COBIT® Focus

Volume 4, October 2013

Come join the discussion! Sagar Anisingaraju will respond to questions in the discussion area of the COBIT 5—Use It Effectively topic beginning 21 October 2013.

What Does COBIT 5 Mean for Your Business?

By Sagar Anisingaraju

When it comes to enterprise use of IT assets, executives are looking for answers to three things:

1. Is the organization getting IT right?
2. Is the organization is buying or building the right IT capabilities?
3. Are there any gaps in capabilities exposing the business to unwarranted risk?

For most companies, the answers to these questions come from understanding the underlying multiple frameworks used across operations. For example, COBIT®[1, 2] enables companies to improve IT governance by ensuring that appropriate process, governance and management enablers are used to build IT capabilities to achieve stakeholder goals. As a framework that can be used to measure and monitor IT services and implement best practices for those services, ITIL[3] provides an operational level of service management. The ISO/IEC 27000 series[4] comprises the preferred standards used by IT security professionals. For companies that compete in regulated segments such as banking, insurance, utilities or health care, additional industry specific standards, frameworks and guidelines may be in use.

When an organization leverages multiple standards, frameworks and guidelines, it may end up creating separate controls recommended by each that are managed separately. As a result, it not only creates duplicate work, as controls may be overlapping, but more important, it becomes challenging for executives to get a comprehensive understanding of their organization's IT risk exposure and governance process. Current tools that enable organizations to create a shared library of common controls across frameworks are cumbersome to use and manage. Control libraries often become huge and complex to use for most companywide governance, risk and compliance (GRC) initiatives.

COBIT® 5, the latest edition of ISACA's globally accepted framework for governance and management of enterprise IT (GEIT), addresses this issue. It provides an end-to-end business view that integrates other standards, frameworks and guidelines, such as ITIL and ISO/IEC 27001, into an overall enterprise governance and management framework. With a COBIT 5-inspired model, stakeholders such as security professionals, IT operations executives and IT auditors can see how their work relates to the overall scope of governance and management. COBIT 5 does not replace these other sources of reference. Instead, it is an overarching umbrella framework that helps them all fit together. For example, COBIT 5 is the frame on which ITIL can provide additional color for daily management of IT operations. Using this frame embodies the same essential principles of business analysis, helping information and technology teams to achieve strategic business goals.

IT has always had to deal with risk factors such as cyberattacks, external hacking and disgruntled employees. New risk factors are, however, driven by consumerization of IT—ranging from bring your own device (BYOD) to social media and associated big data.

With these new unstructured external threats, the security perimeter is changing. *COBIT® 5 for Information Security* offers additional, security-specific guidance designed to help your IT department implement an effective framework and reduce risk exposures.

The key changes in COBIT 5 include:

- A clear distinction between *governance* and *management*, bringing greater relevance to a wider business audience
- A linkage between specific IT-enabler goals and broader enterprise-level goals. It also includes more explicit guidance to levers of change (enablers) beyond process, such as culture, ethics, behavior, people, skills and competencies.
- Modifications to the process model, including new processes
- A new process capability assessment approach, which replaces the COBIT 4.1 capability maturity model (CMM)-based modeling

COBIT 5 is not a panacea. It is not something to lift and use exactly as-is. Each enterprise needs to map it and mold it to the business's requirements, organizational structure and processes. The comprehensive scope of COBIT 5 guidance may overwhelm new users and inhibit its adoption. Use of all available ISACA guidance and tools, as well as having key staff take the COBIT 5 training available in the marketplace (COBIT Foundation, COBIT Implementation and COBIT Assessor courses), is highly recommended.

COBIT 5 should be implemented to ensure that the organization has a road map that will allow it to address all of its IT governance and risk issues. If the organization is already using some level of COBIT selectively within pockets of the organization, the changes in COBIT 5 should be reviewed to identify where it can help address specific issues or organizational changes. In addition, with COBIT 5 as a single enterprisewide IT GRC framework, the organization can implement a comprehensive analytics solution that enables it to continuously measure and improve its governance status, risk exposure, and overall compliance with policies and regulations. There will be no further need to reconcile multiple silos through reports to assess the organization's overall risk or compliance status.

COBIT 5 is an important milestone. Adopting it will be a very promising journey to simplify the organization's efforts in implementing a single organizationwide GRC framework. If the organization already has a mature GRC environment, it will quickly realize that COBIT 5 gives it a better handle on GEIT. If the organization is just starting, COBIT 5 will give it the formal road map it needs for a fast-track approach.

Sagar Anisingaraju

Is the chief strategy officer at Saama Technologies Inc. Anisingaraju creates strategic initiatives to lead Saama into emerging business areas with competitive differentiation. He enjoys his time spent with customers to understand their business problems specifically related to big data. He was the winner of the 2013 Chief Strategy Officer of the Year award, presented by Innovation Enterprise.

Endnotes

[1] ISACA, COBIT 5, USA, 2012

[2] ISACA, COBIT 5 Training and Accreditation FAQs

[3] APM Group Ltd., ITIL

[4] International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), ISO/IEC 27000, Information Security Management Systems (ISMS) standards

president of ISACA.