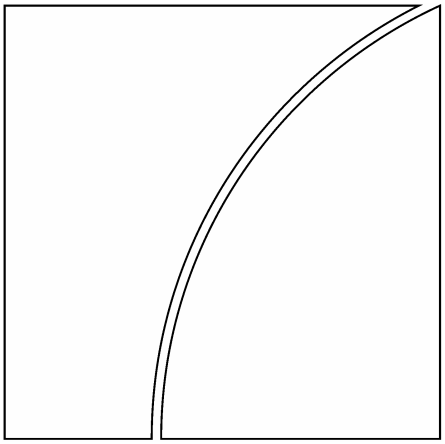
Basel Committee
on Banking Supervision

The Joint Forum



Outsourcing in Financial Services

Consultative document

August 2004

BANK FOR INTERNATIONAL SETTLEMENTS

THE JOINT FORUM

BASEL COMMITTEE ON BANKING SUPERVISION
INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS
INTERNATIONAL ASSOCIATION OF INSURANCE SUPERVISORS
C/O BANK FOR INTERNATIONAL SETTLEMENTS
CH-4002 BASEL, SWITZERLAND

Outsourcing in Financial Services

2 August 2004

Table of Contents

Outsourcing in Financial Services

1. Executive Summary

Financial services businesses throughout the world are increasingly using third parties to carry out activities that the businesses themselves would normally have undertaken. Industry research and surveys by regulators show financial firms outsourcing significant parts of their regulated and unregulated activities. These outsourcing arrangement are also becoming increasingly complex.

Outsourcing has the potential to transfer risk, management and compliance to third parties who may not be regulated, and who may operate offshore.

In these situations, how can financial service businesses remain confident that they remain in charge of their own business and in control of their business risks? How do they know they are complying with their regulatory responsibilities? How can these businesses demonstrate that they are doing so when regulators ask?

To help answer these questions and to guide regulated businesses, the Joint Forum established a working group to develop high-level principles about outsourcing.

In this paper, the key issues and risks are spelt out in more detail and principles are put forward that can serve as benchmarks. The principles apply across the banking, insurance and securities sectors, and the international committees involved in each sector[1] may build on these principles to offer more specific and focused guidance. Selected international case studies (see Annex A) show why these questions matter.

Today outsourcing is increasingly used as a means of both reducing costs and achieving strategic aims. Its potential impact can be seen across many business activities, including information technology (eg, applications development, programming, and coding), specific operations (eg, some aspects of finance and accounting, back-office activities & processing, and administration), and contract functions (eg, call centres). Industry reports and regulatory surveys of industry practice indicate that financial firms are entering into arrangements in which other firms – related firms within a corporate group and third-party service providers – conduct significant parts of the enterprise's regulated and unregulated activities.[2]

Activities and functions within an organisation are performed and delivered in diverse ways. An institution might split such functions as product manufacturing, marketing, back-office and distribution within the regulated entity. Where a regulated entity keeps such arrangements in-house, but operates some activities from various locations, this would not be classified as outsourcing. The entity would therefore be expected to provide for any risks posed by this in its regular risk management framework.

Increasingly more complex arrangements are developing whereby related entities perform some activities, while unrelated service providers perform others. In each case the service

---

[1] The Basel Committee on Banking Supervision (BCBS), the International Organization of Securities Commissions (IOSCO) and the International Association of Insurance Supervisors (IAIS).

[2] Bank Information Technology Secretariat (BITS) Framework for Managing Technology Risk for IT Service Provider Relationships, Version II, November 2003, p. 2.

provider may or may not be a regulated entity. The Joint Forum principles are designed to apply whether or not the service provider is a regulated entity.

Outsourcing has been identified in various industry and regulatory reports as raising issues related to risk transfer and management, frequently on a cross-border basis, and industry and regulators acknowledge that this increased reliance on the outsourcing of activities may impact on the ability of regulated entities to manage their risks and monitor their compliance with regulatory requirements. Additionally, there is concern among regulators as to how outsourcing potentially could impede the ability of regulated entities to demonstrate to regulators (eg, through examinations) that they are taking appropriate steps to manage their risks and comply with applicable regulations.

Among the specific concerns raised by outsourcing activities is the potential for over-reliance on outsourced activities that are critical to the ongoing viability of a regulated entity as well as its obligations to customers.

Regulated entities can mitigate these risks by taking steps (as discussed in the Principles) to: draw up comprehensive and clear outsourcing policies, establish effective risk management programmes, require contingency planning by the outsourcing firm, negotiate appropriate outsourcing contracts, and analyse the financial and infrastructure resources of the service provider.

Regulators can also mitigate concerns by ensuring that outsourcing is adequately considered in their assessments of individual firms whilst taking account of concentration risks in third party providers when considering systemic risk issues.

Of particular interest to regulators is the preservation at the regulated entity of strong corporate governance. In this regard outsourcing activities that may impede an outsourcing firm's management from fulfilling its regulatory responsibilities are of concern to regulators. The rapid rate of IT innovation, along with an increasing reliance on external service providers have the potential of leading to systemic problems unless appropriately constrained by a combination of market and regulatory influences.

This paper attempts to spell out these concerns in more detail and develop a set of principles that gives guidance to firms, and to regulators, to help them better mitigate these concerns without hindering the efficiency and effectiveness of firms.

2. Guiding principles - Overview

The Joint Forum has developed the following high- level principles. The first seven principles cover the responsibilities of regulated entities when they outsource their activities, and the last two principles cover regulatory roles and responsibilities. Here we present an overview of the principles. More detail may be found in section 9.

