Outsourcing

—a practical guide on how to create successful outsourcing solutions

INTERNATIONAL CHAMBER OF COMMERCE
The world business organization

This guide has been produced by a dedicated Task Force within ICC Sweden Financial Services and Insurance Committee. The task force has consisted of Christina Strandman Ullrich (Chair), Mattias Anjou, Åsa Engström, Per Johan Gidlund, Louise Hedqvist, and Johan Kahn.

Outsourcing
—a practical guide on how to create successful outsourcing solutions

Content

PREFACE

In a globalised world, companies seek partners for cooperation and for outsourcing in markets and regions suitable for their business. This may lead to reduced costs and cheaper services for customers. It also creates opportunities for increased global trade between companies and for international relationships between countries. The International Chamber of Commerce (ICC) develops tools—such as this guide—to help businesses conduct trade smoothly and efficiently.

The regulatory environment is becoming increasingly detailed and risk-focused for business operations in a number of historically regulated sectors, such as finance, health care, power supply, telecoms, and a variety of public services. There may also be fundamental risks related to national regulatory requirements, e.g. labour law, that a company or organisation must adhere to when planning to outsource some of its services. Of course, all inherent risks in any such business must be identified and managed in a diligent and proportionate manner. Companies carrying out regulated business activities face particular challenges to control risks and associated costs when outsourcing parts of their activities. Significant requirements and expectations connected to public supervision—including an increased focus on transparency—must be met to avoid sanctions, fines or negative reputational effects.

This practical guide aims to facilitate and support regulated businesses when they outsource their activities and offer a tool for interpreting quality based rules such as “sound governance” and “proper risk management”. By preparing this practical guide, the ICC hopes to strengthen self-regulation in this area, complementing other self-regulatory initiatives. ICC has developed a number of guidelines and handbooks over the years which are also relevant for an outsourcing company, such as the 2017 Anti-Corruption Third Party Due Diligence and the 2007 ICC Legal Handbook on Global Sourcing Contracts, the latter focusing mainly on small- and medium-sized companies.

By providing a baseline and roadmap for outsourcing companies, this guide will contribute to more efficient global trade, better consumer protection, increased stability in the financial and other regulated markets and, ultimately, more trust and confidence in business actors in such regulated sectors.

Chapter 1

INTRODUCTION & PURPOSE

HOW TO READ, INTERPRET AND APPLY THIS PRACTICAL GUIDE

Outsourcing is an arrangement between an *Outsourcing Party* and a *Service Provider* by which the Service Provider performs a process, a service or an activity, either directly or by using sub-contractors, which would otherwise be required to be performed internally by the Outsourcing Party. In this practical guide, the terms "Outsourcing Party" and "Service Provider" are used throughout.

The management of an Outsourcing Party is fully responsible in relation to the stakeholders (e.g. owners, customers, society and regulators) for all business carried out by the company, regardless of whether such business has been outsourced or not. In this practical guide, we use the term *the Management* to include (i) both the senior management and the single board in a one-tier system, and (ii) both the management and the supervisory board of a two-tier board system.

PROPORTIONALITY

This practical guide provides general principles and guidelines for the Outsourcing Party and Service Provider to increase the possibility of a successful outsourcing solution, and is intended to be applicable to any jurisdiction. However, as one size does not fit all, the principles and guidelines provided herein need to be applied regarding the nature, scale and complexity of the outsourced business provided and the inherent risks in relation thereto. The risks inherent in an outsourced arrangement may vary, depending on whether the outsourcing arrangement concerns all or only part of a certain activity or a process. This practical guide is particularly useful where the inherent risks are significant. However, it will also be helpful to a company in relation to less complex outsourcing arrangements.

A TOOL TO BETTER MANAGE AN OUTSOURCING RELATIONSHIP

This practical guide aims to facilitate the management of an outsourcing relationship between, on the one hand, institutions carrying out any type of regulated business as Outsourcing Parties and, on the other hand, the Service Providers. It may provide assistance to a regulated business in its due diligence process when choosing a Service Provider and when negotiating the Outsourcing Agreement. It may also contribute indirectly improving the quality of services offered by the Service Provider.

SUITABLE FOR BOTH REGULATED AND NON-REGULATED BUSINESSES

This practical guide is particularly useful when the Outsourcing Party is a regulated entity. For example, outsourcing is conceptually subject to regulation in the financial industry as financial companies are required to ensure sound management of their business, regardless of whether it is outsourced or not. There are similar requirements for other regulated business sectors such as health care, power supply and tele-communications. Companies subject to regulation and supervision have an interest in

avoiding sanctions and negative effects on reputation due to not being able to meet applicable regulatory requirements and expectations from customers, the market and the society.

Non-regulated companies may not be as familiar with the standards that must be complied with by regulated companies in order to accept an outsourcing arrangement and this guide may therefore facilitate the cooperation between regulated companies and non-regulated companies. For example, larger institutions can encourage their small- and medium-sized partner institutions to use this document for insight into both procurements and quality self-assessments.

Finally, since this guide is a compilation of best practices drawn from practical business experience, regulators will also be able to use it to inform their supervision and policy-making.

* * * *

Chapter 2

OUTSOURCING VIEWED FROM A RISK MANAGEMENT PERSPECTIVE

THE RISK MANAGEMENT PERSPECTIVE

There are obvious reasons for a company to find a partner with specific skills or capacity that can perform certain tasks at a lower cost or in a way that increases the company's revenues. In such cases, though, the company often underestimates the risks associated with outsourcing and the outsourcing arrangement may ultimately have a negative impact on costs or revenues—if such risks are not properly managed.

