007)

Another benefit of a dashboard is the assurance that ORM is implemented as a continuous process and locked within the control processes of the Retained Organisation. Last, but not least, the support approach demonstrating compliance to the following MiFID requirement^{ix}—“the service provider must properly supervise the carrying out of the outsourced functions, and adequately manage the risks associated with the outsourcing.”

To recapitulate the last chapter; ORM demonstrates the Financial Institutions commitment to proactively identify, assess and manage operational BPO risks in order to optimise the value of the BPO. Additional value can be achieved when the Financial Institution and service provider are able to embed a continuous, maturity-based, improvement cycle within the contract and *relationship*.

START FRAME 1: SAS 70 at a glance

In response to the need to understand the service providers' control environment, companies turn increasingly to requesting a Statement on Auditing Standards number 70 (SAS 70) report.

SAS 70 is based on SAS 55 (Consideration of Internal Control in a Financial Statement Audit) and on the Committee of Sponsoring Organisations of the Treadway Commission (COSO) framework. SAS 70 reports come in two formats: Type I and Type II. Type I is a description of control activities while Type II includes the testing of controls over a period of time (typically six months).

The SAS 70 is actually a hybrid audit that includes many of the audit objectives performed during operational audits with a close secondary focus on the information technology that supports the business process and may even include elements of financial audits^x.

A SAS 70 can be useful, but only when it is applied with care. Some of the issues are:

- If the service provider defines the scope itself, it is likely to include those controls with which it feels comfortable.

- If there are no issues reported in the SAS 70 report it is likely that the service provider selected the scope very carefully and did not include complex process activities as they are more likely to show issues over time (in case of a Type II SAS 70 report).
- Some service providers may market themselves as being SAS 70 compliant but there is no such thing as a SAS 70 compliant organisation.

In short, a SAS 70 report has its uses, but its value depends highly on the expertise available within Financial Institutions' Retained Organisation and audit department as these can ensure that relevant services, processes and controls are included in the audit scope.

END FRAME 1: SAS 70 at a glance

START FRAME 2: The Retained Organisation

A Retained Organisation ensures efficient and effective control of existing outsourcing services and professional acquisition of new services allowing the Financial Institution to act as a "professional customer."

The primary tasks of the Retained Organisation, sometimes also called 'Service Management Organisation' or 'Demand-Supply Organisation' are:

- Fulfilling demand from the Financial Institution by purchasing and managing suitable supply from external service providers.
- Aligning and governing the relationship on tactical and operational levels.
- Gathering and applying of specific industry and BPO knowledge and competencies.

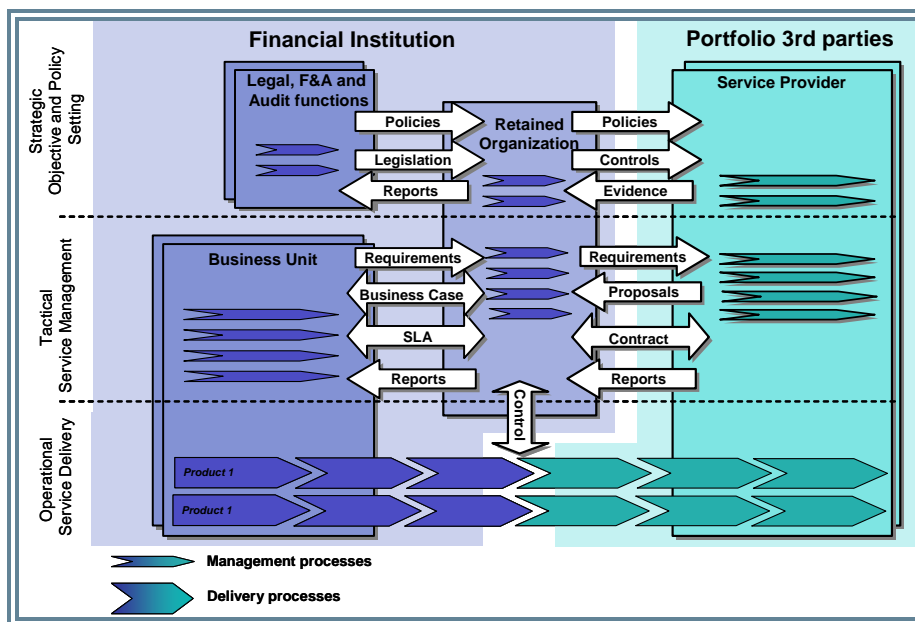


Figure 8: Schematic overview of a Retained Organisation and its interfaces (Source: Protiviti 2007)

The eSCM-CL model identifies some 17 capability areas enabling the organisation to effectively manage their outsourcing activities and relationships. Of these areas, eight are associated with the BPO Implementation phase and the remaining nine with the ongoing BPO Delivery phase (figure 3). However, discussing all these capabilities is outside the scope of this white paper¹⁰.

¹⁰ More information about eSCM can be found on: <http://itsqc.cs.cmu.edu/>.

In some cases the more operational activities required to manage the end-to-end value chain are executed by a specialised third party instead of the Retained Organisation. The concept is known as a Managed Service Provider (MSP) and gains in popularity as Financial Institutions often lack the resources and knowledge to manage these complex processes themselves.

However, an MSP is no silver bullet and requires, among others, specific arrangements to ensure it has the mandate to effectively manage the other third parties in the chain. The Retained Organisation *always* remains end-responsible for the performance and legislative compliance of any of the third parties.

END FRAME 2: The Retained Organisation

ⁱ Gottfredson M., Puryear R, Philips S., Strategic Sourcing, from Periphery to the Core, Harvard Business Review, February 2005.

ⁱⁱ Zielemans F., IT value preservation in the SOX-era, BS15000 and IPWMM as means for effective management control, White Paper Quint Wellington Redwood, 2005.

ⁱⁱⁱ Basel Committee on Banking Supervision, Sound Practices for the Management and Supervision of Operational Risk, February 2003.

^{iv} The commission of European communities, Implementing Directive 2004/39/EC of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms, and defined terms for the purposes of that Directive, June 30 2006.

^v Benvenuto N., Brand D., Managing the Risks of Outsourcing in a Post-Sarbanes World, Information Systems Control Journal, Volume 5, 2004.

^{vi} Basel Committee on Banking Supervision, Sound Practices for the Management and Supervision of Operational Risk, February 2003.

^{vii} FFIEC, Risk Management of Outsourced Technology Services, November 28, 2000.

^{viii} Basel Committee on Banking Supervision, Sound Practices for the Management and Supervision of Operational Risk, February 2003.

^{ix} The commission of European communities, Implementing Directive 2004/39/EC of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms, and defined terms for the purposes of that Directive, June 30 2006.

^x Frenette, J., SAS 70 Primer, EDPACS, The EDP audit, control and security newsletter, May 2002 Vol. XXIX, Number 11.

Article from Protiviti KnowledgeLeader – www.knowledgeleader.com.

KnowledgeLeader is a subscription-based website that provides audit programs, checklists, tools, resources and best practices to help internal auditors and risk management professionals save time, manage risk, and add value. Free 30-day trials available.

Protiviti is a leading provider of truly independent internal audit and business and technology risk consulting services. We help clients identify, measure and manage operational and technology-related risks they face within their industries and throughout their systems and processes. And we offer a full spectrum of audit services, technologies and skills for business risk management and the continual transformation of internal audit functions.

Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.