I. **A regulated entity seeking to outsource activities should have in place a comprehensive policy to guide the assessment of whether and how those activities can be appropriately outsourced. The board of directors or equivalent body retains responsibility for the outsourcing policy and related overall responsibility for activities undertaken under that policy.**

II. **The regulated entity should establish a comprehensive outsourcing risk management program to address the outsourced activities and the relationship with the service provider.**

III. **The regulated entity should ensure that outsourcing arrangements neither diminish its ability to fulfil its obligations to customers and regulators, nor impede effective supervision by regulators.**

IV. **The regulated entity should conduct appropriate due diligence in selecting third party service providers.**

V. **Outsourcing relationships should be governed by written contracts that clearly describe all material aspects of the outsourcing arrangement, including the rights, responsibilities and expectations of all parties.**

VI. **The regulated entity and its service providers should establish and maintain contingency plans, including a plan for disaster recovery and periodic testing of backup facilities.**

VII. **The regulated entity should take appropriate steps to require that service providers protect confidential information of both the regulated entity and its clients from intentional or inadvertent disclosure to unauthorised persons.**

VIII. **Regulators should take into account outsourcing activities as an integral part of their ongoing assessment of the regulated entity.**

Regulators should assure themselves by appropriate means that any outsourcing arrangements do not hamper the ability of a regulated entity to meet its regulatory requirements.

IX. **Regulators should be aware of the potential risks posed where the outsourced activities of multiple regulated entities are concentrated within a limited number of service providers.**

3. Definition

Outsourcing is defined in this paper as a regulated entity's use of a third party (either an affiliated entity within a corporate group or an entity that is external to the corporate group) to perform activities on a continuing basis that would normally be undertaken by the regulated entity, now or in the future.

Outsourcing can be the initial transfer of an activity (or a part of that activity) from a regulated entity to a third party or the further transfer of an activity (or a part thereof) from one third-party service provider to another, sometimes referred to as "subcontracting." In some jurisdictions, the initial outsourcing is also referred to as subcontracting.

According to this definition, outsourcing would not cover purchasing contracts, for example, contracts to purchase standardised products such as furniture or software.

This paper will refer to a **regulated entity** as the body that is authorised for a regulated activity by a regulator. The principles set forth in this paper are targeted at such entities.

Third party or **service provider** refers to the entity that is undertaking the outsourced activity on the behalf of the regulated entity.

The term regulator refers to all supervisory and regulatory authorities that authorise firms to undertake any regulated activity and supervise that activity.

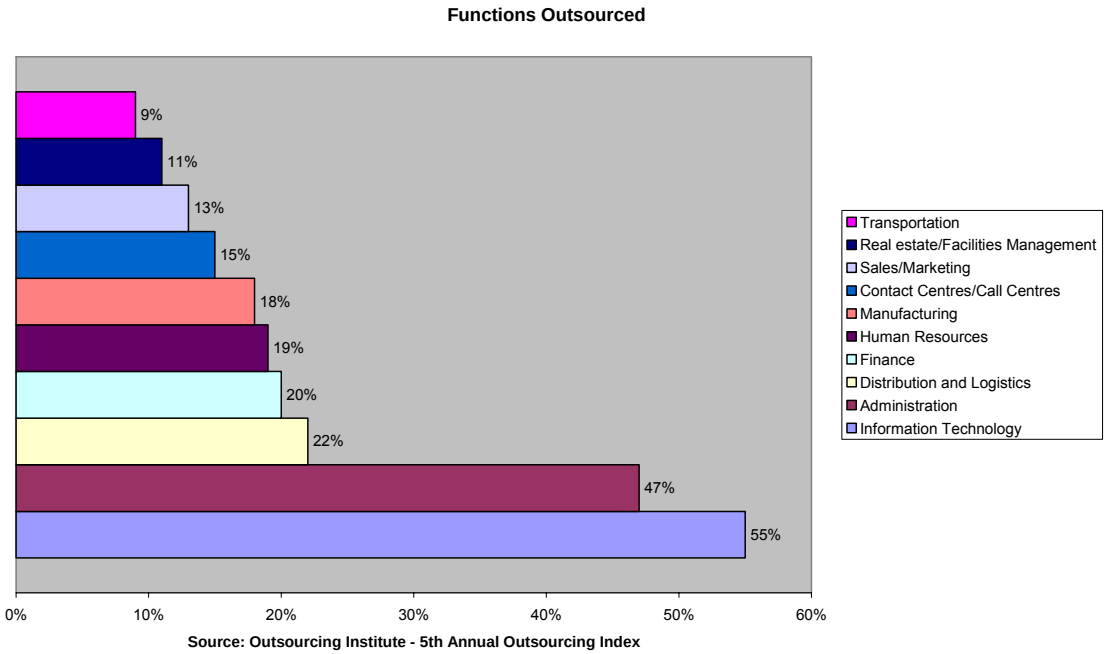
4. Developments in Industry Practice and motivation

Whilst primarily anecdotal and partial in nature, a body of evidence points to the rapid growth of outsourcing activity in recent years.

For example, Deloitte has estimated that US$ 356 billion of the US Financial Service's Industry will be outsourced to offshore locations in the next five years[3]. This represents 15% of the industry's current cost base according to Deloitte. The Outsourcing Institute has conducted surveys of various companies and organizations on their outsourcing practices. According to its 5th Annual Outsourcing Index, activities being outsourced by respondents include the following:

[3] **Deloitte** presentation to Board of Governors of the Federal Reserve System *Offshoring and Cross-Border Outsourcing by Banks*, March 30 2004.

