Delivering the Telco Deal Right: Practical Considerations for Suppliers Managing Compliance Risk

by Martin Hayward - m.hayward@tamimi.com - Dubai International Financial Centre

March 2019

Introduction

The rollout of big telecommunications infrastructure projects in the Middle East and Africa ('**MEA**') by international telecommunications suppliers subject to key internal compliance mandates, poses material, complex challenges for the suppliers.

As the MEA continues to experience heavy investment in telecommunications infrastructure, both in terrestrial and submarine cable systems, suppliers are increasingly seeking ways to take advantage of these opportunities whilst effectively managing their compliance risk.

The financial cost (both in fees, fines and penalties and, for listed suppliers, possible share price losses) caused by a compliance breach, along with the management time taken in managing a compliance breach and resulting investigation, follow-up remediation, additional controls and oversight, can have such a material adverse effect on a supplier that it can take years to recover from.

The brand and reputational damage can be even more damaging with the loss of key clients and potential blacklisting from lucrative government contracts. In addition to this, suppliers can face civil and criminal actions against its directors and officers (including shareholder actions).

This article looks at the key compliance issues and the practical mitigation strategies considered by suppliers as they evaluate MEA opportunities and then deliver the telecommunications infrastructure projects.

Due Diligence During the Bidding Stage

Central to telecommunications suppliers' evaluation of whether to bid or not is the potential compliance risk of delivering the project. These projects can cover multiple MEA countries, particularly if it is a submarine cable consortium project; countries often with very different compliance risk profiles. The projects can have multiple customers, often involving government owned or controlled companies, which only heightens the compliance risk.

Suppliers will often start with a high-level analysis drawing on resources like international risk indexes to identify high risk countries and using publicly available sources to highlight early in their decision-making process any key compliance issues that need to be factored in.

This data forms a key part of the decision-making matrix as the supplier determines whether to apply the resources to bid for a project which, depending on the type and size of the project, may last many months. Also, it will enable suppliers to add costs to their commercial offers upfront to cover the cost of compliance mitigation.

Identifying the Right Partners

Many deals will be in MEA countries where suppliers do not have an on-the-ground presence. As a result, suppliers face an added layer of compliance risk engaging with both sales partners, through which the supplier will sell, and/or service partners, through which the supplier will outsource all or part of the project delivery. Identifying the right partners is critical. Suppliers cannot avoid compliance risk by partnering; but they can mitigate their risk by identifying the right partners and ensuring that ‘adequate procedures’ are in place to ensure ethical and robust procedures are implemented.

Depending on their assessment of compliance risk, suppliers will conduct enhanced due diligence on all or part of the partner supply chain, identifying and evaluating all partners, including, in many cases, any contractors sub-contracted by one of the partners to deliver a particular element of the project.

Full details of each partner will be collected through compliance questionnaires, verifying their corporate identity. Government affiliations will be analysed. Key shareholders, officers, directors and employees at each level of the partner supply chain will be identified and screened against the relevant denied party watchlists.

Partners will be expected to sign undertakings confirming their compliance with compliance laws and the supplier’s compliance policies and procedures as well as to undertake not to place the supplier in breach of any such laws, policies or procedures. Similar undertakings will be included in the supplier’s contract with the partners who will indemnify the supplier against the cost of a compliance issue (not only in terms of potential fines and penalties but also internal costs). Partners will be contractually obliged to flow these terms down to their subcontractors and to undertake similar due diligence.

Partners will be evaluated based on their internal compliance programmes and the level of executive awareness and (active) sponsorship of the internal compliance programme within the partner. Partner policies and procedures will be reviewed along with how effective their responsive processes are in the event of a regulatory breach. Their compliance training will be reviewed from a frequency and content perspective. Partners may undergo specific tailored compliance training delivered by the supplier’s legal or compliance teams or outsourced to compliance professionals (often with a focus on key practical issues to enable the partner to identify and avoid situations that may increase compliance risks).

