COBIT® 5

Briefing Paper

September 2013

Protect • Comply • Thrive

COBIT® 5

Overview

Businesses today must understand the value of information and the importance of managing their IT in such a way as to maximise that value. The ubiquity of information and IT is such that even organisations that would not traditionally consider themselves part of the IT industry must consider it a significant component of their business.

There is also increasing regulatory pressure regarding the security and use of this information. Governments and business partners want to know that information is secure; shareholders and investors seek maximum returns on leveraging information.

COBIT® 5 is an increasingly popular and widely used control framework for the management of the IT organisation. The framework seeks to ensure that IT delivers value to the organisation through controlling the inputs and outputs of business processes. Further, it is of use to all organisations in any sector due to its dedication to first principles of governance and management.

Increasing the effectiveness of your organisation's governance and management of IT can lead to significant benefits:

- Improvement of services related to or served by IT
- Streamlining complex business processes
- Increased confidence from investors and business partners
- Compliance with regulations

About COBIT 5

Developed by ISACA®, COBIT (Control Objectives for Information and Related Technology) is a framework for IT service management which has traditionally offered benefits across the business spectrum. First released in 1996, COBIT is now in its fifth edition, and has become broader and more comprehensive through drawing in related systems and standards.

COBIT 5 consolidates the tools and processes developed in COBIT 4.1 and earlier, as well as ValIT (governing and managing investments) and RiskIT (governing and managing risk). As such, COBIT 5 is a holistic approach to IT governance and management, with the added advantage that it remains technology agnostic.

By remaining technology agnostic, COBIT 5 ensures that the guidance offered for the management of IT is valid regardless of your organisation. This approach is based on five key principles, which are transferrable across private, public and non-profit organisations.

"Governments and business partners want to know that information is secure; shareholders and investors seek maximum returns on leveraging information."

The five principles are:

- Meeting stakeholder needs
- Covering the enterprise end-to-end
- Applying a single, integrated framework
- Enabling a holistic approach
- Separating governance from management

COBIT 5 comes with inputs and outputs for each and every management practice, while COBIT 4.1 only provided these at a process level. The inclusion of this additional level of detail naturally makes COBIT 5 a significantly more exhaustive system.

The main strengths of this new approach is that it is more robust, reliable and repeatable.

Meeting stakeholder needs

It is important for any governance and management system to identify the stakeholders' needs. By establishing early on the essential functions, inputs and outputs, business processes can be managed in a manner that improves oversight and efficacy. COBIT 5 offers a model for identifying internal and external stakeholders, and their interest in the outcomes of its implementation.

Covering the enterprise end-to-end

It is important in any major endeavour to ensure that the whole enterprise and all processes are accounted for. The key practices identified by COBIT 5 cover the full business process, including all interactions between IT, other business units and external suppliers/customers.

Applying a single, integrated framework

Probably the most important detail of COBIT 5 is its 'modular' nature that enables the organisation to draw in processes and controls from other frameworks and standards. In this way, the organisation is able to tailor the system to their needs and regulatory requirements.

Enabling a holistic approach

COBIT 5 recognises that there are multiple key facets in the governance and management of information. The framework provides controls to enable your organisation to effectively manage risk, continuity, security and privacy of information, while ensuring compliance with required standards and regulations.

Separating governance from management

Governance and management comprise different activities to serve different purposes, and thus different organisation structures and processes are necessary. COBIT 5 defines distinct categories of process in order to ensure that governance goals and processes are identified and implemented as separate from those of management.

Compliance

Governance of corporate IT is seeing rapid growth as a regulatory requirement.

In South Africa, the Department of Public Service and Administration (DPSA) has mandated COBIT 5[1] for all public services, as well as many private and non-profit organisations with which they do business.

In the US, COBIT 5 is recognised as an effective method of complying with the Sarbanes-Oxley Act[2]. The mandate to produce an internal control report included in their annual Exchange Act report is readily generated as a by-product of the adoption of COBIT 5. IT Control Objectives for Sarbanes-Oxley, written by the IT Governance Institute, provides a further reference source for executives when evaluating an organisation's IT controls as required by the Act.

The COBIT 5 methodology

COBIT 5 provides a structure for the governance of enterprise IT through the alignment of enterprise goals and IT goals. It achieves this through a broad set of guidance that can be applied to any business model, and integrates with other frameworks to offer precision and a wide scope of compliance opportunities.

The guidance offered is broken down between seven enablers – features of the ITSM that can be leveraged to achieve the five key principles. Within this structure,

individual business processes are identified and further broken down into key practices. By working down through the layers, the organisation naturally works towards achieving the primary goals of improving the business, aligning corporate and IT goals, and compliance with legal, regulatory and contractual obligations.

These principles, enablers and processes are deliberately non-prescriptive. An implementation of COBIT 5 can only be considered successful if it refers consistently to the organisation at hand: the goal is for the organisation to create a framework that is a synergy between COBIT 5 and the enterprise's needs.

Implementing COBIT 5

In implementing COBIT 5 as a framework, your organisation will likely discover that the flexibility of the framework equally causes some consternation. The absence of specific measures for specific technologies requires the board and management to consider carefully how the organisation conducts its business internally. This – while potentially frustrating for those seeking a swift transformation – is of great benefit to an organisation embarking on a major governance programme.

Organisations that are well prepared and already exist in a state of regulatory compliance, meanwhile, will find the transition to COBIT 5 simple, and may find that the structure offers a more streamlined approach.