Graph 1: Activities Outsourced

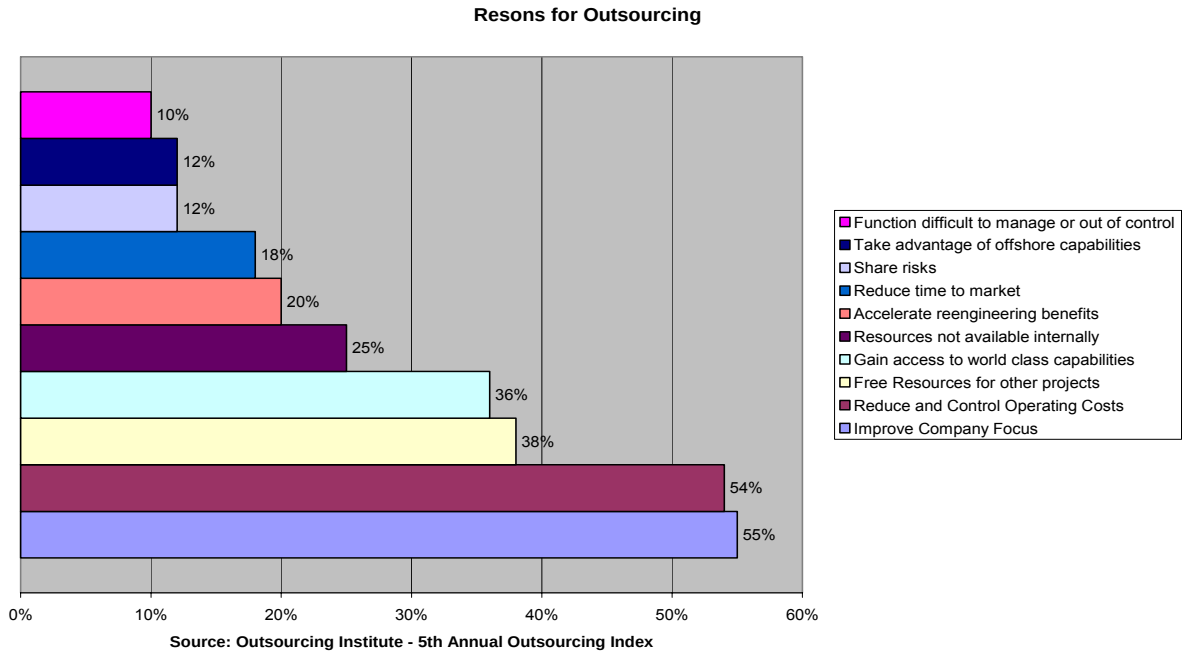


The graph shows that IT related services appear to be the most frequently outsourced activities, which chimes with evidence from other studies and the Joint Forum's own experience. One estimate[4] is that of some $340 billion spent on IT globally in 2003 $120 billion or a third was entrusted to third parties. However, the graph also illustrates the growth of other activities that are now being outsourced, including human resources and finance. Such growth is part of a trend away from outsourcing of specific tasks towards the growth of strategic outsourcing (see outsourcing trends below).

There are many compelling commercial reasons for outsourcing, not least of which is the potential for significant cost savings by outsourcing to an operator who has managed to develop scale economies in a particular transactional area, or to an operator who has access to lower cost labour in another country. The main reasons given for outsourcing certain activities are set out in the table below.

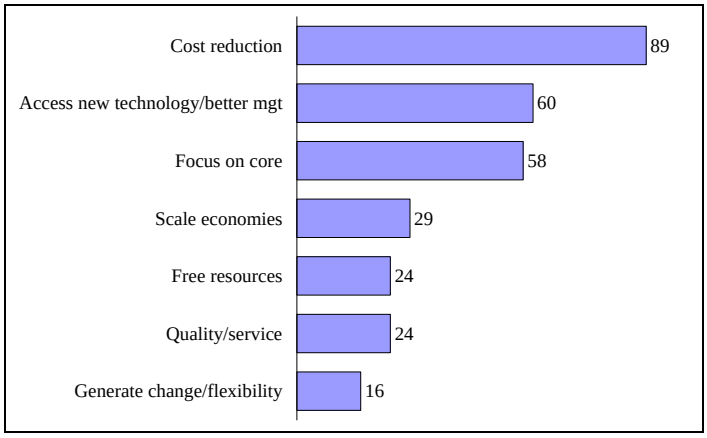
[4] www.banktech.com February 27 2003.

Graph 2: Reasons for Outsourcing



More geographically specific details exist for the EU where the European Central Bank has undertaken a survey of motives for outsourcing.

Graph 3: EU banks' motives for outsourcing (%)



Source: European Central Bank

While outsourcing has grown in importance across all three financial sectors, patterns of outsourcing are not identical in each sector. In particular the fund management and insurance sectors have for some time outsourced activities which could be potentially considered to be core functions. These include:

- Investment management: Many insurers and fund managers now outsource investment management to external parties and/or related group entities.

- Unit pricing and custody: In many instances the striking of unit prices and custody arrangements are outsourced to third parties in respect of unit linked funds and products.
- Underwriting and claims payment: some underwriters allow insurance brokers to accept certain underwriting risks on their behalf and to process claims.

There are genuine reasons for this trend, such as the importance of core expertise when entering a new market, and the benefits of economy of scale, but arrangements can still go wrong as Case study 3 in Annex A demonstrates.

5. Current Trends in Outsourcing

Financial firms have entered into outsourcing arrangements for many years, albeit not to the extent seen in the recent past. For example, in the securities industry, since the 1970s, firms have outsourced quasi-clerical activity, such as the printing and storage of records. This was undertaken because of the comparative cost savings.

As technology has evolved, outsourcing of information services has become more common. In the 1980s and 1990s, such deals tended to be large scale and often involved the outsourcing of whole IT divisions primarily based on cost and the importance of remaining up to date with rapidly evolving technology.

Subsequently we have seen a growth of outsourcing in more strategic areas such as human resources and some have observed the trend of "business processing outsourcing," (BPO) i.e., end-to-end outsourcing of a business line or process in its entirety. BPOs also mean that the relationship between the outsourcer and the third party changes somewhat as the latter becomes more of a strategic partner than a traditional supplier.

Another major trend in outsourcing that appears to have gained momentum is "off-shoring," i.e., effectively outsourcing activities beyond national borders. Many conglomerates are trying to create global efficiencies by basing transaction processing and call centres offshore. Arrangements are sometimes entered into with unrelated parties, while in other cases the outsourcing firm establishes its own off-shore base (i.e., through an affiliate) to provide services.

In India alone a range of organisations have set up outsourcing arrangements as illustrated by the sample of firms in the table below. (Approximate staff numbers in parentheses).

Table 1: Financial Services Companies in India in 2003

ABN Amro (300+)	Amex (1000+)
Axa (380)	Citigroup (3,000)
Deutsche Bank (500)	GE (11,000)
HSBC (2000)	JP Morgan Chase (480)
Mellon Financial (240)	Merrill Lynch (350)
Standard Chartered (3,000)	

Source: **Deloitte** presentation to Board of Governors of the Federal Reserve System *Offshoring and Cross-Border Outsourcing by Banks*, March 30 2004.

