THE POWER OF BEING UNDERSTOOD

RSM

Estefani

One of the
RSM team

White Paper - Outsourcing and Third-party Risk Management

White Paper

Outsourcing And Third-Party Risk Management

For Circulation
16 November 2024

1.0. Introduction

The purpose of the paper is to understand the meaning of outsourcing, the emergence of outsourcing, its key drivers and benefits. It also examines the management of the risks associated with outsourcing by organisations and service providers. The paper also examines key regulatory requirements for outsourced businesses in India. It covers both local as well as overseas outsourcing - often known as offshoring, including captives set up by organisations at offshore locations. The scope of the paper is restricted to Information Technology (IT) and Business Process (BP) outsourcing.

2.0. What is Outsourcing?

The term outsourcing is derived from the words outside resourcing. It can be defined as practice of hiring service providers to perform tasks, activities or processes that would ordinarily be performed within the organisation. This could include enlisting the services of third-party service providers as well as affiliates or subsidiaries of the outsourcing entity. Organisations that outsource to affiliates or subsidiaries maintain an arm's length relationship them on par with third party service providers. Most large organisations commenced their outsourcing journey to focus on core activities, to increase efficiencies and save on overheads and infrastructure. IT services outsourcing means transferring of key IT tasks including application/program development and maintenance, technical support, IT infrastructure including data centres and cloud storage to service providers. Gartner defines IT outsourcing as the use of external service providers to effectively deliver IT-enabled business process, application service and infrastructure solutions for business outcomes. Business process outsourcing means the contracting of business functions or activities and processes including data entry and transcription, accounting, back office and data analysis to service providers.

3.0. Background and emergence of IT and BP Outsourcing:

While outsourcing had been in existence since the early 20th century, it gained momentum around the 1980s when the US manufacturing giants used overseas service providers. Outsourcing in IT activities started since the 1960s, with Electronic Data Systems (EDS) founded by Ross Perot, being amongst the early movers, providing IT facilities management services to US based businesses.

In the late 1980s, IBM set up an outsourced data centre for Japanese giants Kodak. Indian firms commenced their journey as IT services providers in the late 1960s and the 1970s, but the sector witnessed an accelerated growth in the late 1980s and the 1990s. IT organisations in India established themselves as reliable IT partners to overseas and Indian clients. On the business process outsourcing side, a few multinational banks and airlines were amongst the early movers who set up captives in India to support local and international businesses in the 1990s. India, Philippines, China, Mexico, Brazil and Malaysia feature amongst the topmost outsourcing destinations in the world. India's

emergence as an IT and Business Process powerhouse is due to the existence of a large talent pool of highly skilled banking, IT, finance, accounting and marketing professionals with strong English-speaking skills. This was complemented by supportive Government policies providing infrastructure, tax and other incentives which continue till this day. These included exemptions and incentives under Sections 10A, 10B and 80 HHE of the Income Tax Act, creation of technology parks and special economic zones under the STPI and SEZ Regulations, respectively and state level incentives including stamp duty waivers and support in capital and operating expenditures. Moreover, the National Association of Software and Service Companies (NASSCOM) established in 1988, which is a non-governmental organisation serves as an advocacy group that promotes the growth of the IT and BP outsourcing sector and provides a platform for networking between members.

4.0. Types of Business Process Outsourcing:

The broad categories of business process outsourcing, based on the nature of services provided has been set out below.

4.1. **Back Office Processing:** This category of outsourcing covers a wide range of activities including basic data entry activities, invoicing, bank reconciliations, claims processing, cash management & funds transfers, trade services, trade processing and payroll processing. This is the most prevalent form of business process outsourcing across industries like manufacturing, banking and financial services and pharmaceuticals.

4.2. **Finance & Accounting (F&A):** F&A outsourcing includes activities related to day-to-day accounting, ledger and bank reconciliations, financial reporting, accounts payable and receivable and preparation and submission of tax returns and filings. F&A outsourcing is prevalent across the financial services industry as well as the manufacturing sector. F&A outsourcing is concentrated in locations which have an existence of a talent pool of accounting professionals.

4.3. **Knowledge Process Outsourcing:** Knowledge Process Outsourcing or KPO refers to outsourcing knowledge-based tasks and activities, to qualified subject matter experts. This type of outsourcing requires a high degree of research, technical and analytical skills. Some of the most common KPO offerings include Equity Research in the Banking and Financial services space, Market Research, Data Analytics and Research and Development across industry verticals and legal and medical advisory services.

4.4. **Customer Services Outsourcing:** It would include handling customer interactions on behalf of organisations including customer complaints or product related queries, which may be received through emails or through telephone calls.

