LEADMARK

contracts collaboration control

A Practical Guide on Managing Outsourcing Risk

How Risk Management forms a cornerstone of effective outsourcing governance

For further information: john.smit@leadmark.nl

Version 1.1

15-3-2017

Table of Contents

Acknowledgement

This Working Paper on risk management within an outsourcing governance framework presents our best current thinking on the topic and is intended to provide insight and encourage discussion internally and externally.
In writing this guidance we built on a) the guidance on managing outsourcing risk by the Board of Governors of the US Federal Reserve System, b) the work of Heiko Gewald and Daniel Hinz of the German Institute for Information Systems at the Johann Wolfgang Goethe University in Frankfurt am Main and c) the principles for the sound management of operational risk by the Basel Committee on Banking Supervision.

1. Introduction

Outsourcing governance and operational risk and are two major topics on today's agenda of top executives, especially in heavily regulated industries like financial services and the healthcare sector. The reasons for this are various like: continuous cost pressure, technical innovation, new regulatory laws and a dynamic business environment. Leadmark uses a comprehensive governance framework to highlight the potential risk arising from the use of service providers and to effective control the engagement to maximize value.

This guidance describes the elements of an appropriate service provider risk management program.
For purposes of this guidance, "service providers" is broadly defined to include all entities that have entered into a contractual relationship with an organization to provide business functions or activities which may include, Human Resource Management, Accounting, Information Technology and Facility Management.

Not all concepts presented in this guidance are original, indeed parts are built on accepted thinking and practices. However, they are not commonly known in the context of the sourcing governance. The aim of this document is to provide insight in a risk management approach within a coherent framework for governing sourced services and third party relationships.

2. Risks from the Use of Service Providers

The use of service providers to perform operational functions presents various risks to organizations.
In this context a risk is defined as a set of circumstances that hinder the achievement of objectives.
Some risks are inherent to the sourced service itself, whereas others are introduced with the involvement of a third party service provider. Risks can be the result of poor design of the engagement or emerge from poor supplier performance or poor governance. If not managed effectively, these risks can result in operational disruption, financial loss, loss of reputation and regulatory or legal action. Risk assessments are therefor a critical component of the governance of sourced services or third party relationships. They can be conducted at various levels of the organization, from different points of view and at different moments during the life cycle of the engagement. The objectives and events under consideration, determine the scope of the risk assessment to be undertaken. Organizations should consider the following categories of operational risk during the life cycle of the deal:

Engagement risk includes:

i. *Strategic risk* arises when the services, products or activities of a service provider no longer align with the strategic intent, requirements of the organization or user/client expectations. Also in this category are longer term risks, such as losing the capability to execute outsourced processes in-house due to loss of talent and knowledge.

ii. *Provider risk* arises when the service provider operates in an unsustainable manner (i.e. insufficient access to knowledge) or when service delivery is not in compliance with applicable laws and regulations.

iii. *Relational risk* arises from poor communication and management of the engagement.

Delivery risk includes:

i. *Service risk* arises from services, products or activities of a service provider which do not align with contractually defined service levels.

ii. Financial risk arises when services, products or activities of a service provider generate higher costs or when financial processes are not executed correctly and conscientiously.

iii. *Coordination risk* arises from the complexity of the arrangement which refers to the number of entities (e.g. contracts, processes, people, technologies, risks, issues) and relationships (e.g. multi sourcing) that have to be managed simultaneously to realize engagement objectives.

Definition of operational risk

Operational risk is "the risk of a change in value in terms of quality, cost or speed of delivery, caused by the fact that actual losses, incurred from inadequate or failed internal processes, people or systems, or from external events (including legal risk), differ from expected losses."

Examples of other types of operational risks assessments (not specific to sourcing or third parties):

- *Strategic risk assessment* refers to the evaluation of risks relating to the organization's mission and strategic objectives, typically performed by senior management teams in strategic planning meetings, with varying degrees of formality.

- *Compliance risk assessment* refers to the evaluation of risk factors relative to the organization's compliance obligations, considering laws and regulations, policies and procedures, ethics and business conduct standards, and contracts, as well as strategic voluntary standards and best practices to which the organization has committed. This type of assessment is typically performed by the compliance function with input from business areas.

- *Internal audit risk assessment* refers to the evaluation of risks related to the value drivers of the organization, covering strategic, financial, operational, and compliance objectives. The assessment considers the impact of risks to shareholder value, as a basis to define the audit plan and monitor main risks. This top-down approach enables the coverage of internal audit activities to be driven by issues that directly impact shareholder and customer value, with clear and explicit linkage to strategic drivers for the organization.

- *Fraud risk assessment* refers to the evaluation of potential instances of fraud that could impact the organization's ethics and compliance standards, business practice requirements, financial reporting integrity, and other objectives. This is typically performed as part of Sarbanes-Oxley compliance or during a broader organization-wide risk assessment, and involves subject matter experts from key business functions where fraud could occur (e.g., procurement, accounting, and sales) as well as forensic specialists.

- *Security risk assessment* refers to the evaluation of potential breaches in an organization's physical assets and information protection and security. This considers infrastructure, applications, operations, and people, and is typically performed by an organization's information security function.

- *Information technology risk assessment* refers to the evaluation of potential for technology system failures and the organization's return on information technology investments. This assessment would consider such factors as processing capacity, access control, data protection, and cyber crime. This is typically performed by an organization's information technology risk and governance specialists. In IT sourcing this type risk would be regarded a service risk.

3. Board of Directors and Senior Management Responsibilities

The use of service providers does not relieve an organization of its accountability to ensure that sourced activities are conducted in a safe-and-sound manner, and in compliance with applicable laws and regulations.
This responsibility lies inalienable with the organization's Board of Directors or senior management.
Policies governing the use of service providers should be established and approved by the Board of Directors, or senior management. These policies should establish a service provider governance framework that addresses risk assessment and due diligence, standards for contract provisions and considerations, ongoing monitoring and steering of service providers, and business continuity and contingency planning.

