Add Value to What Is Valued

I was raised by my mother, a single parent, in relative poverty. This meant that she would sometimes come home with a new shirt or a pair of jeans for me and declare what great value they were! I must admit, at the time I could not see the value. My only thought was that I had to go outside onto the mean streets of the north side of Dublin, Ireland, in those clothes! The point of this anecdote? To demonstrate that value means different things to different people, depending on their perspective.

This is also true in business. Enterprises have many stakeholders, and "creating value" means different—and sometimes conflicting—things to each of them.[1] Bearing this in mind, how can we leverage IT audit to create value?

Defining Value

Internal audit does not define value for the enterprise. That is a function of governance. The governance system should consider all stakeholders when making benefit, risk and resource assessment decisions. For each decision, the following questions can and should be asked: For whom are the benefits? Who bears the risk? What resources are required?[2] In other words, value creation means realizing benefits at an optimal resource cost while optimizing risk (**figure 1**).[3]

Ian Cooke, CISA, CRISC, CGEIT, COBIT Assessor and Implementer, CFE, CPTE, DipFM, ITIL Foundation, Six Sigma Green Belt
Is the group IT audit manager with An Post (the Irish Post Office based in Dublin, Ireland) and has 30 years of experience in all aspects of information systems. Cooke has served on several ISACA committees and is a current member of ISACA's CGEIT® Exam Item Development Working Group. He is the community leader for the Oracle Databases, SQL Server Databases, and Audit Tools and Techniques discussions in the ISACA Knowledge Center. Cooke supported the update of the *CISA® Review Manual* for the 2016 job practices and was a subject matter expert for ISACA's CISA® and CRISC™ Online Review Courses. He is the recipient of the 2017 John W. Lainhart IV Common Body of Knowledge Award for contributions to the development and enhancement of ISACA publications and certification training modules. He welcomes comments or suggestions for articles via email (Ian_J_Cooke@hotmail.com), Twitter (@COOKEI), or on the Audit Tools and Techniques topic in the ISACA Knowledge Center. Opinions expressed are his own and do not necessarily represent the views of An Post.

The Goals Cascade

Stakeholder needs can be related to enterprise goals by using, for example, the balanced scorecard (BSC).[4] These, in turn, are cascaded to IT-related goals using the IT balanced scorecard (IT BSC). Finally, IT-related goals are cascaded to enabler goals (**figure 2**).[5] Enablers are factors that, individually and collectively, influence whether something will work.[6]

If enablers influence whether something will work, and this can be traced back to stakeholder needs, then it follows that auditing these enablers to check whether a standard or set of guidelines is being followed, records are accurate, or efficiency and effectiveness targets are being met[7] will add value.
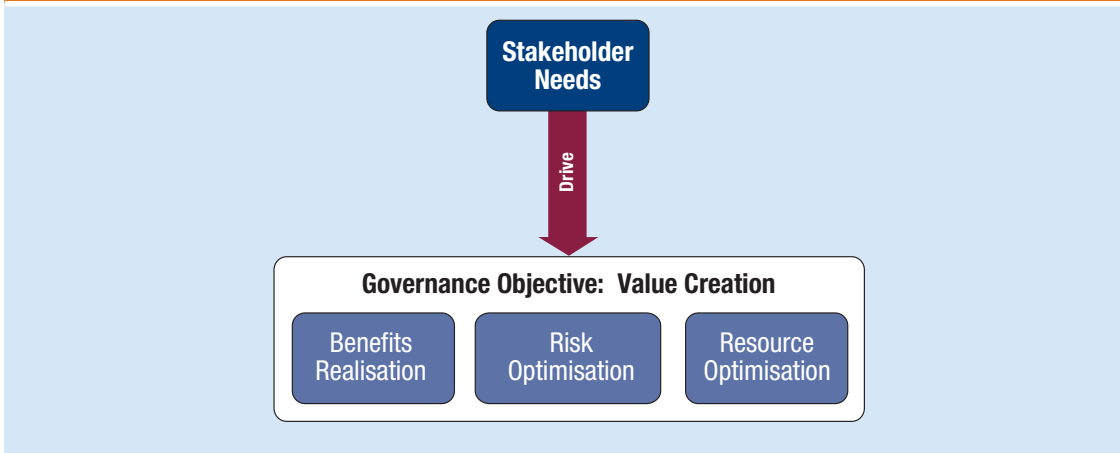
There is, of course, a potential problem here: What if one's enterprise has not adopted COBIT® 5? What if (quite likely) there is no goals cascade? The good news is that there is a solution—one can work in reverse. If the enterprise's IT processes are mapped to the COBIT 5 process reference model,[8] the resulting COBIT 5 processes can be used to determine the IT-related goals.[9] These, in turn, can be used to determine the enterprise goals.[10] For example, business continuity would map to COBIT process Deliver, Service and Support (DSS) DSS04 *Manage continuity*. This maps to IT goal ITG07 *Delivery of service in line with business requirements*, that, in turn, maps to enterprise goal EG07 *Business service continuity and availability*. Note that this will result in generic IT and enterprise goals that can and should be adjusted by senior business and IT managers. The enterprise should then decide which of these adds the most value.