4.5. **Outbound Collections and Sales Services:** These include firms that provide outbound call services for collections of overdue debts on loans and cards. Outbound call centres also make sales calls on behalf of organisations and service calls for existing customers.

5.0. Types of IT Outsourcing:

5.1. **Application Development and Maintenance:** This includes services provided at local or offshore development centres by third party IT developers or dedicated offshore/ nearshore development centres set up by affiliate entities of the outsourcing organisations.

5.2. **Technical support:** Organisations also outsource technical support or helpdesks functions which provide services to users facing issues in their computing environment as well as in application usage.

5.3. **Testing Services:** Outsourcing organisations also rely on service providers to support them with software testing services. Testing services include loading, stress or performance testing and user acceptance testing. This could be provided at offshore, onshore or nearshore centres.

5.4. **Data centres:** Organisations may resort to outsourcing data centre activities including management of operating servers, host platforms and data storage either partially or wholly. This is aligned to the organisation's distributed data processing or business continuity planning strategy. IBM was one of the pioneers in this form of IT outsourcing and set up one of the first data centres for Kodak in 1989.

5.5. **Cloud storage:** Increasingly, firms are using the services of third-party service providers to transfer and save data at offsite locations in logical pools or clouds. Data can be retrieved through the public internet or a dedicated private network. The storage and security of the data is the responsibility of the service provider.

6.0. Rationale for Outsourcing:

Organisations outsource for varied reasons including cost savings, rationalisation, better turnaround times and focus on key business functions. The key drivers for outsourcing are briefly explained below:

6.1. **Cost Savings:** The initial push for outsourcing to overseas and local low-cost destinations came from cost savings due to labour arbitrage. The business case for continued and sustained outsourcing is driven by other factors described below.

6.2. **Focus on Core Business Activities:** As the practice of outsourcing gained vintage, organisations discovered the merits of focusing on implementation of core business activities, leaving the repetitive tasks as well as specialized functions to outsourced entities.

6.3. **Innovations and Process Improvements:** As the outsourcing practice evolved**,** service providers realised that enhanced performance in a competitive environment could be delivered through innovation and process improvements. The approach added greater value to the outsourcing firm's business than mere cost savings.

6.4. **Business Continuity & Resilience:** Outsourcing aids in business continuity planning by spreading delivery locations within the country and in other geographies, to provide the customer uninterrupted

services. This is especially relevant in times of localised infrastructure disruptions and or geo-political disturbances.

6.5. **Distributed Processing:** Building a network of outsourced partners in different geographies enables an organisation to provide a 24x7 customer support. Through planned work allocation amongst regions and effective queue management, it enables the organisation to maintain and enhance customer delivery.

6.6. **Savings in infrastructure and technology:** Outsourcing organisations experience saves on investments and running costs of infrastructure, as the responsible service providers build the requisite infrastructure for execution.

6.7. **Access to Subject Matter Experts / Talent Pool:** Resource pools with required skill sets maybe concentrated in certain areas or with service providers which the outsourcing organisation can benefit from. This may individually or in combination with any of the above areas, make a compelling case for outsourcing.

6.8. **Scalability:** Organisations can reap the benefits of scalability in an outsourced scenario, as they are not burdened with the tasks of redeployment and adjustment of staff and facilities due to changes in business conditions. These can be effectively managed by service providers.

7.0. Key Risks in Outsourcing and Third-Party Management:

The benefits of outsourcing enumerated above, should be evaluated with the associated inherent risks and challenges. The key risks in outsourcing with relevant risk incidents have been explained below.

7.1. **Cyber/information security Risk:** In today's digital world, organisations are susceptible to a range of vulnerabilities or threats include malware attacks, direct-access attacks, denial of service and eavesdropping. In the context of the customer data, process information and critical processes that service providers handle, this presents a significant risk. In April 2011, hackers infiltrated the network of a leading multinational corporation. This placed confidential information of customers including names, addresses, and potentially credit card details at risk.

7.2. **Data Confidentiality Risk:** Service providers have access to customers' confidential data which is susceptible to misuse and leakage. Not all service providers have access to sophisticated systems or enhanced controls to detect and prevent data leakages. In 2020, a US regulator fined a leading multinational bank and wealth manager, USD60 million for data leakages arising out of a failure to oversee decommissioning of a data centres and destruction of records by a vendor.

7.3. **Process Disruption & Outages:** Outsourcing could result in disruption of processes in the initial stages especially where part of the processes are still retained by the outsourcer. Similarly, processes could suffer from outages due to disruptions at the service provider's end.