The passage through this process can be enlightening for an organisation as it aligns the IT goals with the enterprise goals. Recognition of divergence can bring about effective change to streamline business processes, and each aspect of the framework – such as risk management, information security, business continuity, and so on – can highlight weaknesses beyond the IT department.

While it is possible that a company can migrate to COBIT 5 quickly and efficiently, it is likely that many organisations will need some additional guidance. Consultants can offer expertise in implementation, as well as identifying key competencies and their spread throughout the enterprise. Toolkits, such as the IT Governance Control Framework Implementation Toolkit, can provide the backbone of the policies and procedures that will need to be established.

For organisations seeking to develop the skills and expertise to handle the implementation and day-to-day duties associated with COBIT 5, training and CGEIT (Certified in the Governance of Enterprise IT) qualifications are available. This can be further bolstered by developing expertise in related standards and frameworks, thereby providing the organisation with a solid basis for continued compliance, improved practices and a solid business model.

Integration with other frameworks and standards

COBIT 5 has been designed to integrate cleanly and painlessly with other major frameworks and standards, including the IT Infrastructure Library® (ITIL), ISO/IEC 27000, COSO and PMBOK®. It has also been developed in such a way as to align with ISO/IEC 38500:2008 – the international standard for the corporate governance of information technology.

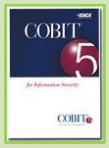
As a 'modular' framework, the enterprise can adapt the system to comply with the regulations and standards applicable to the industry and obligations. By complying with necessary regulations and standards as part of the implementation of a COBIT framework, the organisation can ensure that all needs are met as part of a single programme. This is clearly preferable to multiple implementations, which may require repeated examination of business processes that are of concern to different standards, such as risk management or business continuity.

Useful Resources

IT Governance offers a unique range of products and services, including books, standards, pocket guides, training courses, staff awareness solutions and professional consultancy services.

COBIT 5 Resources

- **COBIT 5 for Information Security**



In this manual you will be shown how the relevant frameworks, best practices and standards for information security can be adapted to form a cohesive framework using COBIT 5. COBIT 5 is mapped to International Standards and relevant frameworks in the appendix to the book to aid this process.

- **Governance and Internal Controls for Cutting Edge IT**

In Governance and Internal Controls for Cutting Edge IT, Karen Worstell explains strategies and techniques to guide IT managers as they implement cutting edge solutions for their business needs in the context of COBIT 5.

- **IT Governance Control Framework Implementation Toolkit**

Drawing on a decade of experience in IT governance, combined with ITGP's established skills in publishing easy-to-use, customisable policy and procedure documentation templates, this COBIT® 5 Documentation Toolkit will help you accelerate your IT governance project, while helping you avoid documentation dead-ends or re-inventing the procedural wheel.

- **COBIT 5 Foundation (2 day) Course**

This is the official 2-day COBIT 5 Foundation Course using content with the permission of ISACA. It includes the official COBIT 5 foundation exam from APMG. It is an interactive classroom-based training course based on the latest version, COBIT 5.

- **Certified in the Governance of Enterprise IT (CGEIT) Training**

The CGEIT designation is designed for professionals responsible for managing, providing advisory and assurance services, or otherwise support the governance of an enterprise's IT, and wish to be recognised for their IT Governance-related experience and knowledge.

- **COBIT 5 Foundation Training (90 Days Online Access, Excluding Exam)**

Now you can study for the COBIT 5 Foundation exam using this online e-learning course. Study as and when you want basing your studies around your normal work schedule. This e-learning course includes a practice exam that allows you to test your knowledge prior to taking the actual COBIT 5 Foundation exam.

IT Governance Solutions

IT Governance source, create and deliver products and services to meet the evolving IT governance needs of today's organisations, directors, managers and practitioners.

IT Governance is your one-stop-shop for corporate and IT governance information, books, tools, training and consultancy. Our products and services are unique in that all elements are designed to work harmoniously together so you can benefit from them individually and also use different elements to build something bigger and better.

Books

Through our website, www.itgovernance.co.uk, we sell the most sought after publications covering all areas of corporate and IT governance. We also offer all appropriate standards documents.

In addition, our publishing team develops a growing collection of titles written to provide practical advice for staff taking part in IT Governance projects, suitable for all levels of staff knowledge, responsibility and experience.

Toolkits

Our unique documentation toolkits are designed to help small and medium organisations adapt quickly and adopt best management practice using pre-written policies, forms and documents.

Visit www.itgovernance.co.uk/free_trial to view and trial all of our available toolkits.

Training

We offer training courses from staff awareness and foundation courses, through to advanced programmes for IT Practitioners and Certified Lead Implementers and Auditors.

Our training team organises and runs in-house and public training courses all year round, covering a growing number of IT governance topics.

Visit www.itgovernance.co.uk/training for more information.

Through our website, you can also browse and book training courses throughout the UK that are run by a number of different suppliers.

Consultancy

Our company is an acknowledged world leader in our field. We can use our experienced consultants, with multi-sector and multi-standard knowledge and experience to help you accelerate your IT GRC (governance, risk, compliance) projects.

Visit https://www.itgovernance.co.uk/consulting for more information.

Software

Our industry-leading software tools, developed with your needs and requirements in mind, make information security risk management straightforward and affordable for all, enabling organisations worldwide to be ISO27001-compliant.

Visit https://www.itgovernance.co.uk/software for more information.

Contact us: + 44 (0) 845 070 1750

www.itgovernance.co.uk servicecentre@itgovernance.co.uk

[1] http://www.itweb.co.za/office/isaca/PressRelease.php?StoryID=237268
[2] http://sox.ulitzer.com/node/2240485