Senior management is responsible for ensuring that board-approved policies for the use of service providers are appropriately executed. This includes overseeing the development, implementation and execution of an appropriate governance framework that includes risk management, reporting and ongoing supplier monitoring and steering. Senior management is also responsible for regularly reporting to the Board of Directors on adherence to policies governing sourced services and third party arrangements.

4. Service Provider Governance

The governance of sourced services and service providers is not an end in itself. It is a means to drive value by realizing the business objectives of sourcing and supplier relationships, while minimizing risk and costs.

An effective governance approach provides a clear insight in the performance of a supplier and the risks associated with the service being delivered. It makes sure the controls commensurate with the level of value at risk presented by the sourcing engagement. A lack of controls will leave the organization exposed to value loss. An excess of controls on the other hand will result in unnecessary efforts and costs.

Effective governance should prioritize quality control by the service provider. By entering into the engagement, the supplier has taken responsibility for meeting its service obligations under the contracted conditions. It may be expected that the supplier has an effective quality management system and supporting processes in place to meet its value proposition. The sourcing company should focus on verifying the service provider's quality system and processes that underpin the sourced services. The sourcing company manages the engagement by using a dynamic mix of controls, addressing the supplier's quality system, delivery processes and services provided, and takes action if performance is unsatisfactory or risk exceeds an acceptable threshold.

Summary of the basic principles of sourcing and supplier relationship governance:

1. the sourcing company is accountable for ensuring activities are conducted in a safe-and-sound manner and in compliance with applicable laws and regulations;
2. the supplier is responsible for the quality of its products and services;
3. the supplier manages its quality at a system, process and product/services level;
4. the supplier will ensure accurate and timely reporting on performance and risk;
5. governance should be based on a comprehensive framework;
6. the framework should balance value and risk and ensure monitoring and control;
7. the framework should ensure productive cooperation between parties to the engagement.

At Leadmark we have included these starting points in our comprehensive Value-Led governance approach. Value-Led governance provides a framework to monitor and steer the service provider's performance to maximize value, while minimizing risk and costs. It utilizes a dynamic set of metrics and controls, relevant to the risk impacting the achievement of objectives within the agreed boundaries of quality, cost and time. Applying the Value-Led governance framework will yield the following benefits:

Focus
By putting a strong emphasis on value and risk, it helps governance teams to focus on the things that really matter and to not get distracted by the noise that often surrounds sourcing engagements.
It helps to drive value whilst at the same time reduce costs and mitigating risks.

Transparency
It focuses thoughts on what will the supplier will deliver, why, when, by whom and how it is controlled.

Lean and agile
The standard way of working, its focus on value and risk and the dynamic mix of controls targeted at the supplier's quality system and processes, allows the organization to be lean and agile resulting in lower costs of control.

Quality of Service
Complementary to preventive system and process controls, product controls provide a post delivery check on the quality of service. The combination of controls allows effective steering on service improvements and reduction of failure costs.

Common way of working
It provides an sourcing organization a common approach and vocabulary that can be applied across the organization to all sorts of sourced services contracts. This makes it easier for people to work together, switch between governance teams and standardize management reporting.

Continuous improvement
It provides an existing body of knowledge that prevents an outsourcing organization to reinvent the wheel when it enters into an arrangement. It also allows an organization to learn and continuously improve its governance capabilities.

Collaboration
It strengthens collaboration because a structured approach makes it clear to the supplier how the engagement is being managed, on what criteria and which actions are considered if service delivery is unsatisfactory or risks exceed an acceptable level. It allows the supplier to address issues proactively.

Risk Management
Risk management plays an essential role in the Value-Led framework.
The depth and formality of risk management within the Value-Led governance approach, depends on the criticality, complexity, value, and number of critical business activities being outsourced. An organization may have sourced critical business, but the number may be few and/or with highly reputable and trusted service providers with whom they have long standing relationships. Therefore, risk management may be simpler and use less elements and considerations. For those organizations, with higher levels of complexity, that may use many service providers for numerous business activities that have material risk it may be needed to use many more elements and considerations to manage the higher level of risk and reliance on service providers. Then there is also risk appetite to consider. This can be defined as 'the amount and type of risk that an organization is willing to take in order to meet its strategic objectives.

This document will focus on the approach to risk management within the Value-Led governance framework.

5. Service Provider Risk Management

While the activities necessary to implement an effective service provider risk management program can vary, based on the scope and nature of an organization's sourced activities, effective programs typically include the following core elements during the life cycle of the engagement.

A. Risk assessments;
B. Due diligence and selection of service providers;
C. Contract provisions and considerations;
D. Incentive compensation review;
E. Oversight and monitoring of service providers;
F. Business continuity and contingency plans.

5.1 Risk assessments

Risk assessment of a business activity and the implications of performing the activity in-house or having the activity performed by a service provider, are fundamental to the decision of whether or not to source.
An organization should determine whether sourcing an activity is consistent with the strategic direction and overall business strategy of the organization. An explicit decision needs to be made on why to source – what is the problem or objective – and what is expected from the sourcing arrangement. After that determination is made, an organization should analyze the benefits and risks of sourcing the proposed activity as well as the service provider risk, and determine cost implications for establishing the sourcing arrangement. Consideration should also be given to the availability of qualified and experienced service providers to perform the service on an ongoing basis. Additionally, management should consider the organization's capability to provide appropriate ongoing oversight and governance of the relationship. In this stage the focus is mainly on strategic, provider and coordination risk.

The risk assessment should be updated at appropriate intervals. An organization should revise its risk mitigation and control plans, if appropriate, based on the results of the updated risk assessment.

5.2 Due Diligence and Selection of Service Providers

An organization should conduct an evaluation of and perform the necessary due diligence for a prospective service provider prior to engaging the service provider. The depth and formality of the due diligence performed will vary depending on the scope, complexity and importance of the planned outsourcing engagement, the organization's familiarity with the prospective service providers, and the reputation and industry standing of the service provider. Throughout the due diligence process, organization technical experts and key stakeholders should be engaged in the review and approval process as needed.

