COVID-19 PANDEMIC: OUTSOURCING ARRANGEMENTS REINVENTED

LC Lawyers
林朱律師事務所
Law firm member of the EY global network

26 June 2020 | **Kareena Teh**, **Catherine Wong**

In considering outsourcing and/or changing outsourcing arrangements, it is important for organisations to bear in mind two key issues

The trading landscape for markets and firms has changed considerably over the last decade. Regulatory reforms, technology developments, increased connectivity between market participants, and increased levels of electronic trading and process automation have heightened the complexity of markets and increased focus on operational efficiency. These developments have incentivized firms to outsource certain tasks to service providers, due to the benefits it offers, including reducing operating costs and overheads, as well as improving focus and service quality. In 2019, the global market size of outsourced services amounted to US$92.5 billion.[1]

However, COVID-19 crisis has revealed some challenges in outsourcing arrangements, particularly including those involving offshore outsourcing service providers (**OSPs**). Most of these weaknesses arose due to the movement control orders that were implemented to curb the spread of the pandemic. Take, for example, in India, which was ranked as the most attractive country to offshore business services to in 2019,[2] the Indian Government on 24 March 2020 imposed a compulsory lockdown to restrict commerce and travel across the nation, and such lockdown has been extended to 30 June 2020.[3] Despite announcement of certain relaxations outside of the COVID-19 containment zones, during the original lockdown period, only businesses providing "essential services" were permitted to operate. Some states specifically expanded their list of exempted industries to include data centers.[4] On 15 April 2020, the Indian Government allowed IT establishments (whether providing "essential services" or not) to operate, subject to the limitation of only 50% capacity.[5] Some OSPs also had problems implementing remote working arrangements that became necessary, including in getting laptops

1 https://www.statista.com/statistics/189788/global-outsourcing-market-size/

2 https://www.statista.com/statistics/329766/leading-countries-in-offshore-business-services-worldwide/

3 https://economictimes.indiatimes.com/news/economy/indicators/lockdown-extension-to-have-deep-impact-on-indian-economy-report/articleshow/76132363.cms

4 https://economictimes.indiatimes.com/news/company/corporate-trends/worlds-back-office-scrambles-to-stay-online-as-india-locks-down/articleshow/74781330.cms?from=mdr

5 https://www.mha.gov.in/sites/default/files/MHA%20order%20dt%2015.04.2020%2C%20with%20Revised%20Consolidated%20Guidelines_compressed%20%283%29.pdf

to service provider personnel, setting up virtual private network access, ensuring WiFi availability, and providing the requisite security software applications.

These difficulties have resulted in many OSPs struggling to operate fully, if at all. Concerns have also arisen as to whether the remote working systems used by the OSPs (most of which have neither been tested nor specifically designed for the disruption arising from the pandemic) can securely handle confidential data and maintain the integrity and availability of their services. As a result, some organizations have started to bring their outsourced operations back in-house and/or find alternative service providers which are less affected by the pandemic at short notice.

Some conflicts have also arisen because of this, with:

- OSPs which were unable to perform their services seeking to delay the performance of their contractual obligations and/or avoid liability for non-performance.
- Organizations seeking to replace their existing OSPs with alternative service providers which are less affected by the pandemic and whose services are more reliable.
- Organizations affected by the economic downturn seeking to cut costs and terminate their outsourcing contracts prematurely to cut costs.

Nonetheless, it is anticipated that the outsourcing trend will continue, with more and more organizations turning to outsourcing, including of core or supporting functions such as accounting, finance, human resources administration, legal, marketing, payroll and tax. For finance and tax, 73% of the respondents to the EY 2020 Tax and Finance Operate survey said they are more likely than not to co-source some critical activities in the next 24 months in order to add value, reduce risk and decrease cost.[6]

In considering outsourcing and/or changing outsourcing arrangements, it is important for organisations to bear in mind two key issues:

1. Whether there are laws and/or regulations governing outsourcing; and
2. Whether the third-party service provider has the requisite expertise and experience and business continuity capability to support the outsourcing.

As a guide to issues and risks to watch out for, we summarize below Hong Kong's regulatory regime for outsourcing and conclude with some recommendations for proactively managing these issues and risks.