Enablers

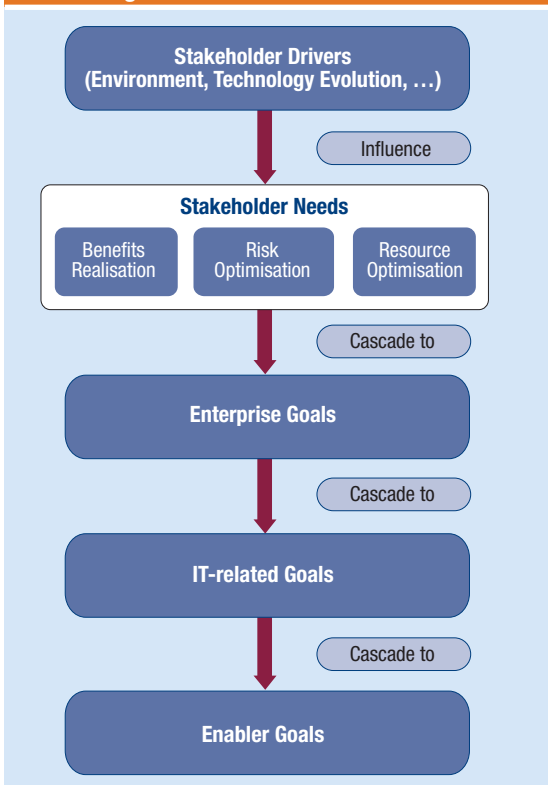The COBIT 5 framework describes seven categories of enablers (**figure 3**):[11]

- Principles, Policies and Frameworks are the vehicle to translate the desired behavior into practical guidance for day-to-day management.

- Processes describe an organized set of practices and activities to achieve certain objectives and

Figure 1—The Governance Objective: Value Creation

Stakeholder Needs

Drive

Governance Objective: Value Creation

Benefits Realisation | Risk Optimisation | Resource Optimisation

Source: ISACA, COBIT® 5, USA, 2012. Reprinted with permission.

Figure 2—COBIT 5 Goals Cascade

Stakeholder Drivers (Environment, Technology Evolution, …)

Influence

Stakeholder Needs

Benefits Realisation | Risk Optimisation | Resource Optimisation

Cascade to

Enterprise Goals

Cascade to

IT-related Goals

Cascade to

Enabler Goals

Source: ISACA, *COBIT® 5 for Assurance*, USA, 2013. Reprinted with permission.

produce a set of outputs in support of achieving overall IT-related goals.

- Organizational Structures are the key decision-making entities in an enterprise.
- Culture, Ethics and Behavior of individuals and of the enterprise are very often underestimated as a

success factor in governance and management activities.

- Information is pervasive throughout any organization and includes all information produced and used by the enterprise. Information is required for keeping the organization running and well governed, but at the operational level, information is very often the key product of the enterprise itself.
- Services, Infrastructure and Applications include the infrastructure, technology and applications that provide the enterprise with information technology processing and services.
- People, Skills and Competencies are linked to people and are required for successful completion of all activities and for making correct decisions and taking corrective actions.

Auditing the Enablers

At this stage, those who have read previous IS Audit Basics columns[12, 13, 14] are likely expecting the introduction of the ISACA® white paper on creating audit programs[15] and, indeed, this would work. However, in my opinion, the audit approach suggested in the white paper is best suited to enabler six, that is, auditing a discrete piece of infrastructure or technology or an individual application. This is because the approach is purely risk-based, which typically results in the audit objective being described in a control context. For example, in the paper on creating audit programs, the example given for an audit objective is "to determine whether program