The due diligence process includes a review of the service provider with regard to:

1. Business background, reputation and strategy;
2. Financial performance and condition;
3. Operations and internal controls.

1. Business background, reputation and strategy

Organizations should review a prospective service provider's status in the industry and corporate history and qualifications; review its background, reputation and its principals; and ensure that the service provider has an appropriate background check program for its employees.
The service provider's experience in providing the proposed service should be evaluated in order to assess its qualifications and competencies to perform the service. The service provider's business model, including its business strategy and mission, service philosophy, quality initiatives, and organizational policies should be evaluated. Organizations should also consider the resiliency and adaptability of the service provider's business model as factors in assessing the future viability of the provider to perform services.
Organizations should check the service provider's references to ascertain its performance record, and verify any required licenses and certifications. Organizations should also verify whether there are any pending legal or regulatory compliance issues (for example, litigation, regulatory actions, or complaints) that are associated with the prospective service provider and its principals.

2. Financial Performance and Condition

Organizations should review the service provider's financial condition and of its closely-related affiliates. The financial review may include:

- Most recent financial statements and annual report with regard to outstanding commitments, capital strength, liquidity and operating results;
- The service provider's sustainability, including factors such as the length of time that the service provider has been in business and its growth of market share for a given service;
- Its commitment (both in terms of financial and staff resources) to provide the contracted services to the organization for the duration of the contract;
- The adequacy of the service provider's insurance coverage;
- The adequacy of its review of the financial condition of any subcontractors;
- Other current issues the service provider may be facing that could affect future financial and/or operational performance.

3. Operations and internal Controls

Organizations are responsible for ensuring that services provided by service providers comply with applicable laws and regulations and are consistent with safe-and-sound business practices. Depending on the characteristics of the outsourced activity, some or all of the following may need to be reviewed on the adequacy of standards, policies and procedures:

- Internal quality systems and controls;
- Facilities management (such as access requirements or sharing of facilities);
- Training, including compliance training for staff;
- Security of systems and privacy protection of the organization's confidential information;
- Maintenance and retention of records;
- Systems development, maintenance and contingency planning;
- Service support and delivery;
- Employee background checks;
- Adherence to applicable laws, regulations and supervisory guidance.

5.3 Contract Provisions and Considerations

Organizations should understand the service contract and legal issues associated with proposed sourcing arrangements. The terms of service agreements should be defined in written contracts that have been reviewed by the organization's legal counsel prior to execution. The characteristics of the business activity being sourced and the service provider's strategy for providing those service will determine the terms of the contract. Elements of well-defined contracts and services agreements typically include:

1. Intent
   A starting point for every successful sourcing or third party relationship is a mutual understanding of intents and expectations. An arrangement where, for example, one party expects innovation while the other believes its all about stability is doomed from the start.

2. Scope:
   Contracts should clearly define the rights and responsibilities of each party, including:
   - Support, maintenance and customer service;
   - Contract timeframes;
   - Compliance with applicable laws, regulations and regulatory guidance;
   - Training and instructing of organization's employees;
   - The ability to subcontract services;
   - The distribution of any required statements of disclosures to the organization's customers;
   - Insurance coverage requirements;
   - Terms governing the use of the organization's property, equipment and staff.

3. Cost and compensation:
   Contracts should describe the compensation, variable charges, and any fees to be paid for non-recurring items and special requests. Agreements should also address which party is responsible for the payment of any legal, audit, and examination fees related to the activity being performed by the service provider. Where applicable, agreements should address the party responsible for the expense, purchasing, and maintenance of any equipment, hardware, software or any other item related to the activity being performed by the service provider.
   In addition, organizations should ensure that any incentives (for example, in the form of variable charges, such as fees and/or commissions) provided in contracts, do not provide potential incentives to take imprudent risks or drive inappropriate behaviour. For reason of manageability it is required that fees, expenses and other cost elements within the financial model of the engagement, have a clear relationship with elements in the service model. Without this relationship it will be very difficult to apply financial levers in case of underperformance.

4. Right to audit:
   Agreements may provide for the right of the organization or its representatives to audit the service provider's quality systems, processes or products/services and/or to have access to audit reports. Agreements should define the types of audit reports the organization will receive and the frequency of the audits and reports. The types of audit should be based on the risk profile of the engagement.

5. Establishment and monitoring of performance standards:
   Agreements should define measurable (SMART) obligations and performance standards, structured in a comprehensive service model aligned with business needs. A dynamic set of risk based controls and metrics should be clearly linked to the service obligations its targeted to monitor.

6. Confidentiality and security of information:
Consistent with applicable laws, regulations, and supervisory guidance, service providers should ensure the security and confidentiality of both the organization's confidential information and the organization's customer information.
Information security measures for sourced functions should be viewed as if the activity were being performed by the organization, and afforded the same protections. Organizations have the responsibility to ensure service providers take appropriate measures designed to meet the objectives of relevant security guidelines. These measures should be mapped directly to the security processes of the sourcing organization, as well as to be included or referenced in agreements between the organization and its service provider(s). These obligations also require specific controls.

Service providers should also address its use of sourcing organization's information and its customers . On this note we would advice organization to review the effects of the new European GDPR law which applies from 25 May 2018 to all EU member states.

7. Ownership and license:
Agreements should define the ability and circumstances under which service providers may use outsourcing organization property inclusive of data, hardware, software and intellectual property. Agreements should address the ownership and control of any information generated by service providers. If organizations purchase software from service providers, escrow agreements may be needed to ensure that organizations have the ability to access the source code and programs under certain conditions.

8. Indemnification:
Agreements should provide for service provider indemnification of outsourcing organizations for any claims against the organization resulting from the service provider's negligence.