Training will cover the supplier’s compliance policies and procedures so partners have a clear understanding of the internal rules governing the supplier. Scenarios will be role played to prepare partner personnel for dealing with key compliance challenges that may arise as part of the project (e.g. how to recognise and avert unethical business practices). The supplier’s own personnel on the ground during the delivery stage will receive similar training. More on this below.

Post Award, Prior to Delivery

Key risk countries identified during the due diligence process will be subject to detailed assessment to identify the key compliance risks relating to importing, storing, transporting and delivering telecommunications equipment to partner warehouses, staging sites and/or the customer sites and moving personnel in and out of the country as part of the project delivery.

Entering the Country

The first key challenge to overcome is importing equipment and bringing personnel into MEA

countries where the project is to be delivered.

Depending on the size of the shipments, one of the country's airports will likely be the importation point. Suppliers will analyse, often with the help of their logistics teams and forensic investigation experts, the level of risk at the chosen point of entry.

The first question will be whether there is a choice of airport. This is key. Suppliers may wish to choose an airport closest to their final destination for the speed of delivery. This may not be the best port of entry for the reasons summarised below.

Importation is normally handled by third party logistics/customs clearance agents. Suppliers need to have properly assessed these partners, carrying out the due diligence set out above. Suppliers will often choose international logistics providers with established compliance policies and procedures, and who are also subject to international extraterritorial laws governing business integrity, rather than local logistics agents.

The systems that suppliers will need to navigate as part of the customs clearance process need to be carefully researched. Is it electronic or manual and paper based? Can documentation be uploaded in advance to speed up the process? A complete set of the right paperwork avoids delays and potential compliance situations. Also, knowledge of how long the process normally takes, the steps involved, if it is a particularly difficult or complex process (and if so what aspects (e.g. do certain products require technical inspections; regulatory approval, etc.?)), if there are fast track or VIP services that can be used (and the cost) are all important considerations.

A clear understanding of the customs fees in each country is important. How much should the supplier be paying? Are the fees officially published? Are there any hidden fees or charges? Checks need to be put in place to ensure that this is confirmed and that there are no hidden or unusual fees or payments that could be interpreted as bribes or facilitation payments. Are there any deposits or down payments that need to be made? Are they legitimate and how difficult will it be to get these payments back? All these points need to be assessed. To the extent that any such payments can be made, online in advance through official portals, this should be done to limit any financial exchanges.

Suppliers will likely be subject to customer timelines (often with heavy penalties attached). Delays on entry, of both products and personnel, need to be managed properly to avoid the penalties that suppliers can incur. This needs to be balanced, though, against managing the compliance process correctly.

Personnel from particular countries may enter countries with greater ease and less bureaucracy. The more bureaucracy, the greater the potential compliance risk and delay to the project. Personnel need to make sure their documentation is in order (e.g. passports with over six months' validity; e-visas secured if possible beforehand; entry paperwork filled in on the plane over, etc.). Suppliers should, to the extent possible, carefully choose the personnel they send into certain countries to limit the bureaucracy. They should ensure their partners do the same. In addition, any intelligence on complications with the security process, baggage collection, etc. is useful to prepare personnel for entering the country. It should be clearly understood if visas fees are payable. To the extent these fees can be paid in advance, online through official portals, this should be done to limit any financial exchanges at the point of entry.

All the same issues need to be considered on exit, in addition to entry, for personnel.

Enforcement of local laws, and proper oversight of local immigration and customs officials will be assessed to help determine the likelihood of illicit activity being properly deterred (and/or punished) along with the level of compliance training local immigration and customs officials receive (along with the general levels of professionalism). Official policies and procedures governing the

immigration and customs officials need to be reviewed. In addition, it needs to be determined if the officials are government officials or privately contracted.

Particular times of the day, or days of the week (e.g. before a weekend or before a public holiday) will be identified if they carry increased compliance risk for suppliers and partners entering particular countries and dealing with customs and/or immigration officials.