7.4. **Regulatory Risk:** Data protection regulations in most jurisdictions especially in the context of outsourcing are stringent and non-compliances arising therefrom may result in fines and penalties.

Service providers need to be conversant with the regulatory requirements in different geographies. For e.g. EU and GDPR regulations require anonymising of data while processing, firms and individuals require licences in certain jurisdictions in the US to contact customers for debt collections.

7.5. **Geopolitical Risk:** Prior to outsourcing, organisations need to evaluate the political situation, labour laws, other socio-economic policies of the proposed outsourcing destination and the overall regional stability. This is imperative to ensure seamless transition of activities to the outsourced destination and continued support therefrom.

7.6. **Service Quality Risk:** Outsourcing of activities to a service provider may result in deterioration of service quality and delivery resulting in an impact to the end customer. Outsourcers and service providers may address this through a combination of training programs and close monitoring in the initial phases of delivery.

7.7. **Concentration Risk:** Where operations/ processes of an organisation are wholly supported by one service provider, any disruption or deterioration in performance at the service provider's end may significantly impact the business. Moreover, excessive dependence on one or more service providers for a particular function would result in diminution of domain expertise within the outsourcing organisation.

7.8. **Fraud Risk:** Like all other businesses outsourced businesses are susceptible to fraud risk particularly in view of the sensitive and confidential nature of client information being handled.

The above risks may impact the reputation or franchise risk of the outsourcing organisation, unless effectively mitigated. These risks are inherent to the process and the organisations and service providers alike, devise appropriate strategies to effectively counter and minimise these risks.

8.0. Managing Outsourcing or Third-Party Risk:

Organisations manage these key risks through a combination of preventive and detective controls and other measures. These are embedded through strong governance frameworks including vendor oversight, risk management practices, audits and contractual obligations, which are discussed below.

8.1. **Initial and Periodic Assessments:** Prior to appointing a service provider, organisations perform due diligence on various aspects including the capability of the service provider, previous experience in supporting outsourcing arrangements, financial position and market reputation. In doing so, organisations perform reference checks with existing clients of the service providers. Organisations have established procedures to evaluate service provider performance on a periodic basis to support decisions on renewal or discontinuance of services.

8.2. **Management Oversight:** Organisations design frameworks which build in outsourcer's oversight at different levels of management. This would include the more frequent metrics management reviews to the senior level governance forums wherein critical aspects of overall delivery management, key risk indicators and outstanding issues identified in audits and self-assessments are reviewed. More

matured organisations may have governance forums focussed on risk management including emerging risks.

8.3. **Contractual Framework:** Organisations and their service providers enter into service agreements that define the overall framework including the expected service levels, defect calculations, the liabilities arising out of service delivery and pricing. Outsourcing organisations and service providers enter into Data Protection Agreements (DPAs) which define the framework for processing, storage, safeguarding and retrieval of data and penalties for data breaches. Non-disclosure clauses may be built into the agreement or Non-Disclosure Agreements (NDAs) may be signed off separately.

8.4. **Data Security Controls:** In view of the customer data privacy regulations and concerns, service providers are granted access to outsourcer's systems and environment through Cloud Desktops and Virtual Private Networks **(**VPN). Organisations may also disable service provider's ability to send emails outside their networks and may mandate encryption of data sent via emails, masking of data customer, restricted usage of mobile phones, pens and writing pads on the shopfloor. At the service provider's facilities, processing/development centres for clients are segregated and controlled to prevent unauthorised access.

8.5. **Training:** Organisations carry out extensive training programs prior to outsourcing and supplement them with periodic refresher trainings. In addition to trainings on the applicable regulations, organisations mandate trainings on key aspects of process and risk management including quality framework, fraud management, data security and confidentiality.

8.6. **Roles and Responsibilities definition:** In addition to the contractual agreements prior to outsourcing, the operating procedures, the parties to the contract also sign off a document that articulates the tasks to be performed by the outsourcing firm and the service providers and the dependencies on execution. This avoids ambiguity in delivery execution and in assigning responsibility for quality management.

8.7. **Risk Management frameworks:** Outsourcing firms and service providers may define a risk management framework including risk definition, assessments, root cause analysis, periodic audits and quality reviews. More tenured and larger players in the outsourcing industry, have their own risk management frameworks aligned to the best-in-class practices, which act as a key differentiator in the competitive industry. Service providers also obtain certifications ISO 22301:2019 on business continuity planning and ISO ISO/IEC 27001:2022 on information security management systems and cybersecurity.