To begin with, the Outsourcing Party and the Service Provider may have different starting points. The Outsourcing Party may have different reasons (cutting costs, expanding into a new market, meeting new customers, etc.) for wanting another company to take on or develop part of its business. The Service Provider on the other hand, may be aiming primarily to deliver services at the lowest possible cost.

While the Outsourcing Party and the Service Provider presumably have the common ambition to achieve positive results, the parties' different positions, goals, opinions and ideas as to how the outsourced business should be carried out may lead to problems for both parties. As an example, when the duties and obligations of the Service Provider are not clearly established it may be difficult for the Outsourcing Party to receive updated and relevant information from the Service Provider in order to identify, understand, and manage the risks inherent in the outsourced activities.

Financial regulation as a benchmark for managing risks connected to outsourcing

Companies active in financial markets today are heavily regulated, with a focus on identifying and managing any risk inherent in their business. When it comes to regulating outsourcing, the regulatory regime applicable to the financial industry is suitable as a benchmark regarding risk management in outsourcing for companies active in other industries or business areas.

Financial sector regulation is based on hard-learnt lessons over the past 20 years, where failed strategies and improper governance has led to severe losses for financial institutions, investors, customers and, in the worst cases, the community. As a first important step to create global standards for internal control in the 1990s, the COSO framework[1] developed a basic understanding regarding the importance of creating a sound business organisation with clear roles and mandates, setting goals for the business activities, understanding risks for not reaching the goals, et al. This framework can be applied to all types of businesses, especially when customer protection and reputation are important success factors.

In the wake of the 2008 global financial crisis, national and international regulators recognised the need for more comprehensive regulation. Among other things, post-2008 international regulations emphasise governance in terms of internal control, responsibility and risk management, compliance with regulatory requirements, and transparency towards regulatory authorities and customers.[2] All requirements

1 Internal Control—Integrated Framework by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).
2 International regulatory framework for banks by the Basel Committee on Banking Supervision.

regarding the business of a financial institution also apply to any part of the business that is outsourced.

As it may apply to any business, calculated risk taking is at the core of a company's strategy, even for non-financial companies. However, risks may arise and develop in an unexpected way and such risks must continuously be identified and managed in order for a business to be successful and to meet relevant business objectives. In relation to outsourcing there are certain risks that are more relevant than others and which should be eliminated or mitigated as far as possible. These are, for example, operational risks (including specific IT or cyber risks), reputation risks, and compliance risks.

There is a significant regulatory duty imposed on these companies to ensure that they have the best understanding of existing risks as well as new and developing risks on an ongoing basis. Experience has shown that when risk- consciousness is present in a company's daily business, bad things are less likely to happen: companies using a risk-based approach are more successful in the long run and more likely to meet the expectations of regulators and stakeholders and maintain a high degree of trust and confidence in the business in the long run.

A company that carries out a regulated business is required to manage all types of financial, operational, and business conduct risks. If such risks are mismanaged, the relevant supervisory authority may decide to revoke the licence, impose fines or penalties, or demand specific actions to be taken. This means that a regulated business, e.g. a regulated company in the financial sector, must invest at least the same effort, cost and time to maintain a sound and profitable long-term business whether the business is carried out internally by the company's own staff or externally, as an outsourced business carried out by a third-party Service Provider.

The responsibility for appropriately managing risks of non-compliance with stakeholder requirements and expectations lies exclusively with the Management of the Outsourcing Party. When outsourcing certain business to a Service Provider (that may in turn have sub-outsourced certain activities), the Outsourcing Party must make sure to identify and manage the specific risks that may arise in the particular outsourcing relationship. By way of example, risks connected to IT solutions, external data storage service providers (cloud solutions), and similar activities where cyber risks may arise, may require due diligence and review prior to setting up the outsourcing arrangement.

An Outsourcing Party must ensure that the Outsourcing Agreement includes comprehensive and thoroughly-negotiated provisions for the control and management of the Service Provider as well as a high degree of transparency and access to information about both the outsourced services and the Service Provider. The control, management and transparency requirements are as valid for intra-group outsourcing arrangements as they are in relation to external Service Providers. This means that even if the Outsourcing Party is a subsidiary to the Service Provider, the parties need to enter into a proper contractual arrangement and negotiate an Outsourcing Agreement that meets the same high standards as are required in relation to an external Service Provider.

Chapter 3

PRINCIPLES FOR SOUND GOVERNANCE OF AN OUTSOURCING RELATIONSHIP

A business relationship without proper governance can lead to costly effects such as renegotiations, redelivery or regulatorily-driven costs such as sanctions from a supervisory or regulatory authority or loss of reputation and customers. The principles below elaborate on how sound governance in an outsourcing arrangement can be achieved and maintained by the Outsourcing Party and the Service Provider.

During the past 20 years, companies on the financial markets have learned, understood and implemented sound governance systems based on the idea of ensuring:

- an appropriate and effective organisation and management of the business;
- reliable financial results; and
- compliance with relevant rules and regulations.

The business must be based on clear and measurable objectives and goals. The outcome shall be measured against set targets. All risks which may threaten the objectives and goals must be identified and managed.

The above also applies to all outsourced activities.