Anecdotal evidence suggests that China, Malaysia and the Philippines are also seen as desirable outsourcing locations.

According to a 2004 report by Deloitte[5], offshoring will continue to grow throughout this decade. The report estimates the percentage of global financial services companies with offshore facilities grew to 67% in 2003 compared with 29% in 2002. It further estimates that by 2005 some $210bn of industry costs will be offshore, rising to $400bn or 20% of the total industry cost base in 2010.

The report notes that the percentage for large firms is significantly higher than for small firms and also notes that increasingly firms are setting up their own operations offshore, distinguishing this trend from the growth of outsourcing per se.

At a practical level this growth in off-shoring has led to a need for regular monitoring of "country risk" which means that an outsourcing institution needs to monitor foreign government policies and political, social, economic and legal conditions in the country where it has a contractual relationship with a service provider. It should also develop appropriate contingency plans and exit strategies. As part of an organisations' need to consider business continuity issues it should consider whether the processes could quickly revert to the home country in extremis?

6. Regulatory Developments

Regulators have recognised the issues that outsourcing presents at both a national and international level. The Joint Forum has liaised with a number of other international working groups in developing this set of principles, which is applicable across all financial sectors. Other international work streams include:

- The Committee of European Banking Supervisors (CEBS) has taken forward the work started by the Groupe de Contact by publishing a set of principles, in April 2004, on outsourcing for public consultation. The principles are primarily aimed at EU banks with additional guidelines for regulators. But they are designed in such a way that they could be read across to other sectors and the other EU sectoral committees.
- The Committee of European Securities Regulators (CESR) is developing advice on the implementation of EU legislation on outsourcing within the Markets in Financial Instruments Directive (MIFID).
- The Committee of European Insurance and Occupational Pensions Supervisors (CEIOPS) is also likely to have an interest in this area.
- The Basel Committee's E-banking Group is about to review IT outsourcing practices among its members and consider a new mandate related to outsourcing.
- An IOSCO standing committee has drafted a set of principles on outsourcing. It is expected that the draft will be provided to the securities industry for consultation. In addition, it is expected that the standing committee will conduct a survey and/or review the results of surveys done on securities firm outsourcing practices.

[5] Deloitte's second annual offshore survey *The Titans Take Hold*.

- The IAIS is monitoring emerging outsourcing practices and regulatory responses.

A number of national regulators already have standards or legislative controls on outsourcing. Here is a broad sample of national approaches:

Table 2: National Approaches to Outsourcing

Australia	Prudential Standards on outsourcing for banks were introduced with effect from 1 July 2002. The insurance sector has been advised that they are also expected to follow these standards pending their formal introduction.
Belgium	In June 2004 the CBFA issued a common guidance circular for both the banking and investment services sector, based largely on the CEBS consultative paper. Consultation has started for implementing the same for the insurance sector.
Canada	In May 2001 OSFI introduced guideline B-10, setting out the expectations when outsourcing,. A revised version of the guideline was issued in December 2003. All federally regulated entities are expected to comply with the revised guideline by 15 December 2004.
Germany	In December 2001 the German authorities issued guidelines covering all credit institutions and financial services institutions. These guidelines describe the requirements for outsourcing, which should ensure that the outsourcing of operational activities does not impair: (1) the orderliness of such business or services; (2) the managers' ability to manage and monitor those activities; or (3) BaFin's right to audit and ability to monitor the credit institution under its jurisdiction.
Japan	In April 2001 the Bank of Japan published a sound practice paper for financial institutions, setting out its expectation for risk management in outsourcing. The Financial Services Agency issues inspection manuals for financial institutions. The manuals establish risk management check points for outsourcing arrangements.
Netherlands	On 1 April 2001 De Nederlandsche Bank (prudential supervisor of credit institutions) issued the Regulation on Organisation and Control. Section 2.6 of this regulation is dedicated to the outsourcing of (components of) business processes. On 1 February 2004 the Pensioen- & Verzekeringskamer (Pensions and Insurance Supervisory Authority of the Netherlands) (the prudential supervisor of insurance companies and pension funds) issued the Regulation on Outsourcing by Insurance Companies.
Switzerland	In August 1999, the Swiss Federal Banking Commission (SFBC),introduced "Outsourcing Guidelines" for banks and securities firms, allowing outsourcing without explicit consent by the SFBC. Compliance with the guidelines are subject to the annual external audit. Outsourcing has to be established in a written contract and requires the integration of outsourced activities in the scope of the internal control system of a financial institution. An outsourcing contract must explicitly allow for visits and controls by the financial institution, its internal and external audit firm and the SFBC. Outsourcing is not allowed for functions of the board and for

	central functions of the management of the financial institution.
United Kingdom	The UK FSA sets out its guidelines for banks and building societies in the Interim Prudential Sourcebook for banks. A guidance note P3 in the Interim Prudential Sourcebook for insurers covers much the same ground. The guidelines cover both material and non-material outsourcing but concentrate on material outsourcing. A firm should always notify the FSA prior to entering into a material outsourcing arrangement. In December 2004 new guidelines will be introduced in SYSC 3A.7, a new chapter of the FSA handbook. .
United States (Securities Firms)	Historically, securities regulators have given prior approval to certain outsourcing proposals that represent changes to traditional processes and procedures previously housed within securities firms. Rules 342, 346 and 382 of the New York Stock Exchange (of which most large firms are members) have been interpreted to preclude or limit outsourcing either entirely or only to regulated persons. The registration requirements of the Securities Exchange Act have been interpreted to preclude unregistered persons (registered with proper securities organizations) from doing certain kinds of activities.
United States (Banks)	The FFIEC, the umbrella organisation for the five US financial institution regulatory agencies, has issued a series of guidelines and bulletins aimed at clarifying banks' duties in managing risk in IT outsourcing relationships and providing guidance to examiners. Recent updates specifically address information security risks in third-party relationships. Current key US bank regulatory guidance on outsourcing include: OCC Bulletin 2001-47, Third-Party Relationships: Risk Management Principles (November 2001). FFIEC Guidance on Risk Management of Outsourced Technology Services (November 2000). FDIC's three technology bulletins entitled Effective Practices for Selecting a Service Provider; Tools to Manage Technology Providers' Performance Risk: Service Level Agreements; and Techniques for Managing Multiple Service Providers (June 2001). FFIEC IT Handbook entitled "The Supervision of Technology Service Providers (TSP) Booklet" (May 2003), which outlines a risk-based supervision approach to the oversight and management of TSP relationships. In mid-2004 US bank supervisors finalised an updated FFIEC IT Examination Handbook on Outsourcing Technology Services, which will provide guidance and examination procedures to assist examiners in evaluating a financial institution's risk management processes to establish, manage, and monitor IT outsourcing relationships.

