

# review **Vendor Management Using COBIT 5**

The increased use of outsourcing arrangements and the acceptance of cloud computing models has benefits and associated risk. Although organizations outsource processes, accountability cannot be delegated and, therefore, managing vendors and their performance in accordance with business expectations is of primary importance for business management. Although some readers may interpret from the name of the book that it is meant only for organizations using COBIT 5, *Vendor Management: Using COBIT® 5* is, in fact, very good guidance on vendor management for all organizations.

*Vendor Management: Using COBIT® 5* provides comprehensive guidance on managing vendors. The major topics covered in the book are:

- The vendor management life cycle and process and an organization's responsibilities
- The risk associated with vendor management and risk mitigation actions
- Documentation that can help in binding vendors
- Managing cloud service providers

The book contains 12 appendices that include sample templates for vendor selection, tender documents, contracts and service-level agreements (SLAs). The appendices also include a sample checklist and mapping of COBIT® 5 and ITIL v3 for vendor management.

Since the vendor management process includes various stakeholders, this book is useful for legal, compliance, audit, finance, risk management, senior management, procurement functions and overall management functions that use outsourced services.

This book discusses life cycle management for third-party services and the overall vendor management process. The life cycle steps include initial setup work, e.g., defining requirements, inviting proposals, selecting a vendor and negotiating with the vendor. The second step relates to the contract, and the third step is executing the contract and managing operations. The final step is termination

or transitioning the vendor. This section of the book also describes various stakeholders' responsibility in vendor management.

The next chapter discusses the common threats in vendor selection; contract development; and requirements, governance and strategy for vendor management. It also addresses the financial impact of inadequate vendor management.

The fourth chapter describes risk mitigation actions. Although it is true that the risk associated with outsourcing varies for every organization, there is some common risk and, hence, common mitigation actions. The book describes 22 risk mitigation actions for identified threats and provides guidance from COBIT 5 processes and enablers. This chapter also provides a practical case study.

The fifth chapter describes different documents required in every phase of the vendor management life cycle, e.g., tender, contract, SLA, operational level agreement. This chapter provides guidance on developing these documents and discusses common pitfalls.

The last chapter provides guidance on managing a cloud service provider. Since management's main concern is information security, excerpts from ISACA's publication *Security*

*Considerations for Cloud Computing* are included for reference. These excerpts form the main contents of this chapter. The guidance relates to different cloud services, e.g., Infrastructure as a Service, Platform as a Service, and Software as a Service, on different types of clouds, e.g., public, private, hybrid and community. An appendix from the excerpted publication, which covers mapping threats and risk-mitigating actions, is included.

## Editor's Note

*Vendor Management: Using COBIT 5* is available from the ISACA® Bookstore. For information, visit [www.isaca.org/bookstore](http://www.isaca.org/bookstore), contact support at <https://support.isaca.org/> or telephone +1.847.660.5650.



## Reviewed by Sunil Bakshi,

CISA, CGEIT, CISM,  
CRISC, ABCI, AMIIB,  
BS 25999 LI, CEH,  
CISSP, ISO 27001  
LA, MCA, PMP

Who is a visiting faculty member and an industry expert at the National Institute of Business Management (India) and a consultant and trainer in IT governance and information security.