FIRST PRINCIPLE
—the responsibility of the Management of the Outsourcing Party

The Management has the ultimate responsibility for organising and managing the business so that the principles for sound governance are met. It includes ensuring that all regulations and expectations from supervisory authorities as well as other stakeholders are followed and complied with. This responsibility cannot be outsourced. On the contrary, the Management must make sure and is responsible for the out-sourced activity meeting the regulatory requirements applicable to the Outsourcing Party.

The Management is responsible for establishing the business strategies and targets and following up on the results. This responsibility also applies to any outsourced activities.

The Management adopts policies and internal rules on an overall and general level with a holistic perspective. Such policies and internal rules should also comprise the outsourced activity. If the Management has implemented control functions (e.g. Risk Control and Compliance and Internal Audit), it shall ensure that such control functions are provided with resources and the contractual power to monitor and control any outsourced activity carried out by the Service Provider.

Daily business operations and activities should be executed in line with the Management's expectations and demands including compliance with the relevant legal framework. For any outsourced activity, the Management must ensure that such expectations and demands also comprise that activity.

The organisation shall ensure that the Management receives timely, accurate,

appropriate and relevant information to facilitate its decision-making. The operational staff shall also inform the Management on an ongoing basis about the development of the business as well as inherent risks. This should also apply to any outsourced activity, where arrangements should be made, including appropriate provisions in the Outsourcing Agreement, to ensure that relevant information concerning the outsourced business, and the inherent risks in relation thereto, are transferred to the Management.

The Management shall ensure the implementation of effective systems for communication and information throughout the company, including IT systems and services, organisation, routines and processes which will deliver relevant and timely information to relevant staff and parts of the organisation. Equally, it may be important that an outsourced activity integrates internal routines and processes and, if appropriate, IT-systems.

SECOND PRINCIPLE —Internal Control

The requirement to establish and maintain sound governance applies for all the business of a company, including its outsourced activities. The Management is responsible for ensuring that these requirements and expectations are met. The concept of internal control applies to all the company's business whether it is carried out in-house or is outsourced to a Service Provider.

A sound governance environment starts with the Management setting the tone, preferably by implementing a culture where measurable business objectives are set and where the results and outcome are measured against such objectives. A central consideration is an appreciation of the risk that the results do not meet the objectives. All such risks must be managed in a proper way. To be able to manage the risks, they must be identified, measured, controlled, followed up and reported to the Management. This also applies to risks that may arise in an outsourced activity.

Risks may be different in many ways. Some risks are accepted as such risk-taking constitutes the basis for the company's business. Such risks should accordingly not be avoided or eliminated. For a financial company, such risks are e.g. the different financial risks which the company takes on behalf of its customers (such as credit risk, market risk and liquidity risk). A regulated company must however, understand, measure and validate these risks in the day-to-day business in order to be prepared to handle and withstand such risks should they materialise. It is equally important to understand, measure and validate how the risks may develop. This includes existing risks as well as new risks. Usually it is possible to assign a certain amount or a value to a financial risk. Financial risks taken by a non-financial institution must be treated in the same way.

Different business risks also require attention and management in a diligent way. Do we offer the right products to the right customers in the right market? Targets and objectives must be set and the business outcome must be measured against the targets.

Operational risks are not typically part of a company's established and agreed central business. They are unwanted, unpredictable, hard to evaluate before they materialise and often costly to manage. Operational risk includes risks resulting from breakdowns in internal procedures, people and systems. Operational risks may be particularly relevant in an outsourcing relationship, as it may be more difficult for the Outsourcing Party to manage such risks, e.g. operational risks relating to staff or systems that are controlled by the Service Provider, or leaks of proprietary or confidential information.

Cyber risks derive from the handling and transferring of e.g. proprietary information with the support of information technology (IT). Cyber risks may be particularly relevant to manage and mitigate in relation to an outsourcing arrangement since the arrangement is dependent on an effective and safe exchange of information between two parties. These risks may be internal or external. They may also include intentional behaviour as well as accidents originating with the Service Provider, its employees or sub-providers.

Compliance risks relate to how the business is conducted towards customers and on the market. In addition to complying with applicable regulations, it is about trust and reputation, about treating customers and the public fairly, and giving objective and trustworthy advice and information. Conflicts of interest must be identified and managed (reduced or avoided) and the party who may be affected negatively by the conflict shall be informed about it. It is also about complying with other requirements linked to the specific licenced business and understanding the expectations from the regulator as well as the customers and the market. Such expectations are constantly developing and changing and are often emphasised by the media. Not being responsive or interested in such developing views and expectations may affect the reputation of the company in a detrimental way. These risks are often referred to as reputational risks. They are embedded in the company's culture and governance system. Generally, compliance and reputational risks, like operational risks, are more difficult to evaluate and assess in monetary terms in advance than financial risks. In an outsourcing relationship, it is accordingly important for the Outsourcing Party to manage compliance risks that may arise due to the outsourcing relationship and due to the acts and omissions by the Service Provider.

Financial risks, both in terms of amount and type, are part of a company's strategy and they must be identified, managed and understood but not primarily reduced. Operational risks and compliance risks on the other hand can hardly be part of a company's strategy. Accordingly, they must be identified, understood and managed wherever possible so that they are reduced as far as possible.

There are at least four different ways to manage risks. Risks can be: 1) reduced; 2) transferred to another party (e.g. insurance); 3) eliminated; or 4) accepted. The company's established risk appetite and risk tolerance will guide the Management in deciding how and to what extent the risks shall be managed.