9. Default and termination:
Agreements should define events of a contractual default, list of acceptable remedies, and provide opportunities for curing default. Agreements should also define termination rights, including change in control, merger or acquisition, increase in fees, failure to meet performance standards, failure to fulfill the contractual obligations, failure to provide required notices, and failure to prevent violations of law, bankruptcy, closure, or insolvency.
Contracts should include termination and notification requirements that provide organizations with sufficient time to transfer services to another service provider. Agreements should also address a service provider's preservation and timely return of data, records, and other resources.

10. Dispute resolution:
Agreements should include a dispute resolution process in order to expedite problem resolution and address the continuation of the arrangement between the parties during the dispute resolution period.

11. Limits on liability:
Service providers may want to contractually limit their liability. The sourcing organization should determine whether the proposed limitations are reasonable when compared to the risks to the organization if a service provider fails to perform.

12. Insurance:
Service providers should have adequate insurance and provide sourcing organizations with proof of insurance. Further, service providers should notify organizations when there is a material change in their insurance coverage.

13. Customer / employee complaints:
Agreements should specify the responsibilities of sourcing organizations and service providers related to responding to complaints. If service providers are responsible for complaint resolution, agreements should provide for summary reports to the sourcing organizations that track the status and resolution of complaints.

14. Business resumption and contingency plan of service provider:
Agreements should address the continuation of services provided by service providers in the event of operational failures. Agreements should address service provider responsibility for backing up information and maintaining disaster recovery and contingency plans. Agreements may include a service provider's responsibility for testing of plans and providing testing results.

15. Foreign-based service providers:
For agreements with foreign-based service providers, organizations should consider including express choice of law and jurisdictional provisions that would provide for the adjudication of all disputes between the two parties under the laws of a single, specific jurisdiction. Such agreements may be subject to the interpretation of foreign courts relying on local laws. Foreign law may differ from European / national law in the enforcement of contracts. As a result, organizations should seek legal advice regarding the enforceability of all aspects of proposed contracts with foreign-based service providers and the other legal ramifications of such arrangements.

16. Subcontracting:
If agreements allow for subcontracting, the same contractual provisions should apply to the subcontractor. Contract provisions should clearly state that the primary service provider has overall accountability for all services that the service provider and its subcontractors provide. Agreements should define the services that may be subcontracted, the service provider's due diligence process for engaging and monitoring subcontractors, and the notification and approval requirements regarding changes to the service provider's subcontractors. Special attention should be paid to any foreign subcontractors, as information security and data privacy standards may be different in other jurisdictions. Additionally, agreements should include the service provider's process for assessing the subcontractor's financial condition to fulfill contractual obligations.

5.4 Incentive Compensation Review

Organizations should also ensure that an effective process is in place to review and approve any incentive compensation that may be embedded in service provider contracts, including a review of whether existing governance and controls are adequate in light of risks arising from incentive compensation arrangements.
If the service provider represents the organization by selling products or services on its behalf, the organization should consider whether the incentives provided might encourage the service provider to take imprudent risks. Inappropriately structured incentives may result in reputational damage, increased litigation, or other risks to the sourcing organization. An example of an inappropriate incentive would be one where variable fees or commissions encourage the service provider to push products with higher profit margins without due consideration of whether such products are suitable or required for the customer.

5.5 Oversight and Monitoring of Service Providers

The delivery stage of outsourcing is of special interest, as this is the phase where operational risk actually manifests, risks in the earlier stages are envisioned and not materialized. To effectively monitor contractual requirements, outsourcing organizations should establish controls and performance metrics that the business line or relationship management determines to be indicative of acceptable performance and risk levels.
Sourcing organizations should ensure that personnel with oversight and management responsibilities for service providers have the appropriate level of expertise and stature to govern the outsourcing arrangement.
The oversight process, including the level and frequency of management reporting, should be risk-focused. Higher risk service providers may require more frequent assessment and monitoring and may require organizations to designate individuals or a group as a point of contact for those service providers.
Organizations should tailor and implement risk mitigation plans for higher risk service providers that may include processes such as additional reporting by the service provider or heightened monitoring by the sourcing organization. Further, more frequent and stringent monitoring is necessary for service providers that exhibit performance, financial, compliance, or control concerns. For lower risk service providers, the level of monitoring can be lessened.

Financial condition: Sourcing organizations should have established controls to monitor the financial condition of service providers to evaluate their ongoing viability.
In performing these assessments, organizations should review the most recent financial statements and annual report with regard to outstanding commitments, capital strength, liquidity and operating results. If a service provider relies significantly on subcontractors to provide services to organization, then the service provider's controls and due diligence regarding the subcontractors should also be reviewed.

Internal controls: For significant service provider relationships, organizations should assess the adequacy of the provider's quality control environment. Assessments should include reviewing available audits or reports and on-site inspections. Performance devaluations or security incidents at the service provider may also necessitate the organization to elevate its monitoring of the service provider. (e.g. more in-depth / frequent reporting or inspections)

Escalation of oversight activities: Sourcing organizations should ensure that governance processes include triggers to escalate oversight and monitoring when service providers are failing to meet performance, compliance, control, or viability expectations.

These procedures should include more frequent and stringent monitoring and follow-up on identified issues, on-site control reviews, and when an institution should exercise its right to audit a service provider's adherence to the terms of the agreement. Organizations should develop criteria for engaging alternative outsourcing arrangements and terminating the service provider contract in the event that identified issues are not adequately addressed in a timely manner.

5.6 Business Continuity and Contingency Considerations

Various events may affect a service provider's ability to provide contracted services. For example, services could be disrupted by a provider's performance failure, operational disruption, financial difficulty, or failure of business continuity and contingency plans during operational disruptions or natural disasters. Outsourcing organization contingency plans should focus on critical services provided by service providers and consider alternative arrangements in the event that a service provider is unable to perform.

When preparing contingency plans, organizations should:

- ensure that a disaster recovery and business continuity plan exists with regards to the contracted products and services;
- assess the adequacy and effectiveness of a service provider's disaster recovery and business continuity plan and its alignment to their own plan;
- document the roles and responsibilities for maintaining and testing the service provider's business continuity and contingency plans;
- test the service provider's business continuity and contingency plans on a periodic basis to ensure adequacy and effectiveness;
- maintain an exit strategy, including a pool of comparable service providers, in the event that a contracted service provider is unable to perform.