In Storage

Customs delays are frequent in the MEA. Products can be in storage for long periods as they are processed through customs clearance. This is not only a cost for telecommunications suppliers but also a potential compliance risk. Details of where products are being warehoused, the cost of storage and for how long they will be stored need to be well understood. Most importantly, the process for releasing products from storage needs to be clear.

On the Road

Once people and products are through the entry point and in transit to partner warehouses or stages points and/or on to end customer sites, the compliance focus switches to understanding the key challenges on the routes that the telecommunications supplier's third party freight forwarders will be managing on the ground.

Once again, due diligence is key. There are some important questions to ask: Has the right freight forwarder been chosen? Has their local customer base been analysed? Does it include international customers, government departments/ministries, etc.?

What is the route? Are there any alternatives? How long should the journeys take? Are there tolls or security checkpoints that need to be traversed? Is the local transport police active on these routes and do they have a reputation for stopping traffic (particularly vehicles shipping goods)? If a vehicle is stopped, what paperwork can the transport police legitimately ask for and what type of inspections are they legally allowed to carry out? Can (and do) they apply on the spot fines and penalties? All this information helps avoid difficult situations and prepare supplier (and partner) personnel for dealing with such situations.

Routes (and travel times) need to be chosen carefully to avoid such challenges. If tolls are in operation, what are the tolls? Will extra charges be demanded? If there are checkpoints, are any legal payments required (and if so, what are they?). These are important details for suppliers and their partners, including third party freight forwarders, to have (and be trained on, if necessary) to equip them to manage any such challenges and minimise delays.

In addition to the above, the security risk of hijacking or other criminal activity on the roads needs to be assessed and managed.

Accessing Customer Sites

Proper due diligence is required to understand the requirements to secure access to customer sites. Access may often require additional paperwork and customer employees in attendance. All this needs to be thoroughly checked in advance. Site hours need to be checked to make sure arrival is timed correctly and customer staff are available, reducing the potential for requiring special actions from customer staff and possible resulting compliance issues.

Acceptance of the Initial Project

Acceptance, post-delivery and implementation, is a key stage in any major telecommunications

infrastructure project and often a difficult and time-consuming process. These projects are usually contracted on a turnkey basis with the majority of payment back ended to acceptance (i.e. once the equipment has been installed and the installed tested and accepted by the customer). It is critical for suppliers to ensure acceptance is swiftly and successfully executed so cash can be collected (and, depending on the supplier's accounting rules, project revenue (whether in whole or in part) recognised)). Supplier involvement during this stage is critical to manage any compliance issues as the supplier's personnel and/or its partners work closely with customer personnel to secure acceptance.

After the Initial Project is Completed

Ongoing support and maintenance and the importation of spare product parts will continue to bring the supplier and its partners in and out of countries where the initial project was delivered and engaging with multiple third parties. Continued diligence after initial project completion is critical to ensure that issues do not occur post-implementation, particularly if partners change over time.

Reporting

Everything happening on the project needs to be reported to the supplier by its personnel and its partners and a simple and effective process needs to be put in place (and supplier personnel and partners trained on that process) to facilitate this. Things that are known about can be more effectively managed. The sooner the supplier knows of an issue, the sooner the supplier can evaluate it, take appropriate action and mitigate its risk. Key to the supplier successfully managing compliance risk is a well-resourced project management team with deep compliance experience. Key to ensuring that the supplier has timely access to information is a culture where supplier employees and partners are comfortable that they can report any issues without fear of supplier retaliation.

Conclusion

As this article seeks to demonstrate, proper due diligence and planning are key to managing MEA compliance risk. This applies both in the telecommunications industry, and across industry sectors, and companies benefit from ensuring that they fully understand every aspect of the delivery and implementation of a major project (and any post-implementation challenges) in advance.

Al Tamimi & Company's TMT team regularly advises customers and suppliers on the delivery of large scale, business critical MEA telecommunications and technology projects. For further information, please contact Martin Hayward (m.hayward@tamimi.com).