To help the business to identify and manage risks, the Management may rely on specific methods of controlling the risks. These methods may be proactive or reactive. They may also be technical or manual methods. In general, it is more cost

efficient to establish technical (IT) controls which have a proactive aim. Examples of such controls are IT systems which "demand" certain information to let the user continue, for instance in connection with opening an account for a customer. Segregation of duties, the 'four eyes' principle, and bookkeeping routines and processes are other examples. These controls need to be followed up to make sure that they are effective and deliver the desired results. The appropriate tools to manage risks must also be used by the Outsourcing Party in relation to the outsourced activity. To ensure proper risk management the Outsourcing Party should have in place sufficient internal rules, manuals and guidelines.

Managing a risk that has developed in an undesired way and is thus discovered after its occurrence may be burdensome and costly. Proactive controls are more effective than reactive ones, even though reactive controls are necessary to some extent.

Manual controls can be substituted by technical controls to a certain extent, but a company will never be able to completely rely on IT systems.

THIRD PRINCIPLE —Transparency

Regulated companies rely on the continuing trust and confidence of customers, investors, supervisors and other stakeholders. One important component in order to gain and maintain such trust and confidence is to be transparent. When a sound governance system is implemented in the business, the risks are managed and controlled in a predictable way. The aim is to avoid negative effects from risks materialising and to attend to risks as early as possible.

Regulations provide the supervisory authorities with a right to demand continuous information regarding the day-to-day business through regular reporting requirements or ad-hoc requests for information. Further, regulated companies are required to disclose and publish a lot of information concerning their financial situation, but also concerning their services and products, on their website. Accordingly, some information is required to be reported to the supervisory authority and some information is required to be made publicly available.

Personal data, customer information as well as proprietary information and trade secrets must of course be treated with confidentiality, care and respect as well as in accordance with applicable data protection regulations. Internal rules, manuals or guidelines in place enhance governance in data handling.

The concept of transparency applies to all the company's business whether it is carried out in-house or is outsourced to a Service Provider. Accordingly, it may be important for the Outsourcing Party and the Service Provider to agree on how information should be shared between the parties and what information that should be continuously reported to the Outsourcing Party by the Service Provider in order for the Outsourcing Party to fulfil its obligations as regards transparency.

* * * *

Chapter 4

GUIDELINES

The following guidelines are based upon the three principles for sound governance in outsourcing discussed above and are targeting three stages of an outsourcing arrangement:

1. entering the arrangement,
2. developing the arrangement, and
3. terminating the arrangement.

Each guideline is followed by an explanatory text specifying practical measures.

BUSINESS SUITABLE FOR OUTSOURCING

Guideline A. *Many business activities conducted by a regulated company may be suitable for outsourcing. This applies to technology outsourcing such as IT-operations and application development as well as other activities. However, specific regulatory diligence must be applied when outsourcing directly regulated activities. The procurement process and the contractual arrangement for outsourcing are crucial both from a business and regulatory perspective. A well designed and elaborated Outsourcing Agreement may make outsourcing of a specific activity permissible while the opposite may apply if the contractual arrangement is sub-standard.*

1. Any business activity that could be carried out more efficiently by a specialised Service Provider than by the Outsourcing Party could be an option for outsourcing. A more efficient production of such business activity would normally result in lower costs or improved services, or both. More specialisation and economies of scale will, at least in theory, yield a more efficient execution of such an activity.

2. In addition to efficiency gains, outsourcing may also be used as a catalyst to manage consequences of mergers and acquisitions and technology transformations. Outsourcing driven by such structural or technological changes would focus more on the transformational part of an outsourcing arrangement. This means that the business activities transitioned to the Service Provider would undergo transformation during the term of the outsourcing arrangement and that the services are intended to be produced differently at the end of the term.

3. Outsourced business activities could range from advanced technology functions such as IT-infrastructure services and application development and maintenance (ADM) to more or less complex business processes such as procurement, customer support services, human resource processes and facility management. Support and maintenance under-takings in relation to business-critical systems would normally count as a form of outsourcing, though not always labeled as such, since the services rendered under such arrangements would otherwise have had to be

produced by the Outsourcing Party. Business activities that are directly regulated and licensed such as fund and portfolio management require specific regulatory diligence when assessing if such services are suitable for outsourcing or not.

4. Even though IT-infrastructure and maintenance of business-critical systems are directly business critical and a decisive factor in the assessment of operational risk, such functions are often considered for outsourcing. Whether such functions are suitable for outsourcing or not depends on the proper set-up and contracting for such an arrangement. It may very well turn out that a Service Provider may offer sufficient capability in terms of the services as such. However, if the Outsourcing Agreement does not provide sufficient measures for the Outsourcing Party to control and effectively enforce the undertakings in the agreement, the services may not be suitable for outsourcing. Hence, a sub-standard Outsourcing Agreement can turn a service which is otherwise suitable for outsourcing into one which is unsuitable for outsourcing. This would be the case if it is not elaborate enough and thereby does not provide the control and steering measures, incentives and enforceability required for outsourcing in the financial sector due to regulatory requirements and stakeholder expectations. In addition, the Outsourcing Agreement must also provide the commercial benefits that justified the deal in the first place.