United States (Insurance)	Insurers' outsourcing of activities is addressed by state insurance supervisors in a variety of ways in the U.S. Outsourcing essential functions is addressed through specific legal authority granted to the supervisor Examples of this include the laws on managing general agents and third-party administrators (set forth in the NAIC Managing General Agents Model Act, Third-Party Administrator Model Statute). Other activities which are outsourced would be addressed in the on-site market conduct examination process where a company's internal controls would be examined - eg, claims processing or investment management - and violations addressed through the supervisor's authority to prevent unfair claims settlement or unfair trade practices. The NAIC Market Regulation and Consumer Affairs (D) Committee has created a Third Party Vendor Working Group to address further where current regulatory authority does not extend to certain areas in which insurance companies use third party service providers. The Group expects to produce recommendations for incorporation into the NAIC's Market Conduct Examiners Handbook.

7. Key Risks of Outsourcing

While the outsourcing of certain activities can create a number of benefits to a financial services organisation there are a number of risks which need to be managed effectively. Some of these key risks are mapped out in the table below.

Table 3: Some Key Risks in Outsourcing

Risk	**Major concerns**
Strategic Risk	The third party may conduct activities on its own behalf which are inconsistent with the overall strategic goals of the regulated entity. Failure to implement appropriate oversight of the outsource provider. Inadequate expertise to oversee the service provider.
Reputation Risk	Poor service from third party Customer interaction is not consistent with overall standards of the regulated entity. Third party practices not in line with stated practices (ethical or otherwise) of regulated entity.
Compliance Risk	Privacy laws are not complied with. Consumer and prudential laws not adequately complied with. Outsource provider has inadequate compliance systems and controls.
Operational Risk	Technology failure. Inadequate financial capacity to fulfil obligations and/or provide remedies. Fraud or error. Risk that firms find it difficult/costly to undertake inspections.
Exit Strategy Risk	The risk that appropriate exit strategies are not in place. This could arise from over-reliance on one firm, the loss of relevant skills in the institutions

Risk	Major concerns
	itself preventing it bringing the activity back in-house and contracts which make a speedy exit prohibitively expensive. Limited ability to return services to home country due to lack of staff or loss of intellectual history.
Counterparty Risk	Inappropriate underwriting or credit assessments. Quality of receivables may diminish.
Country Risk	Political, social and legal climate may create added risk. Business continuity planning is more complex.
Contractual Risk	Ability to enforce contract. For off-shoring, choice of law is important.
Access Risk	Outsourcing arrangement hinders ability of regulated entity to provide timely data and other information to regulators. Additional layer of difficulty in regulator understanding activities of the outsource provider.
Concentration and Systemic Risk	Overall industry has significant exposure to outsource provider. This concentration risk has a number of facets including: • Lack of control of individual firms over provider; and • Systemic risk to industry as a whole

8. Issues in Approaching the Principles

Definition: The Joint Forum's working group engaged in significant debate when drawing up an adequate definition of outsourcing. Key issues of concern were keeping the definition as broad and brief as possible whilst acknowledging the importance of avoiding coverage of tasks that are normally beyond the remit of financial supervisors, such as the provision of water or office furniture (even though theoretical but extreme scenarios could be construed in which these services became of relevance to supervisors). To this end the group relied heavily on work undertaken by the Committee of European Banking Supervisors (CEBS) and the International Organisation of Securities Commissions (IOSCO). The latter was helpful in determining a positive approach by outlining activities that we would normally expect a regulated entity to undertake on an ongoing basis. The former was helpful in defining the group's understanding of the key purchasing contracts that should be excluded.

Affiliates*:* The group held a related discussion about whether the definition should include outsourcing to affiliates. The group decided unanimously that it should. The group acknowledges however concerns expressed about setting out principles to cover affiliates that themselves may have been set up for regulatory or other legal purposes. The group took some comfort from the fact that the recommendations laid out here are most likely to be in place anyway for affiliates.

Materiality: The group discussed the helpfulness of differentiating between material and non-material activities and having different levels of compliance according to the level of materiality. However, this route was not chosen in recognition that materiality would mean different things in different sectors and countries. Instead the definition used here deliberately excludes some obviously non-material activities from the scope of this project, such as purchasing contracts. Further, the principles encourage firms to consider the level of

materiality in scoping their risk management processes, and give some guidelines to assist this consideration.

Responsibility of firm's management: The group was unanimous in its view that the principles should stress the responsibility of firms' senior management for all activities, whether outsourced or not.

Proscription of particular activities: There was some debate about the utility and applicability of proscribing the outsourcing of certain core activities. However, in light of the broad coverage of these principles, and the differences in the sectors for which they are designed, a limiting approach was agreed under which no particular activity would be proscribed with the recognition that more detailed sectoral principles could build on the Joint Forum principles to proscribe the outsourcing of certain activities.

Systemic issues: The Joint Forum was acutely aware of the risks of systemic issues that could arise from outsourcing, even though these principles are designed to tackle the risks of outsourcing on a micro-firm level basis. To this end the group felt compelled to include a specific principle to assist supervisors in monitoring the risks of concentration in third party providers and the systemic risks therein.

