LEGAL AND REGULATORY COMPLIANCE

Compliance is not optional – everyone must obey the law. Not so long ago, a short paragraph buried amid other 'boilerplate' obliged both parties to obey applicable laws. Nothing more seemed necessary.

Times have changed. Legislators and regulators, like hackers and thieves, have discovered personal data and identity theft. Regulated businesses are more closely regulated than before and more and more outsourced solutions involve regulated activities, as opposed to operation of computers and networks. Customers expect suppliers to provide compliant solutions.

How, then, to meet customers' needs, allocate risks and responsibility and help keep all concerned in the good graces of regulatory authorities?

First, understand the ground rules. Customers cannot delegate regulatory obligations. Bankers, for instance, who answer to regulators for the safety of depositors' funds, cannot hand off those responsibilities and wash their hands. They can and do prescribe procedures rooted in their understanding of regulatory requirements, then hold suppliers accountable for compliance with those procedures. Suppliers of service may have deep knowledge of regulated industries, but do not and cannot give legal advice or practice accountancy. Customers should (and do) rely on their own accountants and lawyers.

Second, separate compliance obligations into distinct elements, not only (i) compliance with specific requirements; but (ii) interpretation of those requirements; (iii) definition and implementation of processes to meet requirements; (iv) monitoring changes in requirements; then (v) development and implementation of changes in policies and procedures to accommodate those changes.

Third, allocate responsibilities between the parties according to their respective legal and operational responsibilities, as well as common sense. Consider which side is best positioned to assess and manage risk or has ultimate legal responsibility. For example, where an HR solution includes payroll, the customer will decide, mindful of legal requirements, its policies concerning overtime, vacation, fringe benefits, maternity and other leave and a host of other issues. Customers expect suppliers to know federal and state payroll tax rates and calculate withholding appropriately.

Many customer-oriented forms divide the legal universe into 'customer laws' (generally, those that apply to the customer's industry, such as banking or insurance) and 'supplier laws' (essentially, everything else). Skewed definitions are unhelpful, and many of the most important laws (concerning privacy, for instance) apply to both parties but in different ways. In the unlikely event that personal data are hacked, state notice laws require the supplier in possession of the data to inform the customer, as owner of the data, who must give notice to affected individuals and certain public agencies.

CONTINUED

COMMENTARY | LEGAL AND REGULATORY COMPLIANCE

This publication is a summary of legal principles. Nothing in this document constitutes legal advice, which can only be obtained as a result of a personal consultation with an attorney. The information published here is believed accurate at the time of publication, but is subject to change and does not purport to be a complete statement of all relevant issues.

In general,

- Suppliers assume responsibility for compliance with laws affecting their business, including the laws of other countries from which they provide service.
- Customers remain responsible for compliance with laws affecting their businesses. When those laws affect outsourced services, customers may prescribe requirements, embed them in written policies and operating procedures, then hold suppliers accountable for compliance. They may also expect suppliers to report obvious issues that come to their attention (eg, improper payments).
- Where the parties' responsibilities overlap detailed matrices mapping their responsibilities are an excellent tool for sorting and then managing the parties' responsibilities. With privacy issues, the European distinction between 'controllers' and 'processors' is useful.

What if laws and regulations change, as often they do? Since regulatory changes are risks beyond anyone's influence or control (like embargoes, quarantines and other kinds of unpredictable official action) they are not risks suppliers should be expected to assume (although some customer-oriented forms would assign suppliers all risk of future regulatory changes).

Accommodation of change may involve a combination of (i) customer-specific project work or process changes and (ii) system changes affecting many customers, such as those in a particular industry such as insurance or health care. The latter can often be apportioned among affected customers, so that no single customer bears disproportionate costs. Operational costs for new, compliant services may or may not be captured by existing metrics such as numbers of devices, cycles or transactions. Sometimes, adjustments based upon net impact may be warranted.

Finally, both customers and suppliers should treat compliance as an ongoing responsibility and activity. Rather than wait upon events, then react, all concerned are well advised to consult frequently together, build compliance reviews into governance and change management, assign responsibility to named individuals (as is often done for security) and conduct periodic compliance training to maintain awareness of important issues.

Neither side should assume disproportionate risk or insure the other; but active, disciplined collaboration can reduce unavoidable compliance risks.