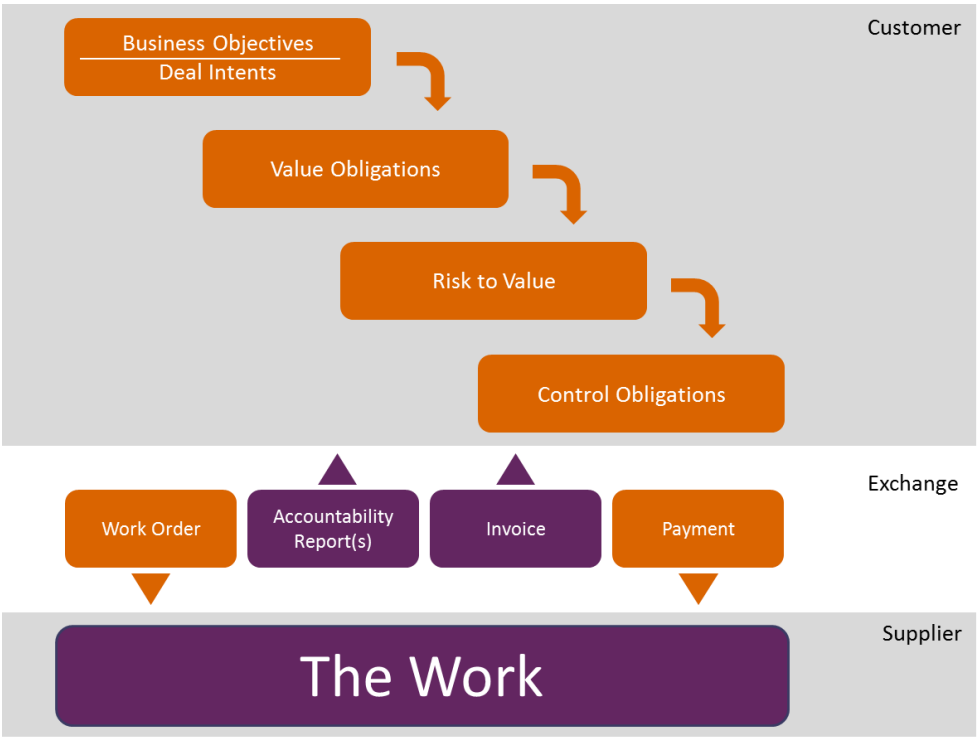

Figure 1: Risk in the basic structure of outsourcing

Fundamental principles of operational risk management:

- *Principle 1*: The board of directors should take the lead in establishing a strong risk management culture. The board of directors and senior management should establish a culture that is guided by strong risk management and that supports and provides appropriate standards and incentives for professional and responsible behavior.

- *Principle 2:* Sourcing organizations should develop, implement and maintain a risk framework that is fully integrated into the organization's overall risk management and sourcing governance processes.

- *Principle 3:* The board of directors should establish, approve and periodically review the framework. The board of directors should oversee senior management to ensure that the policies, processes and systems are implemented effectively at all decision levels.

- *Principle 4:* The board of directors should approve and review a risk appetite and tolerance statement for operational risk that articulates the nature, types, and levels of operational risk that the organization is willing to assume.

- *Principle 5*: Senior management should develop for approval by the board of directors a clear, effective and robust governance structure with well defined, transparent and consistent lines of responsibility. Senior management is responsible for consistently implementing and maintaining throughout the organization policies, processes and systems for managing operational risk in all of the organization's sourced material products, activities, processes and systems consistent with the risk appetite and tolerance.

- *Principle 6:* Senior management should ensure the identification and assessment of the operational risk inherent in all material products, activities, processes and systems to make sure the inherent risks and incentives are well understood. Approval process for all new products, activities, processes and systems that fully assesses operational risk.

- *Principle 7:* Senior management should implement a process to regularly monitor operational risk profiles and material exposures to value loss. Appropriate reporting mechanisms should be in place at the board, senior management, and business line levels that support proactive management of operational risk.

- *Principle 8*: Organizations should have a strong and auditable control environment that utilizes policies, processes and systems; appropriate internal controls; and appropriate risk mitigation and/or transfer strategies.

- *Principle 9*: Organizations should have business resiliency and continuity plans in place to ensure an ability to operate on an ongoing basis and limit losses in the event of severe business disruption.

- *Principle 10*: An organization's public disclosures should allow stakeholders to assess its approach to operational risk management.

6. The Risk Classification Framework

The risk classification framework is a critical building block of managing operational risk in sourcing.
The framework provides a practical tool which enables a structured way to assess the operational risks inherent to sourcing.

6.1 Overview of the model

The risk framework is based on a structured decomposition of the identified risks, by employing a matrix system which maps the sources of risk to the service areas where impacts resulting from those risks become apparent.

i. The left hand side of the matrix lists the sources of risk for each of the six operational risk categories mentioned in chapter 2. Within each category, four sources of operational risk are distinguished: processes, systems, people and external events, which can be further broken down into specific key risk drivers (KRDs). A KRD describes the event that results in a risk to one or more sourced services.

ii. The abscissa of the matrix lists the sourced services and key risk indicators (KRIs) of the impact areas quality, cost and time for each of the services sourced. A key risk indicator (KRI) is a metric for measuring the likelihood that the combined probability of an event and its consequence will have a significant negative impact on a service.

iii. If there is a cause-effect relationship between a KRD and a KRI, a risk indicator (RI) will be assigned to the intersection within the matrix. Each risk indicator has to be quantifiable to enable the measurement of the overall risk profile, and to allow an effective control to be determined for it. The Failure Mode and Effect Analyses (FMEA) method provides a practical approach to providing a priority to a risk indicator. It provides each risk indicator with a risk priority ranging from 1 (very low risk) to 1000 (very high risk). The calculation (RPN = S x O x D) is based on the Severity, Occurrence / Likelihood and Detection, with each factor having a value from 1 to 10. In this context Detection refers to the controls put in place to manage the risk.