9. Guiding Principles—Detail

The Joint Forum developed the following high- level principles. A summary can be found in section two.

I. A regulated entity seeking to outsource activities should have in place a comprehensive policy to guide the assessment of whether and how those activities can be appropriately outsourced. The board of directors or equivalent body retains responsibility for the outsourcing policy and related overall responsibility for activities undertaken under that policy.

Prior to the outsourcing of activities, a regulated entity should establish specific policies and criteria for making decisions about outsourcing. These should include an evaluation of whether, and the extent to which, the relevant activities are appropriate for outsourcing. Risk concentrations, limits on the acceptable overall level of outsourced activities and risks arising from outsourcing multiple activities to the same service provider must all be considered.

If a regulated entity desires to outsource any of its activities, its management should develop a comprehensive understanding of the associated benefits and costs. This analysis requires an assessment of the organisation's core competencies, managerial strengths and weaknesses, and future goals.

The regulated entity must also have in place policies that ensure its ability to oversee effectively the activity being outsourced (see principle II).

The regulated entity must take appropriate steps to ensure its ability to comply with legal and regulatory requirements in both its home and host countries, as applicable.

An activity should not be outsourced if it would impair the supervisory authority's right to assess, or its ability to supervise, the business of the regulated entity (See principle III).

The regulated entity's Board of Directors (or equivalent body) has overall responsibility for ensuring that all ongoing outsourcing decisions taken by the regulated entity, and activities undertaken by the third parties, are in keeping with its outsourcing policy. The role of internal audit also will be important in this regard.

II. The regulated entity should establish a comprehensive outsourcing risk management program to address the outsourced activities and the relationship with the service provider.

When establishing an outsourcing risk management programme, the assessment of outsourcing risk at a regulated entity will depend on several factors including: the scope and materiality of the outsourced activity; how well the regulated entity manages, monitors and controls outsourcing risk (including its general management of operational risk); and how well the service provider manages and controls the potential risks of the operation.

Factors that would help to define materiality and a risk management programme include the following:

- The financial, reputational and operational impact on the regulated entity of the failure of a service provider to adequately perform the activity;

- Potential losses to a regulated entity's customers and their counterparts in the event of a service provider failure;
- Consequences of outsourcing the activity on the ability and capacity of the regulated entity to conform with regulatory requirements and changes in requirements,
- Cost;
- Interrelationship of the outsourced activity with other activities within the regulated entity;
- Affiliation or other relationship between the regulated entity and the service provider;
- Regulatory status of the service provider;
- Degree of difficulty and time required to select an alternative service provider or to bring the business activity in-house, if necessary; and
- Complexity of the outsourcing arrangement. For example, the ability to control the risks where more than one service provider collaborates to deliver an end-to-end outsourcing solution.

Data protection, security and other risks may be adversely affected by the geographical location of an outsourcing service provider. To this end, specific risk management expertise in assessing country risk, for example, related to political or legal conditions, could be required when entering into and managing outsourcing arrangements that are taken outside of the home country.

More generally, a comprehensive outsourcing risk management program should provide for an ongoing monitoring and controlling of all relevant aspects of outsourcing arrangements and for procedures guiding corrective actions to be taken when certain events occur.

III. The regulated entity should ensure that outsourcing arrangements neither diminish its ability to fulfil its obligations to customers and regulators, nor impede effective supervision by regulators.

Outsourcing arrangements should not affect the rights of a customer against the regulated entity, including the ability of the customer to obtain redress as applicable under relevant laws.[6]

Outsourcing arrangements should not impair the regulator's ability to exercise its regulatory responsibilities such as proper supervision of a regulated entity.

IV. The regulated entity should conduct appropriate due diligence in selecting third party service providers.

A regulated entity must develop criteria that enable it to assess, prior to selection, the third party service provider's capacity and ability to perform the outsourced activities effectively, reliably and to a high standard, together with any potential risk factors associated with using a particular service provider.

---

[6] A regulated entity may of course pursue any applicable legal rights it may have against a third party provider.

Appropriate due diligence should include: (1) the selection of service providers qualified and with adequate resources to perform the outsourcing work; (2) ensuring that the service provider understands and can meet the objectives of the regulated entity in the specified activity; and (3) recognition of the service provider's financial soundness to fulfil its obligations. Any special needs, such as servicing geographically dispersed activities, must be determined and met by using third parties with similar reach or capability.

Activities should not be outsourced to a service provider that does not meet the criteria.

If a service provider fails, or is otherwise unable to perform the outsourced activity, it may be costly or problematic to find alternative solutions. Transition costs, and potential business disruptions should thus also be considered.

Additional concerns exist if outsourcing an activity abroad. For example, in an emergency, the regulated entity may find it more difficult to implement appropriate responses in a timely fashion. Accordingly, senior management of a regulated entity may need to assess the economic, legal and political conditions that might adversely impact the service provider's ability to perform effectively for the regulated entity.

V. Outsourcing relationships should be governed by written contracts that clearly describe all material aspects of the outsourcing arrangement, including the rights, responsibilities and expectations of all parties.

Outsourcing arrangements should be governed by a clearly written contract, the nature and detail of which should be appropriate to the materiality of the outsourced activity in relation to the ongoing business of the regulated entity. A written contract is an important management tool and appropriate contractual provisions can reduce the risk of non-performance or disagreements regarding the scope, nature and quality of the service to be provided. Some key provisions of this contract would be that:

- The contract should clearly define what activities are going to be outsourced, including appropriate service and performance levels. The service provider's ability to meet performance requirements in both quantitative and qualitative terms should be assessable in advance;
- The contract should neither prevent nor impede the regulated entity from meeting their respective regulatory obligations, nor the regulator from exercising its regulatory powers;
- The regulated entity must ensure it has the ability to access all books, records and information relevant to the outsourced activity in the service provider;
- The contract should provide for the continuous monitoring and assessment by the regulated entity of the service provider so that any necessary corrective measures can be taken immediately;
- A termination clause and minimum periods to execute a termination provision, if deemed necessary, should be included. The latter would allow the outsourced services to be transferred to another third party service provider or to be incorporated into the regulated entity. Such a clause should include provisions relating to insolvency or other material changes in the corporate form, and clear delineation of ownership of intellectual property following termination, including transfers of information back to the regulated entity (see principle VI below) and other duties that continue to have an effect after the termination of the contract;