Regulatory regime for outsourcing in Hong Kong

There are no laws which specifically govern or regulate outsourcing activities in Hong Kong. However, certain government and regulatory authorities have published industry-specific regulations and guidelines for outsourcing activities. To name a few examples:[7]

[6] https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/tax/ey-tax-and-finance-operate-survey-2020.pdf

[7] https://uk.practicallaw.thomsonreuters.com/0-576-6247?transitionType=Default&contextData=(sc.Default)

- The Securities and Futures Commission (**SFC**) has not created its own set of guidelines or principles to regulate outsourcing activities of SFC-licensed entities but has endorsed the Principles on Outsourcing of Financial Services for Market Intermediaries (**IOSCO Principles**) published by the International Organization of Securities Commissions (the **IOSCO**). The IOSCO Principles are intended to provide a framework to guide regulated entities through the steps that should be taken when outsourcing activities.

  Recently in May 2020, the IOSCO issued a media release requesting feedback on proposed updates to its principles for regulated entities that outsource tasks to service providers.[8] Such consultation report was published, as the outbreak of COVID-19 has highlighted the need to ensure resilience in operational activities, and to maintain business continuity in situations where both external and often unforeseen shocks impact both firms and their service providers. The revised principles comprise a set of fundamental precepts and a set of seven principles, each being supplemented with guidance for implementation, covering the following areas:

  - Due diligence in the selection and monitoring of a service provider;
  - The contract with a service provider;
  - Information security, business resilience, continuity and disaster recovery;
  - Confidentiality issues;
  - Concentration of outsourcing arrangements;
  - Access to data, premises, personnel and associated rights of inspection; and
  - Termination of outsourcing arrangements.

- The Insurance Authority publishes guidance for insurers, including the Guidance Note on Outsourcing (Insurance Guidance Note)[9] and the Guideline on Outsourcing[10] which provide guidance for a list of essential issues that an authorised insurer needs to attend to when outsourcing its services.

- The Hong Kong Monetary Authority (**HKMA**)'s Supervisory Policy Manual includes a chapter on outsourcing (SA-2), which is a non-statutory guideline setting out HKMA's supervisory approach to outsourcing and the major points which the HKMA expects authorised institutions to address when outsourcing their activities.[11] In addition, it includes a chapter on general principles for technology risk management (TM-G-1) setting out non-statutory guidelines regarding the technology-related risk controls that authorised institutions are expected to consider.

- According to the Seventh Schedule of the Banking Ordinance (Cap 155), authorised institutions must consider their legal obligations to meet the minimum authorization criteria when considering their outsourcing plans. These obligations include having adequate accounting systems and systems of control and conducting business with the interest of depositors and potential depositors

[8] https://www.iosco.org/news/pdf/IOSCONEWS567.pdf

[9] https://www.ia.org.hk/en/legislative_framework/circulars/reg_matters/files/gn14.pdf

[10] https://www.ia.org.hk/en/legislative_framework/files/GL14.pdf

[11] www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/SA-2.pdf

in mind. Authorised institutions are advised to discuss their outsourcing plans with the HKMA in advance to ensure that their internal control systems or business conduct will not be compromised or weakened after the activity has been outsourced, and that certain major issues are addressed before the outsourcing plans are implemented.

The outsourcing of information technology and cloud services is also not regulated by any specific statute under Hong Kong law. However, the Office of the Privacy Commissioner for Personal Data issued guidance regarding cloud computing to advise organizations on the factors they should consider when considering engaging cloud computing. The guidance mainly refers to the Personal Data (Privacy) Ordinance (Cap 486) and highlights the importance for a data user to fully assess the benefits and risks of engaging cloud computing and understand the implications for safeguarding personal data privacy.[12]

There are also no general laws or regulations that govern the outsourcing of telecommunications services. However, providers of telecommunications services licensed under the Telecommunications Ordinance (Cap 106) are required to ensure that outsourced activities comply with applicable laws, including personal data privacy laws.

In relation to the public sector, the Efficiency Unit of the Hong Kong Government has issued a General Guide to Outsourcing which sets out the steps that private sector OSPs engaged by the government should consider at each phase of the outsourcing process so that they can better understand the procedures and practices followed by the government departments that they provide the outsourced services to.[13]

In sum, organizations in Hong Kong seeking to outsource and OSPs should ensure that they check for and are familiar with the regulations that apply to their outsourcing arrangements prior to entering into the same. If the outsourced services are to be performed outside Hong Kong, these checks must necessarily include the laws and regulations of the country or countries where the outsourcing services are to be performed.