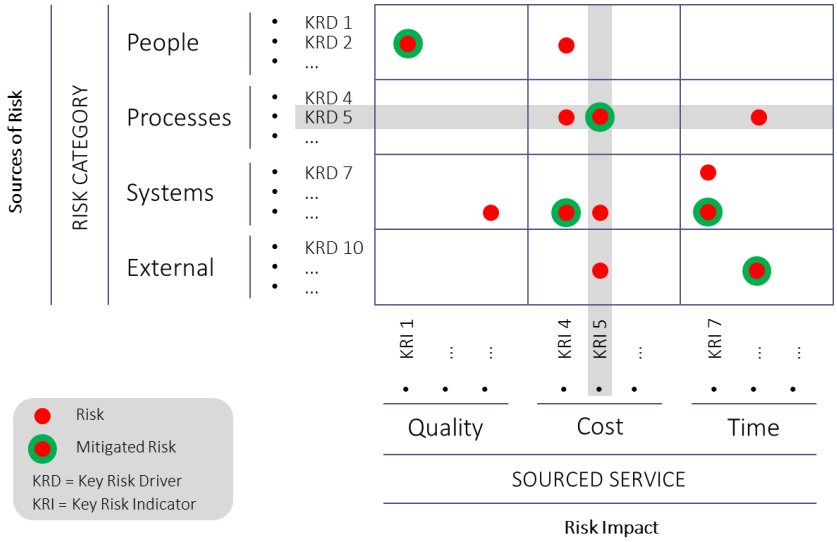

Figure 2: Risk Classification Matrix

6.2 Measurement driven classification

To assess the level of operational risk and its composition, the identified risks should fulfil three main criteria:

1. They have to be measurable to allow for a quantitative assessment;
2. They have to be mutually exclusive, so that double counting is avoided and it would complicate the definition of a clear metric to control the risk. E.g. a risk can not be caused by both a system event and a people event. These would be 2 separate risk, potentially effecting the same service.
3. The risks have to be completely exhaustive so that no relevant risks are missing in the assessment. A violation of this criterion would result in a risk assessment underestimating the risk position and leave risks unmanaged.

The risk classification matrix, with a comprehensive catalogue of sources of risk and mutually exclusive yet exhaustive system of measurable impact areas on the abscissa, ensures consistency with the criteria above. By applying the framework, the risks are assessed in a transparent way.

6.3 Sources of risk

The operational risk model focuses on risk sources within 6 categories of risk:

i. *Strategic risk* which arises when the services, products or activities of a service provider no longer align with the strategic intent or operational and financial requirements of the organization.

ii. *Provider risk* which arises when the services can no longer be provided in compliance with applicable laws and regulations or when the service provider otherwise operates in an unsustainable manner.

iii. *Relational risk* which arises from poor communication and management of the engagement.

iv. *Service risk* which arises from services, products or activities of a service provider which do not align with contractual defined quality standards or user expectations.

v. Financial risk which arises from services, products or activities of a service provider generate higher costs or when financial processes are not executed correctly and conscientiously.

vi. *Coordination risk* which arises from the complexity of the arrangement which refers to the number of entities (e.g. contracts, technologies, risks, issues) and relationships that have to be managed simultaneously to realize engagement objectives.

Within each of the six categories, four sources of operational risk are distinguished: processes, systems, people and external events. These four sources are further classified for the sake of ability to control them. They are either endogenous or exogenous, meaning controllable by the organization or not. A systems failure or process error is an endogenous event, as it is under control by the parties in the sourcing arrangement.
A natural disaster like an earthquake for example or amendment of the law is exogenous, as the occurrence of it cannot be influenced by the organization. Following this thought, external events are classified as exogenous, while risk resulting from processes, systems and people is endogenous. This distinction is important as within the framework we regard the sourcing engagement as endogenous, meaning the risk resulting from processes, systems and people is controllable by the sourcing organization and/or the service provider, therefore the service provider is not seen as external in this context and therefore defects resulting from the service provider are not exogenous. This view is supported by regulatory laws in several countries, which argue that an sourcing organization cannot alienate from its accountability.

Every risk is classified as either originating from one of the following sources:

- *People;* This source of risk covers all people and organizational related matters. In sourcing engagements typically governance capabilities, know-how, and principal-agent questions have to be considered.
- *Processes;* This source of risk incorporates all processes that interact with the sourcing engagement, may this be business processes (especially in BPO), administrative / support / ITIL processes like incident, problem or requirements management.
- *Systems;* The term systems incorporates all information technology and communication systems relevant to the sourcing engagement, including hardware and software.
- *External;* Events as laid out before, external events cover the exogenous part of operational risk, typically natural disasters, terrorist attacks, and political/social risk (e.g. the disseizing of corporate property).

For each of the sources specific key risk drivers (KRDs) are being identified. A KRD being a quantifiable and manageable event that may negatively effect one or more sourced services. An event (KRD) like power outage for example can have a negative effect on service levels like availability and reliability. It should however be noted that it is not required that every risk category includes all four sources of risk. A people risk like a lack of knowledge for example, may be a relevant to the service risk category but not to the category financial risk.

6.4 Impact areas

To support a more focused and diverse assessment we indicate which and how services, or contracted obligations, may be impacted by the identified risks (KRDs). A simple yet compelling way to do this is by using the three operational performance dimensions quality, cost and time, as they are all measurable and commonly used in product development, project management, and manufacturing.

Concerning exclusiveness it is important to realize that these three dimensions are naturally depended, e.g. quality issues can have effects on costs, time lags might have effects on quality and costs. Therefore it is crucial to distinguish between cause and effect and clearly allocate a risk either to only one impact area or to split it up between multiply impact areas to avoid double-counting. Note, that in the same way a risk can have more than one source it can have more than one impact area. Thirdly, these areas are in so far completely exhaustive, that in case a risk cannot be assigned to one or the other impact area, the effects of this risk could be translated to monetary figures and be applied to the cost area. Impact areas are further refined into key risk indicators (KRIs), which represent parameters of the impact areas that allow for condensed communication to senior management. Example for the impact area quality are the KRI failed transactions, dissatisfied customers. Prolonged time to market is an example for impact area time.