- Material issues unique to the outsourcing arrangement should be meaningfully addressed. For example, where the service provider is located abroad, the contract should include choice-of-law provisions and agreement covenants and jurisdictional covenants that provide for adjudication of disputes between the parties under the laws of a specific jurisdiction;
- The contract should include, where appropriate, conditions of subcontracting by the third party service provider for all or part of an outsourced activity In appropriate cases it should require approval by the regulated entity of the use of subcontractors by the third party service provider for all or part of a serviced activity or activity being delivered. More generally, the contract should provide the regulated entity with the ability to maintain a similar control over the risks when a service provider outsources to other third parties as in the original direct outsourcing arrangement.

VI. The regulated entity and its service providers should establish and maintain contingency plans, including a plan for disaster recovery and periodic testing of backup facilities.

A regulated entity should take appropriate steps to assess and address the potential consequence of a business disruption or other problem at the service provider. Notably, it should consider contingency plans at the service provider; co-ordination of contingency plans at both the regulated entity and the service provider; and contingency plans of the regulated entity in the event of non-performance by the service provider.

Recurring performance problems coupled with the absence of comprehensive contingency plans by the service provider and the regulated entity may result in unintended credit exposures, financial losses, missed business opportunities and reputational and legal concerns.

Robust information technology security is a necessity. A breakdown of IT capacity may impair the ability of the regulated entity to fulfil its obligations to other market participants, could undermine the privacy interests of its customers, harm the regulated entity's reputation, and may ultimately impact on the overall operational risk profile of the regulated entity. Regulated entities should seek to ensure that service providers maintain appropriate IT security, and, when appropriate, disaster recovery capabilities.

Contingency plans, in the event of deteriorating performance, must account for the costs of alternative options. In the face of unsatisfactory responsiveness from the service provider, a regulated entity's options include changing service providers, moving the activity internally to the institution, or sometimes even exiting the business. These could be very costly options, which are often taken only as a last measure. Nevertheless, these eventualities and associated costs should be addressed during the negotiation process and specified in the contract. In existing contracts, such clauses should be added at renewal.

VII. The regulated entity should take appropriate steps to require that service providers protect confidential information of both the regulated entity and its clients from intentional or inadvertent disclosure to unauthorised persons.

A regulated entity that engages in outsourcing is expected to take appropriate steps to protect confidential customer information and confirm that it is not misused or misappropriated. Such steps may include provisions in the contract with the third party prohibiting the service provider and its agents from using or disclosing the regulated entity's proprietary information or that of its customers, except as necessary to provide the contracted services and to meet regulatory and statutory provisions. A regulated entity should also consider whether it is appropriate to notify customers that customer data may be

transmitted to a service provider, taking into account any regulatory or statutory provisions that may be applicable.

VIII. Regulators should take into account outsourcing activities as an integral part of their ongoing assessment of the regulated entity.

Regulators should assure themselves by appropriate means that any outsourcing arrangements do not hamper the ability of the regulated entity to meet its regulatory requirements.

Regulators should consider outsourcing activities as part of their overall risk assessment of a regulated entity.

In order to be able to assess and monitor the outsourcing policy and outsourcing risk management program of a regulated entity, regulators should be able, upon request, to obtain promptly any relevant books and records pertaining to the outsourced activity, irrespective of whether they are in the possession of the outsourcing firm or the third party service provider, and to obtain additional information concerning outsourced activities. A regulator's access to such books and records may be direct or indirect, though the regulated entity should always maintain direct access to such books and records. This may include a requirement that the books and records be maintained in the regulator's jurisdiction, or that the service provider agrees to send originals or copies of the books and records to the regulator's jurisdiction upon request.

Regulators should consider implementation of appropriate regulations and measures designed to support access to books, records and information of the service provider about the performance of outsourced activities. This may include the requirement that regulated entities include in outsourcing arrangements contractual provisions that provide the regulated entity with access to, and a right of inspection of, the service provider's books and records dealing with outsourced activities, and similar access to the books and records of any subcontractor, as well as contractual provisions by which the service provider is required to make books, records and other information about outsourced activities by the service provider available to the regulator upon request.

IX. Regulators should be aware of the potential risks posed where the outsourced activities of multiple regulated entities are concentrated within a limited number of service providers.

When a limited number of outsourcing service providers (sometimes just one) provide outsourcing services to multiple regulated entities, operational risks are correspondingly concentrated, and may pose a systemic threat. Alternatively, if multiple third party outsourcing service providers depend upon the same provider of business continuity services (*eg*, a common disaster recovery site), a disruption that affects a large number of those entities may result in a lack of capacity for the business continuity services.

Accepting that some form of concentration risk is inevitable as firms use outsourcing to search for improved efficiency and economies of scale, when assessing and monitoring the outsourcing policy and risk management program of a regulated entity, regulators should pay special attention to the way in which the regulated entity takes account of the potential risk posed by concentration.

Whilst concentration risks may exist, there are mitigating tools available to address the potential systemic risk of concentration. These include, primarily, adequate contingency

planning within regulated entities (see principle VI) as well as other supervisory mitigating tools such as ongoing monitoring and awareness programmes, adapting supervisory programmes, risk assessments and other actions.

Annex: A Case studies

Case Study 1: German Loan Factory
In Germany, an increasing number of credit institutions outsource loan handling to specialised, unregulated service providers, called "loan factories". These service providers specialise in back-office-services concerning loans, and mortgages, and in some cases deciding whether to grant a loan. In 2003 a credit institution wanted to outsource not only the servicing of loans, but also the decision to grant a loan in standard retail-lending-business and in the non-standard-business up to € 2.5m. The result of the assessment by the supervisor was that in the non-standard-business the credit institution was unable to monitor and oversee the loans granted by the loan factory. Though the business is run by the credit institution, which bears the risk emerging from it, the decision on granting the loans had been made by the service provider. Issues which emerged as part of this scenario included: • The outsourcing of decisions concerning the incurrence of new exposure is permissible only if it does not impair the management's ability to manage risks adequately. • This aforementioned would only be met if the regulated entity stringently committed the service provider to apply precise and verifiable evaluation and assessment criteria. With the systems currently used by the financial industry, this is only possible in the standardised retail lending business.