5. Outsourcing must never jeopardise the capability of a regulated company to conduct its licensed operations. The overall capability of a regulated company to fulfil its obligations shall not be undermined by overly extensive outsourcing. Executive management may not be outsourced and the obligations to comply with regulatory requirements as such will of course always remain with the Outsourcing Party. Business functions which constitute the core business or key commercial differentiators for the Outsourcing Party (e.g. unique or proprietary business processes or solutions) compared to its competitors in the market should typically be retained to maintain the Outsourcing Party's competitive advantage. An inadequate outsourcing arrangement, in relation to the business activity as such, the procurement process as well as the Outsourcing Agreement, would therefore expose a regulated company to unjustifiable risk.

6. The assessment of permissibility as well as suitability to outsource a certain business activity is a question of the content of the Outsourcing Agreement. By applying an elaborate and thorough procurement process and contractual arrangement, many risks associated with outsourcing can be mitigated. The checklist at the end of this guide can help facilitate this process to minimise the risk of unwanted effects during an ongoing relation with a Service Provider. Apart from regulatory requirements there are also commercial reasons to require a good contractual arrangement for any outsourcing. It is important to keep in mind that the regulatory requirements relevant to an Outsourcing Agreement are not necessarily sufficient to create a good, competitive outsourcing deal.

COUNTERPARTY DUE DILIGENCE

Guideline B. *The Outsourcing Party shall perform a counterparty due diligence and ensure that the Service Provider has the capability and capacity to perform the outsourced activities and is able and willing to comply with the standards and requirements of the Outsourcing Party. Minutes from meetings shall be kept and the Service Provider should give documented answers through questionnaires. The due diligence shall be performed through an assessment of operational and regulatory risks carried out by personnel at the Service Provider such as risk managers and compliance officers in order to assess ability to exercise internal control. The due diligence should be transparent and documented in a report before an agreement is formalised and different sections should be categorised and indicate if the risk is low, medium or high and reported to Management.*

1. Due diligence should consist of a review of all relevant business operations and documents and records as well as business processes and financial conditions to assess the risks and viability of an agreement with the Service Provider in question. Due diligence is often only permitted once the Outsourcing Party has signed a Non-Disclosure Agreement and the level of the due diligence depends on the perceived risk with the proposed outsourcing arrangement.

2. For a regulated Outsourcing Party, it is important to require the potential Service Provider to give a management presentation and complete a questionnaire. The Outsourcing Party must ensure that the Service Provider is acting in compliance with local laws and standards as well as law and standards in the home country of the Outsourcing Party. A due diligence should therefore, in addition to a questionnaire, include an assessment carried out by managing personnel at the Service Provider. Access to as many information sources as possible is important as well as information from local authorities, and if deemed necessary, other third parties that either charge for their services or have free information on their websites.

3. Ideally, on a client visit, the Outsourcing Party should meet with the Service Provider's representative for risk management to discuss, for example, how the Service Provider controls Operational Risk, the set-up of the general risk management processes, and different types of stress testing.

4. Due diligence may also be complemented by representations and warranties in the Outsourcing Agreement whereby the Service Provider becomes liable for certain conditions and performances in relation to the prerequisites for the outsourcing deal. Contractual protection through assurances, undertakings and representations and warranties may however never substitute the far-reaching responsibility for a

regulated company to ensure that a Service Provider can comply with its contractual obligations under the Outsourcing Agreement and the regulatory requirements. These tools will however create a stronger position for the Outsourcing Party by reducing significant financial risk in relation to the prerequisites.

5. Bank or third party references should be part of the due diligence process.

6. The risk assessment and due diligence should be proportionate and be more thorough if the Service Provider is in a country or region connected to, e.g. higher risk for corruption or money laundering. In addition, other "red flags" during the due diligence, such as incomplete or inaccurate information, will indicate that a more thorough due diligence should be carried out.

7. Due diligence related to outsourcing should include the following main sections, which should be clearly documented.

    - **General Information and Legal Documents**—General corporate information and a detailed explanation regarding ownership (direct and indirect) of the Service Provider. All material information regarding permits, licenses, or authorizations issued by governmental or other local regulatory authorities.

    - **Financial Information**—Historical financial reports (which include financial statements) and a 2-3 year forecast to determine the possibility to maintain the ongoing business. Correspondence between the Service Provider's auditors, both internal and external, for the previous years.

    - **Operational**—Processes and staff associated with the operation of the business is to be documented. An organisational chart of all management and other critical employees. Documentation of the disaster recovery plan, and tests conducted should be presented.

    - **IT**—A detailed listing of all IT systems used in the normal business processes and the Service Provider´s documentation of procedure covering security, backup procedures, controls, and auditing for managing IT-related risks, such as cyber risks.

    - **Intellectual Property**—Agreements and arrangements regarding the intellectual property used by the Service Provider, including a warranty by the Service Provider that there is no violation of third parties' intellectual property when providing the outsourcing solution.

The following items should also be assessed by an Outsourcing Party regulated by a regulatory authority:

- **Ethical, anti-bribery (anti-corruption) and personal data handling** —A description of how the Service Provider's organisation makes it

clear that bribery is not tolerated and will result in disciplinary action, how the Service Provider maintains good ethical conduct, and how it complies with applicable law on personal data handling.

- **Litigation history and authority administration fees** – Lists of any litigation, judgment or fees for late filing of mandatory reports, etc. to the regulatory authority, or pending audits, for the previous years should be presented.
- **Internal control and Information systems** – Description of the system including internal and external reporting lines used by the Service Provider and how the organisation manages and maintains the system in day-to-day activities. Policies and other internal documents should be provided.