6.5 Risk controls

The sourcing organization applies an approach to assess the service provider's performance that involves minimal effort and interference in its delivery processes. Performance control is a dynamic process based on a dynamic mix of risk based controls which aligns with the engagement's changing risk profile. A changing business environment, changes business needs, changing performance levels and changing insights, result in a changing risk profile which calls for a dynamic mix of controls. Compliance with contractual obligations by the service provider, is verified through a set of system, process and service controls. These controls provide a judgement on the performance of the service provider.

A *system control* is a control on the quality management system of the service provider as contractually agreed. The main focus is on the service provider's actions to ensure fulfilling its contractual obligations. This included project and program management, quality reviews, ISAE 3402 reporting and supporting management assertion. The control focusses mainly of the functioning of the Deming-circle at the engagement level.

A *process control* is a control on the working of the service provider's delivery and management processes. Delivery processes, described by the service provider, are commonly captured in project plans, statements of work and the dossier of arrangements and procedures. A process control should contain the following:

- Input – output relations;
- Use of tools;
- Process management;
- Risk management in the process
- Correct functioning of the Deming-circle in the processes

Commonly used forms of process keys are: conducting interviews, attending and observing processes during the realization, and review of process reporting.

A *service or product control* is a control assessing whether services comply with required value parameters in terms of quality, cost and time, with the aim to verify the reliability of service provider's service performance data. The client will compare the value attributes of the services delivered to the test or performance reports of the service provider. (e.g. sample testing, CSAT) The client will not take over responsibility for the service quality.

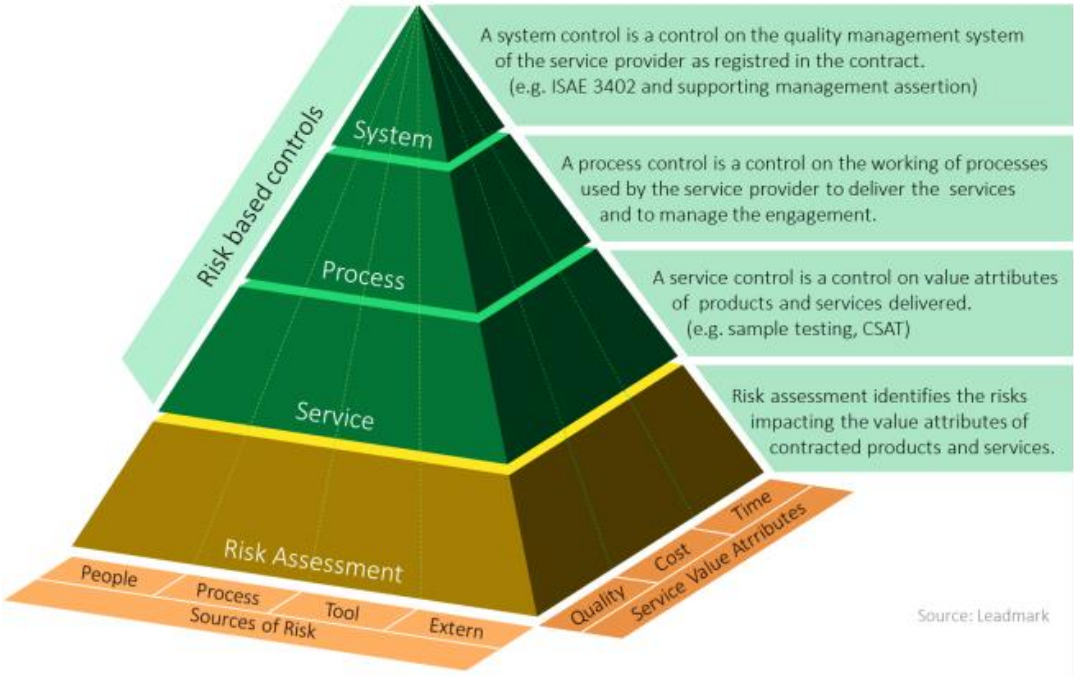

Figure 2: Risk - Control pyramid

6.6 The risk management process

Risk management is an integral part of the ongoing governance of the sourcing arrangement.
Given the dynamic nature of sourcing arrangements, the risk assessment is not something that should only be performed during the initial contracting stage. The ongoing risk process consists of 5 steps:
a) Full risk assessment, b) Define controls, c) Monitor controls, d) Review controls, e) Update risk assessment.

Figure 4: Risk Management Process

- *Full risk assessment;* The full risk assessment is performed using the classification matrix and FMEA model with the goal to get a comprehensive view of the sourcing risks. The result of this step is a prioritized portfolio view of key risk drivers (KRDs) and derived risk indicators (RIs) with their associated risk priority numbers (NPRs) relevant to the sourcing engagement. The assessment is completed by assigning a management strategy to each of the risk indicators which is to either accept, reduce, share or avoid and a statement on which party (sourcing organization or service provider) is best positioned to control the risk.

- *Define controls;* In this step a specific control or performance indicator is defined for each risk indicator. A control is a measurable value or activity that demonstrates how effectively a company is achieving its service levels (quality, cost and time). Controls are planned based on current risks, with the focus on those risks which can be influenced by the service provider and which have the highest risk priority number.

  Within the Value-Led governance framework four types of controls / KPIs are used:

  i. *Basic controls*: applied on the general sources of risk to the arrangement and are included in the service providers quality management system;
  ii. *Reactive controls*: applied on specific sources of risk that may have a more immediate effect on the service should they materialize. These controls typically include business continuity and contingency measures;
  iii. *Reflective controls:* applied on risk with a higher priority and include continuous post-performance monitoring and reporting. e.g. kpi reporting and trend analyses;
  iv. *Proactive controls*: applied on high priority risks and include proactive service quality assessments. (e.g. vulnerability and penetration testing, service inspections).