Case Study 2: Australian regulator investigates bank outsourcing
Australian banks have outsourced activities including information technology, credit card services, procurement, cheque and other electronic clearing services, mortgage processing and payroll amongst others. This raises questions about privacy of customer information, the financial and reputational risks to the banks if a service provider experiences problems or cannot go on providing. In January 2002, the Australian Prudential Regulation Authority (APRA) completed a targeted review of bank outsourcing, and introduced detailed prudential standards from 1 July 2002. APRA found that outsourcing arrangements were managed in a number of ways. Larger institutions generally had a dedicated outsourcing unit responsible for ensuring the institution's outsourcing policy is applied consistently. However, a number of institutions delegated responsibility for outsourcing to business units. In these cases, there was no guarantee that risks would be appropriately identified and assessed, and there was no central point for monitoring outsourcing arrangements. Fewer than one-third of institutions surveyed had a formal policy on outsourcing. In most cases banks were able to articulate the types of activities that could be outsourced or the reasons for outsourcing a activity but this had not been formalised.

Case Study 3: Outsourcing Unit Pricing for Managed Funds

In 1999, a major Australian institution outsourced its unit pricing and custody arrangements to a custodian which was part of the overall group. The custodian was eventually sold to another party but the outsourcing arrangement remained in place.

In January 2004 it was discovered that tax credits had not been claimed for the relevant funds over a number of years and that unit prices had been underestimated as a result. When the problem was discovered, the institution had to set compensate investors, costing approximately AUD$90 million, and and the regulators instructed the institution to carry out an overall review of its systems and processes to ensure that the problem does not recur.

Key issues which emerged included:

- There were insufficient controls and checking mechanisms between the third party provider and the institution.
- The institution was concerned about its ability to easily change processes at the third party provider as the service level agreements had been negotiated when it was part of the group.
- The organisation was taking a significant reputational risk by outsourcing such a activity to a third party provider.

Case study 4: OCC action against a bank and service provider

In 2002, the Office of the Comptroller of the Currency (OCC) in the USA took enforcement action against a Californian bank and a third party service provider to the bank. The service provider originated, serviced, and collected certain loans booked by the bank in 18 states and the District of Columbia.

Among other things, The service provider failed to safeguard customer loan files. The files, which represented loans carried on the books of the bank, were discarded in a trash dumpster in 2002. The OCC alleged that the improper disposal of loan files resulted in violations of laws and regulations.

The OCC also determined that the service provider committed unsafe and unsound practices that included a pattern of following the policies and procedures of the bank and a pattern of mismanagement of the bank's loan files. This case demonstrated the risks national banks expose themselves to when they rent out their charters to third-party vendors and fail to exercise sound oversight.

In the case of the bank, the OCC found that it failed to manage its relationship with the service provider in a safe and sound manner. In addition to violating the Equal Credit Opportunity Act and the Truth in Lending Act, the bank violated safety and soundness standards and also violated the privacy protections of the Gramm-Leach-Bliley Act, which sets standards for safeguarding and maintaining the confidentiality of customer information.

These violations and unsafe and unsound practices led to a cease and desist order against the bank. The order required the bank in civil money penalties and to terminate its relationship with the service provider.

The service provider also paid a sum in penalties and was ordered to not enter into any agreement to provide services to a national bank or its subsidiaries without the approval of the OCC.

To protect the privacy rights of consumers, the order also required the bank to notify all applicants whose loan files were lost. This notification must advise the consumer of any steps they may take to address potential identity theft.

Case Study 5: Joint examinations of third party service providers in the US

Under the Bank Service Company Act (Act) U. S. Federal Banking Agencies comprising the Federal Regulated Institutions Examination Council (FFIEC)[7] have authority to examine banks' third party service providers. The Act provides that a bank service company (definition includes a Technology Service Provider or TSP) is subject to examination and regulation by the regulator of the bank that is receiving the services. In addition, some FFIEC agencies have taken enforcement actions against TSPs. Following is an example of how the FFIEC agencies have chosen to apply the Act to bank service providers.

A service provider is considered for joint examination if it processes mission-critical applications for a large number of regulated entities that are regulated by more than one agency, thereby posing a high degree of systemic risk; or if the provider processes work from a number of data centres located in different geographic regions. The agencies coordinate on the scope, timing, and staffing of these examinations and the resulting examination report is shared with all the member agencies, the examined service provider and its client regulated entities. The FFIEC agencies use a comprehensive and uniform rating system (referred to as URSIT – Uniform Rating System for Information Technology) to assess and rate IT-related risks of the regulated entities and TSPs. The frequency of IT examinations typically varies between 18 and 36 months based on the risk profile of the TSP. National and regional programs currently track approximately 160 service providers, and, based upon risk assessments conducted by FFIEC examiners, 130 are examined on a regular basis.

During 2003, the FFIEC member agencies participated jointly in targeted IT examinations of the U.S. regional offices of a global technology service provider. The scope of the risk-focused examinations included activities, transaction processing services, clearing and settlement, information security, business continuity planning, and the URSIT components (management, audit, development and acquisition, and support and delivery). In each case, examination findings were published as joint examination reports using the FFIEC's uniform report of examination format for IT examinations at TSPs. The examinations also included limited scope reviews of support activities where the support functions were domiciled outside of the entity's regional primary service centres.

It should be noted that international supervisors have requested access to examination reports on TSPs which provide services to regulated entities in other countries. The issue of sharing reports of examinations resulting from the MDPS program with international supervisors remains under consideration.

[7] The FFIEC includes the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Association, the Office of Thrift Supervision, and the Office of the Comptroller of the Currency.