The due diligence should be compiled in a report before an agreement is formalised and different sections should be categorised and indicate whether the risk is low, medium or high.

THE OUTSOURCING AGREEMENT

Guideline C. *There should be a legally binding written contract between the Outsourcing Party and the Service Provider. The wording of the contract should clearly set out the responsibilities of both parties and provide that the outsourced services meet the regulatory requirements applicable to the outsourced activity. The contract should allow for the Outsourcing Party to monitor, audit and control the outsourced activity and for any supervisory authority to supervise the outsourced activity. The contract shall also include the relevant covenants to transfer or reduce any identified risks.*

1. A legally binding written contract between the Outsourcing Party and the Service Provider is an important management tool. Appropriate contractual provisions can reduce the risks of non-performance or disagreements regarding the scope, nature, and quality of the service to be provided. The level of monitoring, assessment, inspection and auditing required by the contract should be proportionate to the risks involved and the size and complexity of the outsourced activity. The respective rights and obligations of the Outsourcing Party and the Service Provider should be precisely defined and specified. This should also serve to ensure compliance with laws and supervisory regulations and guidelines for the duration of the outsourcing arrangement.
2. The contract should include at a minimum, as applicable, provisions dealing with:

Description of the Outsourced Activity and Service Level

- The contract should clearly describe and define the outsourced activity.
- The contract should contain precise requirements concerning the performance of the outsourced service, taking account of the objective of the outsourcing solution.
- The Service Provider's ability to meet performance requirements should be set out in both quantitative and qualitative terms and be able to be measured and assessed (e.g. include key performance indicators "KPIs" and service level agreements).
- To achieve clarity of performance targets and measurements for the Service Provider, a separate sub-agreement should be in place where performance requirements are outlined in detail and be subject to and governed by the terms and conditions of the main outsourcing contract.
- The contract should contain warranties and indemnities connected to the Service Provider's performance of the outsourced services.

Monitoring, Audit and Supervisory Access

The contract should

- Define the Outsourcing Party's legal right over data relating to services provided, as well as the activities regarding personal data that the Service Provider would implement.
- Include an obligation on the Service Provider to allow the Outsourcing Party's compliance, risk control and internal audit departments complete access to its data and the Outsourcing Party's external auditors full and unrestricted rights of inspection and auditing of that data.
- Include an obligation on the Service Provider to allow the Outsourcing Party's supervisory authority direct access to relevant data held by the Service Provider and the right for the supervisory authority, in its regular supervision, to conduct onsite inspections at the Service Provider's premises. The Service Provider must in such a case also be fully transparent to the Outsourcing Party and provide timely and accurate information about the contacts with the supervisory authority.
- Include an obligation on the Service Provider to immediately inform the Outsourcing Party, or the relevant supervisory authority directly, of any changes in circumstances which could have an impact on the continuing provision of the outsourced services as agreed between the parties. Delivery breaches should be notified immediately.

- Provide the Outsourcing Party with tools to evaluate the performance of the Service Provider by using mechanisms such as service delivery reports, self-certification or independent review by the Outsourcing Party's, or the Service Provider's, internal and/or external auditors.
- Ensure that the Service Provider's performance is continuously monitored and assessed so that any necessary corrective measures can be taken promptly.

Sub-outsourcing

- The contract should contain limitations or conditions on the Service Provider's ability to sub-outsource, and to the extent sub-outsourcing is permitted, obligatory approval from the Outsourcing Party and any other related obligation.
- The sub-outsourcing of outsourced activities and functions to third parties (subcontractors) should be treated by the Outsourcing Party in the same way as the primary outsourcing measure. Compliance should be ensured contractually, for example by a clause in the outsourcing contract requiring the prior written consent of the Outsourcing Party as to the possibility and the modalities of sub-outsourcing.
- The Outsourcing Party should require on-going information and the possibility to deny the sub-outsourcing contract or its assignment.

Client Confidentiality and Data Protection

- The contract should adequately define confidential information and contain obligations to protect and keep such information confidential, taking regulatory requirements applicable to client confidentiality and stakeholders' expectations into account. The contract should also require the Service Provider to implement security measures that must be notified to the Outsourcing Party.
- The contract should prohibit the Service Provider and its agents from using or disclosing the outsourcing firm's proprietary information or that of the Outsourcing Party's customers, except as necessary to provide the contracted services (e.g., when outsourcing call center services).
- Whenever information is subject to confidentiality rules at the level of the Outsourcing Party, then at least the same level of confidentiality should apply to the Service Provider.
- Where subcontractors are used, the contract should include terms and conditions relevant to govern adequate firm and client confidentiality.
- When the outsourcing includes processing of personal data, the contract should include terms and conditions governing the

processing of personal data (e.g. names, addresses and other information pertaining to individuals) on behalf of the Outsourcing Party and it shall also consider any specific requirement of applicable laws regarding the processing of personal data as well as the specific security measures required by the Outsourcing Party.

- The Service Provider needs to acknowledge its obligation to manage data in accordance with personal data protection legislation, which in many cases can be far-reaching.