8.8. **Strong BCP strategy:** Organisations mandate service providers to perform BCP testing at pre-defined frequencies and in line with the organisation's policies. In addition to planned testing of BCP at predefined frequencies, organisations also initiate unplanned testing with limited notice, to test the readiness of service providers in real life scenarios.

8.9. **Periodic audits:** Organisations exercise the right to perform risk focussed process and information security audits including SOC 1 and 2 on service providers. In case of larger service provider

organisations with established risk management frameworks, the outsourcer may choose to place reliance on in-house audit teams, based on a mutually agreed pre-defined audit scope.

While outsourcing organisations and service providers proactively put in place these measures, the regulators further reinforce most of these aspects including due diligence, senior management oversight, business continuity planning, confidentiality and right to audit through outsourcing guidelines and regulations. Regulators generally impose restrictions on outsourcing of certain key activities or services including Compliance, KYC/AML, Investment and strategic functions.

9.0. Key Regulations relevant to outsourcing in India:

The key provisions and requirements of a regulations relevant to outsourcing in a few sectors in India have been summarised in the table below:

Key Provisions	**RBI Master Direction - Non-Banking Financial Company,2016 Annex XIX Directions on Managing Risks and Code of Conduct in Outsourcing of Financial Services by NBFCs**	**RBI Master Direction on Outsourcing of Information Technology Services**	**IRDAI (Outsourcing of Activities by Indian Insurers) Regulations, 2017**	**Guidelines on Outsourcing of Activities by Intermediaries**
Prohibited activities	Annexure XIX (2)	-	Regulation 5	Guideline 5
Outsourcing Policy	Annexure XIX (5.1)	Direction 9	Regulations 7 i (a) & (e) & 8 (i), (v) &(ix)	Principle 2
Board & Senior Management Responsibility and Oversight	Annexure XIX (5.2.1 &5.2.2)	Directions 10 & 11	Regulations 7 and 8	Principles 1 and 1.2
Due Diligence on Service Providers	Annexure XIX (5.4)	Directions 6, 14	Regulation 10	Principle 4
Agreement - Contents	Annexure XIX (5.5)	Directions 15 & 16	Regulation 11	Principle 3

Confidentiality	Annexure XIX (5.6)	Appendix I (6)	Regulation 12	Principle 7
Business Continuity/ Disaster Recovery	Annexure XIX (5.8)	Direction 18 Appendix I (7)	Regulation 16	Principle 6
Monitoring and Governance	Annexure XIX (5.9)	Direction 19	Regulation 10	Principle 2
Right to audit	Annexure XIX (5.9)	Appendix I (9), Direction 19	Regulation 13	Principle 2.4

Additionally, service providers in India would be subject to outsourcing guidelines and regulations prevalent at the outsourcers' locations. The Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation in US published a guidance for banks on managing risks associated with third-party relationships. It offered views on various aspects related third party risk management including the entire lifecycle from planning, the due diligence checks, contract management, contingency, ongoing monitoring and termination of the service providers. The Prudential Regulation Authority's (PRA), Monetary Authority of Singapore (MAS), Hong Kong Monetary Authority (HKMA) Regulators and Australian Prudential Regulatory Authority (APRA) regulations and guidance on outsourcing, set out expectations on materiality of outsourcing, the due diligence in the selection of the service provider, governance, risk assessment, data security and the right to audit amongst others. Similarly, the EU General Data Protection imposes responsibilities on the outsourcer and the service provider to ensure confidentiality of data, pseudonymisation and encryption of personal data while processing, ensuring the security of the data processed, data recovery and resilience. The GDPR mandates signing of DPAs between outsourcing organisations in EU and service providers including captives and third-party service providers located within and outside EU.

10.0. Conclusion:

As outsourcing continues to be a vital part of business strategy, organisations need to evaluate existing and emerging risks in a dynamic environment and devise appropriate measures to address these. Additionally, organisations need to bring in innovative measures of process improvements including automation, to continuously enhance process delivery.

For further information please contact:

RSM Astute Consulting Pvt. Ltd.

8th Floor, Bakhtawar, 229, Nariman Point, Mumbai - 400021.

T: (91-22) 6108 5555/ 6121 4444
F: (91-22) 6108 5556/ 2287 5771

E: emails@rsmindia.in

W: www.rsmindia.in

Offices: Mumbai, New Delhi - NCR, Chennai, Kolkata, Bengaluru, Navi Mumbai Surat, Hyderabad, Ahmedabad, Pune, Gandhidham, Jaipur and Vijayanagar

facebook.com/RSMinIndia

twitter.com/RSM_India

linkedin.com/company/rsm-india

Youtube.com/c/RSMIndia

16th November 2024