Recommendations for businesses

Apart from ensuring compliance with laws, industry-specific regulations and guidelines for outsourcing activities, it is also important to proactively address compliance issues. Some key steps to take include:

- **Choosing the right OSPs.** It is important that organizations exercise due care, skill and diligence in the selection of service providers, including conducting suitable due diligence in selecting appropriate service providers and in monitoring their ongoing performance. Organizations should be satisfied that the service providers have the ability and capacity to provide the outsourced tasks effectively and have effective business continuity contingency plans.

[12] https://www.pcpd.org.hk/english/resources_centre/publications/files/IL_cloud_e.pdf

[13] http://www.eu.gov.hk/en/reference/publications/guide_to_outsourcing_200803.pdf

- **Entering into legally binding written contract with each service provider.** The level of detail of the written contract should reflect the level of monitoring, assessment, inspection and auditing required, as well as the size, complexity and the risks of the outsourced services involved. Contractual provisions underpin the relationship between organizations and OSPs and can reduce the risks of non-performance or aid the resolution of any disagreements.

- **Ensuring that applicable contractual terms and laws for determining parties' rights and obligations are included in the written contracts**:

  - Security and data protection provisions and regulations should be included, including compliance with key security policy obligations such as restrictions on the locations, personnel, and technologies used to access and process customer data. Security breaches and cyber incidents can have damaging effects to business reputation. Organizations should seek to ensure that service providers maintain appropriate IT security, cyber-resilience and disaster recovery capabilities.

  - There should also be provisions that prohibit the service providers and their agents or sub-contractors from intentional or inadvertent unauthorized disclosure to third parties. Unauthorized disclosure of clients' and/or organizations' confidential information could have a number of negative consequences, including harm to clients, damage to reputation, financial losses, and loss of or risk to proprietary information (including trade secrets).

  - Termination of the outsourcing arrangements should be specifically provided for to ensure proper and orderly transition of the outsourced activities. Such provisions should clearly identify the events of termination (e.g. in case of insolvency, change in ownership, failure to comply with regulatory requirements, poor performance, breach of confidentiality, vulnerability to cyber intrusions through the OSP etc.), and include appropriate exit strategies (e.g. a minimum period before a termination can take effect to allow an orderly transition and/or that OSPs have the obligation to assist and provide full support for a successful and complete transition).

  - Lastly, force majeure clauses and change of control/material adverse change clauses should be included to cater for circumstances like the ones being encountered presently due to the COVID-19 pandemic.

- **Maintaining a register of outsourcing arrangements**, noting those which are critical to operations. In the event of disruption, this will allow prompt identification and implementation of alternative arrangements necessary to maintain effective operations. For contractual compliance and/or regulatory oversight purposes, organizations should also take appropriate steps to ensure that they have prompt and ready access to the data, IT systems, premises and personnel of OSPs relating to the outsourced activities.

- **Reviewing business continuity policies**, including any recovery planning and resolution planning measures in the event of disruption, and assessing the risk

and exposure of existing and future outsourcing arrangements. Organizations should be aware of the risks posed and should be in a position to manage them effectively. Some factors that increase risks include outsourcing in multiple jurisdictions, dependence on a single OSP for material or critical outsourced tasks, and reliance on OSPs that outsource material or critical outsourcing services to multiple entities.

- **Keeping in close contact and working cooperatively and flexibly with OSPs.** Some of the issues confronting OSPs due to the COVID-19 pandemic may be temporary. Contact and/or call centers in particular, especially those that are offshore, which rely on large number of on-site personnel working on dedicated infrastructure, may be facing very significant challenges, when there is a surge in demand for technical support and services relating generally to remote working models. Short deadline extensions, amended milestones or waiver of rights and remedies (with or without appropriate price adjustments), and assistance in ensuring that the engaged OSPs have adequate technology to work on business matters may provide the necessary relief and avoid termination of the services and the associated time and costs in making alternative arrangements and/or resolving subsequent disputes.

KEY CONTACTS

Kareena Teh
Partner, LC Lawyers LLP
kareena.teh@eylaw.com.hk
+852 2629 3207

Catherine Wong
Associate, LC Lawyers LLP
catherine.ky.wong@eylaw.com.hk
+852 2675 2173

Contact us

LC Lawyers LLP *in Association with* Chen & Co. Law Firm
Suite 3106, 31/F, One Taikoo Place
979 King's Road, Quarry Bay
Hong Kong
Tel: +852 2629 3200
Fax: +852 2956 1980

https://www.eylaw.com.hk/en_hk

Follow us on WeChat