Information Technology Security

- The contract should specify the security requirements of IT-systems to be used by the Service Provider, including the technical and organisational measures that will be taken to protect the Outsourcing Party's data, including customer-related data. Care should be taken to ensure that the privacy of the Outsourcing Party's clients is adequately protected (e.g. relevant ISO-standards).
- The contract should contain requirements that the Service Provider maintains appropriate measures to ensure security of both the Outsourcing Party's software as well as any software developed by the Service Provider for the use of the Outsourcing Party.
- The contract should specify the rights of the Outsourcing Party to change or require changes to security procedures and requirements and of the circumstances under which such changes might occur.
- The contract should contain provisions addressing the Service Provider's emergency procedures, disaster recovery plans and contingency plans as well as any issues relating to the Outsourcing Party's own Service Provider in another jurisdiction. Where relevant, this may include the Service Provider's responsibility for backing up and otherwise protecting program and data files, as well as regulatory reporting.

Remedial Actions, Disputes and Exit Management

- The Outsourcing Party should be prepared to take remedial action if the Service Provider's performance is inadequate. The contract should contain clear remedial actions available to the Outsourcing Party in case of the Service Provider's unsatisfactory performance of the outsourced services, breach of warranties or other breaches of contract. It is also advisable to include an indemnity clause in favor of the Outsourcing Party.
- The contract should contain mechanisms to resolve disputes that might arise under the outsourcing arrangement, including the choice of applicable law and competent jurisdiction.
- The contract should include a termination and exit management

clause, where proportionate and if deemed necessary, which allows the activities being provided by the Service Provider to be transferred to another Service Provider or to be reincorporated into the Outsourcing Party.

- To safeguard control, the outsourcing contract should contain a clause permitting termination for convenience. The contract should contain provisions allowing the Outsourcing Party to terminate the contract by giving reasonable notice, or executing a right of termination for convenience. The Outsourcing Party shall have the right to give notice or extraordinary notice of termination in cases of material breach of contract that are not, or cannot, be remedied, or if required by the supervisory authority.

ONGOING RELATIONS

Guideline D. *In the ongoing relation with the Service Provider, the Outsourcing Party should manage the outsourced activity in a way that ensures it always maintains the responsibility for the outsourced activity and its associated risks. The Outsourcing Party should continuously monitor and review the Service Provider's performance to make sure that the outsourced activity meets regulatory requirements and proper internal control. Regular meetings should be held with the Service Provider and information relating to the performance of the Service Provider should be documented and reported transparently to the Management.*

When an agreement has been entered into between the Outsourcing Party and the Service Provider, the parties need to ensure ongoing alignment with the agreement but also develop the business relationship over time.

1. Establish and maintain a point of contact between the parties.

    - The Outsourcing Party should assign a designated person to manage the outsourced activities, an 'Account Manager'.
    - If the agreement is signed by the CEO, the CEO should also be assigned a role to maintain chain of command.
    - There should also be one point of contact at the Service Provider regarding the ongoing relations.
    - The Account Manager with overall responsibility for the outsourced activity at the Outsourcing Party must possess enough knowledge and experience regarding the outsourced activity to be able to challenge the performance and results of the Service Provider.

2. Establish and maintain a suitable structure for control

    - The Account Manager should establish a meeting structure with a frequency and content appropriate to the level and kind of risks inherent in the outsourcing arrangement. The overarching purpose of this structure is to follow up and maintain alignment with the objectives of the Outsourcing Agreement.
    - Minutes should be kept during the meetings and be archived.
    - The meetings should have an agenda which covers at least:
        - Costs and budget.
        - Outcomes of self-monitoring activities performed by the Service Provider.
        - Material risks in the arrangement and their development during the period concerned.
        - Conflicts of interests that have arisen and their management, including events related to the Outsourcing Party's code of conduct.
        - Incidents that have occurred and their effect on the Service Provider's delivery.
        - Potential new areas of co-operation and improvements of the Outsourcing Agreement.
    - The meeting structure should also require that the Service Provider give the following assurances on a periodic basis:
        - Compliance with the Outsourcing Agreement.
        - Demonstration over time of employment of personnel with adequate skills and experience to ensure that the company has control over the outsourced activities.
        - Implementation of new rules and regulations relevant for the activities performed.
        - Adequacy of the Service Provider's risk management and internal control systems.
        - Demonstration over time of necessary financial resources to perform the additional tasks in a proper and reliable way.
        - Demonstration over time of necessary technical resources to perform the additional tasks in a proper and reliable way.
        - Adequacy of contingency plans in place to deal with emergency situations or business disruptions.

3. Establish a relevant reporting structure to the Management

    - The outcome from the meetings shall be reported in an executive summary which highlights the critical aspects of the deliveries.
    - The critical aspects should be expressed in terms that emphasise their relative urgency, i.e. risks are shown in red, orange, yellow and green, where red calls for immediate attention from the Management of the Outsourcing Party.
    - The report should be reviewed by the appropriate level of management. Thus, when the Management has signed the agreement, they should have access to the report.
    - The Service Provider shall have an obligation immediately to inform the Outsourcing Party of a situation where the Service Provider is approaching a default or being exposed to a change of control, e.g. through new owners. The Outsourcing Party needs to determine whether there are any conflicts of interest with the new owner and if necessary use the possibility to terminate the agreement.

EXIT STRATEGIES FOR OUTSOURCED BUSINESS

Guideline E. *Business continuity is a focus area in many industries. In accordance with the principles of responsibility and internal control, the Outsourcing Party should early in the outsourcing process negotiate general provisions for either transferring the outsourced business to a new Service Provider or resuming control over the outsourced business itself upon full or partial termination or expiration of the outsourcing arrangement.*

Outsourcing arrangements generally last for many years, making it challenging to anticipate the exact actions to be taken upon termination or expiration of the contract. In addition, an exit project could, in respect of more complex outsourcing, last several years and will—in the event of a transfer of the outsourced business to a new Service Provider—run partly parallel to the tender for such a new supplier.

