25

Risk Governance for IT Outsourcing

MARCUS CHOW

In today's digital age, information technology (IT) is a significant part of the operations of most companies. Many businesses outsource part or all of their IT to third-party providers.

The most common types of IT outsourcing are in systems development and maintenance, data centre operations, network administration, disaster recovery services, application hosting, and cloud computing. The outsource function can involve the provision of IT capabilities and facilities by a single third party or multiple vendors located in Singapore or abroad.

The decision to outsource is often one based on cost-benefit analysis, but the important questions around risks and risk management should not be ignored, otherwise, the outsourcing can go awry.

THE BOARD'S ROLE

The responsibility for properly overseeing outsourcing lies with both the board and senior management.

After all, outsourcing is handing responsibility to an external service provider. The wholesale delegation of core business practices and assets to third parties without adequate oversight and, say, no plan around security or business continuity, would be a dereliction of the fiduciary duty of care by directors.

The board should therefore ensure, in the first instance, that management develops and implements appropriate enterprise-wide policies for outsourcing. These policies should address all aspects of the end-to-end outsourcing relationship, including the determination of the service requirements and strategies, selection of the outsourcer, negotiation of the contract, monitoring of the implementation, and making any necessary changes to the outsourced arrangements.

When an outsourced arrangement is tabled for approval, the board should ensure the following:

- That the outsourcing supports the company's overall requirements and strategic plans.
- That the organisation has the expertise to oversee and manage the relationship.
- That the evaluation of potential providers is based on the scope and criticality of the outsourced services.
- That there is a proper risk analysis and risk management programme specific to the selected outsourcer and services.
- That the regulators, where appropriate, are notified of the outsourced relationships.
- That the requisite regulations and best practices guides applicable to the relevant institution are adhered to.

The board should subsequently monitor the outsourcing implementation, focusing not just on the benefits realised and unrealised, but also ensure that risks and the risk management programme are updated.

OUTSOURCING RISKS

The biggest operating risks in outsourcing relate to security and controls. Institutions which handle a large amount of confidential or customer personal data face the challenge of ensuring the robustness of internal control systems to withstand the risks of cyber-attacks and misuse by employees.

Physical site security, malware protection, employee background checks, and controls to protect critical or sensitive IT assets from unauthorised activity by service provider staff such as system administrators with highly privileged access – these are just some of the details that boards must demand accountability for in risk oversight.

Add to that vigilance on the type of data going to offshore jurisdictions, the level of legal protection offered where the servers are physically located, and the security risk issues become very real.

It would be impractical and expensive to address all known and projected risks. Thus, the board should work closely with management to prioritise and manage especially the company's high-risk IT vulnerabilities.

DISCIPLINING THE CLOUD

Among the outsourcing options is the use of cloud computing, a service and delivery model for enabling on-demand network access

to a shared pool of configurable computing resources (including servers, storage, and services).

Clouds can be public (open to anyone who wishes to use them), or private (restricting the number of participants), or a hybrid.

The risks of outsourcing become even more immediate and obvious when using cloud services due to the cloud's openness and complexity. For example, public clouds are open to all, with a number of layers in the services "stack". More specifically, a user engages with a portal (layer one), which opens a piece of software (layer two), operating on a platform which has multiple applications and functions (layer three). These three layers can leverage storage (layer four) from anywhere, which runs on top of an infrastructure base (layer 5). In each layer, there may be a different service provider with whom the end users engage, and these stacks create different risks which may need to be mitigated differently.

For private clouds, the number of participants will be reduced, but the same complexity of layers can exist.

The attendant risks of clouds in areas of data integrity, sovereignty, recoverability, confidentiality and compliance therefore demand a sharp level of business discipline in due diligence and ongoing vendor management.

When all the risks of outsourcing (whether traditional or through the cloud) are considered, one may wonder how anyone ever makes a decision to outsource. Yet, there is good evidence that such deals are done frequently and often satisfactorily from both the buyer's and seller's perspectives. So it is more a question of boards and companies being aware of the risks and pitfalls in the analysis and making of the outsourcing decision, and ensuring the proper contracting and implementation of the outsourcing arrangements. ■