- *Monitor controls;* The organization or person accountable for the control needs to make sure that the controls are measured and reported on following the agreed timeline and frequency.

- *Review controls;* With regular intervals the effectiveness of the controls should be reviewed against their objectives (reduce, share or avoid).

- *Update controls;* Controls are periodically reviewed on relevance and where necessary updated to stay in line with changing business conditions. This includes revoking of controls that have become obsolete because of mitigating actions or just by passing of time. New controls can be introduced if changing business conditions call for it.

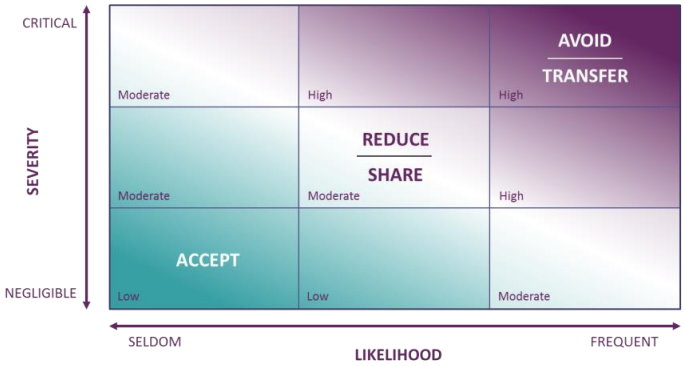

Figure 5: Risk priority matrix

In addition to the process described above, the following starting points need to be respected when implementing sourcing risk management:

- Risk management should align with accountability. This means that the one accountable for a service or outcome should also be accountable for the associated risks and controls. In other words, risk management can not be delegated to a third party or a risk management expert. Also a party cannot be accountable for a risk if they are not in control of the domain from which the risk originates.
  A service provider, for example, cannot be held accountable for the overall spend if he is not in control of demand volumes.

- Risk Management should be an integral part of the sourcing governance function and should be a regular point on the agenda of governance meetings. Managing and reporting on risks and control measures should be done at the same level and with the same frequency as the management and reporting on service quality and other processes.

- Revoking risks and controls, and identifying new ones should be done in consultation with all governance staff on both sourcing organization and service provider side.
  When performance against agreed metrics continues to be under par, hence objectives are not being met, appropriate action should be considered.

For risk assessments to yield meaningful results with minimal burden, organizations should consider the following key principles.

1. *Governance over the risk assessment must be clearly established.*
   Oversight and accountability for the risk assessment process is critical to ensure that the necessary commitment and resources are secured, the risk assessment occurs at the right level in the organization, the full range of relevant risks is considered, these risks are evaluated through a rigorous and ongoing process, and requisite actions are taken, as appropriate.

2. *Risk assessment begins and ends with specific objectives.*
   Risks are identified and measured in relation to the organization's sourcing objectives and services. Services and objectives that are specific and measurable at various levels of the organization are crucial to a successful risk assessment. Evaluating the risks relative to services and objectives allows for specific and measured controls, and facilitates the (re)allocation of resources as necessary to manage these risks.

3. *Risk rating scales are defined in relation to organization's objectives in scope.*
   The Risk Indicators (RIs) identified in the risk classification framework are typically measured in terms of impact an likelihood. Impact scales of risk should align to the impact areas and services relevant to the organization.

4. *Management forms a portfolio view of risks to be controlled*.
   While risks are rated individually in relation to objectives, services and impact areas, it is also important the bring risks together in a portfolio view that pinpoints interrelationships between risks across the sourcing engagement as a whole. Correlations may exist, in which an increased exposure to one risk may also have an effect on another. Concentrations of risks may also be identified through this view, which may call for additional controls.

5. *Leading indicators are used to provide insight into risks.*
   Managing sourcing risk is most effective when risk indicators (RIs) are controlled through a tailored (relevant) and specific metric/KPI that can be measured and reported on. To identify risk indicators and control measures, organizations need to look beyond past events and performance and anticipate new risks resulting from changes in the business environment.

7. How Leadmark can help

Leadmark is boutique services firm specializing in targeted run stage solutions that address the governance challenges of sourced services and supplier relationships. The firm's vision is that simplification of sourcing contracts and governance processes, underpinned by innovative cloud-based technology enables new – more productive – ways of cooperation between clients and their services providers that last and yield better outcomes

Leadmark provides best practice methodologies and a convenient subscription-based governance platform in the cloud to streamline and empower governance efforts. Understanding business needs, open communication, transparency in creating and realizing expectations, and exceptional service are highly valued by our clients.

7.1 Risk assessment workshops

Leadmark can help organizations to facilitate an sourcing risk assessment that will result in a comprehensive, documented risk and controls matrix.

Typical activities to run the workshop are:

- Planning and project management;
- Execute the risk assessment workshop;
- Workshop result reporting.

As input to the workshop Leadmark will provide a comprehensive catalogue of over 250 potential sources of risk to prevent organizations having to start from scratch and help to maximize workshop results.

7.2 Contract assessment

A strong contract and an effective governance function are fundamental to the success of sourcing.
The contract doesn't only have to be legally solid or well structured from a procurement point of view also the governance function isn't just about job descriptions and organizational structures. A good contract has to be manageable and actionable. If obligations and controls are not turned into assigned actions they will not be done, and if the contract doesn't have a set of balanced levers to pull, it's not possible to effectively control and steer the engagement.

Leadmark provides a detailed fact based assessment focused on the manageability of the contract and the extent to which it can be considered an effective instrument to underpin current and future sourcing objectives.

7.3 TRAC governance platform

To underpin the ongoing risk management and mitigation process, and act as a Risk Management Information System beyond the assessment, Leadmark utilizes its governance platform TRAC. This allows organization to continuously manage and report on their sourcing risks in a structured and auditable way fully integrated with the overall governance of the engagement.

+ - + - +