Consequently, the Outsourcing Agreement should contain principles about termination or expiration of the outsourcing arrangement and the general obligations of the Service Provider in such a situation.

The general obligations of the Service Provider should cover at least the following.

- Provision of any exit assistance required to ensure the transfer of the outsourced business to the Outsourcing Party or a new Service Provider, e.g. necessary documentation, processes and relevant information and data.

- Participation in the exit project in a manner that ensures limited disruption to the outsourced part of the Outsourcing Party's business.
- Cooperation with any new Service Provider including allowing any new supplier to perform reasonable due diligence on the outsourced business to enable the transfer of the outsourced business to such new Service Provider.
- Drafting of a plan for exiting the outsourcing relation (an "Exit Management Plan"). The Exit Management Plan shall be maintained and continually updated by the Service Provider during the term of the outsourcing arrangement to ensure its immediate implementation when needed. The Exit Management Plan needs to provide details in respect of, among other things, the Service Provider's obligations to ensure that adequate documentation is drafted and maintained, the Service Provider's obligations regarding the migration of data and—if the outsourcing entails the transfer of hardware and software license agreements—the obligation to negotiate in good faith the retransfer of any transferred assets and the valuation principles applicable to such assets.

In addition, it is important for the Outsourcing Party to have the right to request exit assistance services from the Service Provider during an adequate period of time (which could last for several years) and to provide for the successive termination of the outsourcing services as the transfer to another Service Provider or the retransfer to the Outsourcing Party itself progresses. Since it is difficult to anticipate the duration of the exit project, it is advisable to include a provision in the outsourcing arrangement conferring a right to prolong the exit assistance if needed.

Finally, it is also advisable to agree on the principles for compensation and to detail the Service Provider's obligations as much as possible since the Service Provider's incentive to participate in the transfer of the services to another Service Provider is limited upon termination or expiration of the outsourcing arrangement.

* * * *

Appendix A

CHECK LIST

to be filled in by the Outsourcing Party before signing an Outsourcing Agreement

The check list is based on the principle that the Outsourcing Party cannot outsource the responsibility for how the outsourced services are conducted, how customers are treated, or how regulatory requirements are met. Where the answer to a certain issue is "no', this would raise the question as to why outsourcing would still be recommended. The check list should be signed by the Account Manager responsible for the activities to be outsourced.

The final and signed check list should be an important piece of evidence on the basis of which the final decision by the Outsourcing Party whether to outsource a specific part of the business will be made.

Check points	Yes	No	Comment
1. Do we have updated internal rules adopted by the Management regarding types of activities which may be outsourced, and routines and processes for: · establishing an Outsourcing Agreement · maintaining procurement skills "at home" · ensuring that the Service Provider meets requirements on competence, internal control, quality, long-term possibility to fulfil outsourced activities · maintaining the right to instruct the Service Provider · follow-up of outcome · follow-up and management of risks			
2. Are the reasons for outsourcing, the targets/goals, expected costs and revenues clearly documented?			
3. Can the activities to be outsourced be classified as "problem activities"?			
4. Are the activities to be outsourced related to our core business?			
5. Does the Service Provider meet our regulatory requirements, standards, values?			
6. Are conflicts of interest identified and documented?			
7. Who will have the business responsibility for the outsourced activities going forward (Account Manager)?			

8. Are there controls in place to ensure the desired outcome?			
9. Do we have a strategy and plan for ending the outsourcing assignment and resuming the activities? Are they documented?			
10. Has a group perspective with the Outsourcing Party been explored? Pros & cons? Are possible effects for employees identified (group perspective)?			
11. Have the relevant company functions (Finance, Compliance, Risk, Internal Audit, Security, etc.) been informed and involved in the Outsourcing project? Have they conducted a risk assessment in connection to the planned outsourcing? Are their opinions part of the basis for the decision to outsource?			
12. Are all risks inherent in the activities to be out-sourced identified?			
13. How will such risks be managed and followed up during the Outsourcing Agreement?			
14. What will be the role of support functions and control functions of the Outsourcing Party during the Outsourcing Agreement?			
15. Are all decisions during the Outsourcing project documented and measured against the objective to outsource an activity?			
Issues to be part of the Outsourcing Agreement	**Yes**	**No**	**Comment**
1. Are the services to be outsourced specified in detail?			
2. Are the roles and responsibilities of each part sufficiently described?			

3. Are there possibilities for the Outsourcing Party to give instructions on how to carry out the activities secured?			
4. Are service levels and price levels included?			
5. Is subcontracting allowed? With our consent?			
6. Is the obligation for the Service Provider to implement routines for contingency planning documented?			
7. Has unrestricted accessibility for regulator and auditors been secured?			
8. Is the obligation to immediately notify the Outsourcing Party on conditions/issues which are threatening the outsourced activities secured?			
9. How will confidential information be treated?			
10. Have the mandates to employees with the Service Provider been clearly specified?			
11. Has an effective monitoring and follow-up of how the outsourced activities are carried out been specified? Are there clear sanctions in conjunction with breaches?			
12. How are efficient and relevant information and staff training with the Service Provider ensured?			
13. How will incidents at the Service Provider be managed?			

Hereby I confirm that the above questions have been answered honestly and to the best of my knowledge.

City Date

Name Title