Figure 3—COBIT 5 Enterprise Enablers
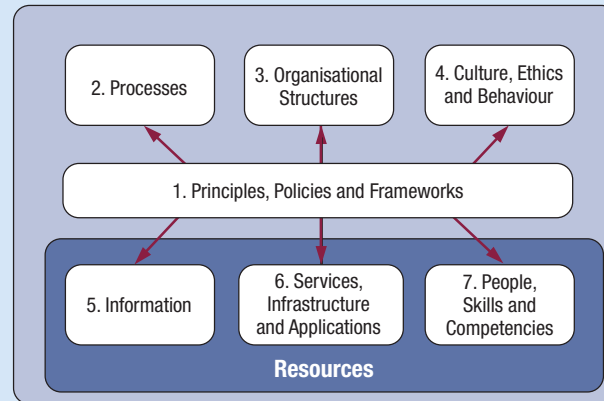
Source: ISACA, *COBIT® 5 for Assurance*, USA, 2013. Reprinted with permission.

source code changes occur in a well-defined and controlled environment."[16]

To meet all stakeholder needs, the assurance engagement should consider all three value objective components: delivering benefits that support strategic objectives, optimizing the risk that strategic objectives are not achieved and optimizing resource levels required to achieve the strategic objectives.[17] To meet these objectives, I recommend the adoption of the generic COBIT 5-based assurance engagement approach (**figure 4**).[18]

This approach is aligned with generally accepted auditing standards and practices, including the

Figure 4—Generic COBIT 5-Based Assurance Engagement Approach
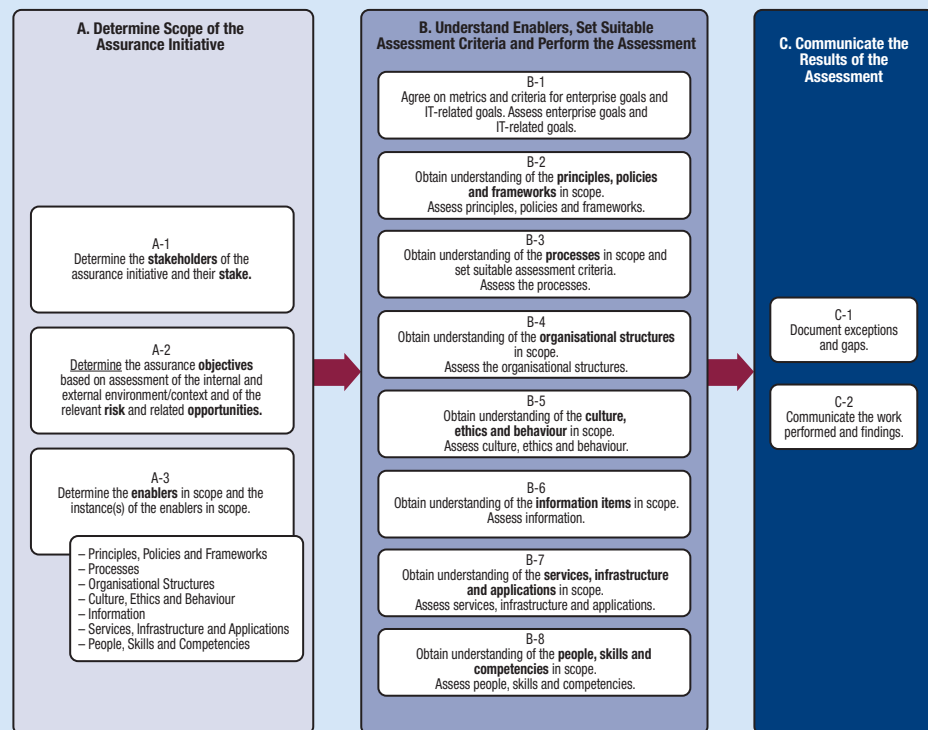
Source: ISACA, *COBIT® 5 for Assurance*, USA, 2013. Reprinted with permission.

phases defined in the creating audit programs document, specifically:[19]

- **Phase A**—Planning and scoping the assurance engagement (planning)

- **Phase B**—Understanding the subject matter, setting suitable assessment criteria and performing the actual assessment (fieldwork/documentation)

- **Phase C**—Communicating the results of the assessment (reporting/follow-up)

Furthermore, it references the COBIT 5 goals cascade to ensure that detailed objectives of the assurance engagement can be put into the enterprise and IT context, and, concurrently, it enables linkage of the assurance objectives to enterprise and IT risk and benefits.[20]

In addition to this process being described in detail in *COBIT® 5 for Assurance*,[21] ISACA has used the approach to develop audit/assurance programs for 34 of the 37 COBIT 5 processes.[22] Where these are used to audit horizontally[23]—that is, the same process across several different applications—the assurance engagements can not only create, but also demonstrate the link to enterprise value.

Conclusion

In May 2016, Dublin had the honor of hosting EuroCACS.[24] I met some ISACA colleagues in a social setting (incidentally, I was wearing a new shirt and jeans bought especially for the occasion!) prior to the evening reception. The conversation turned to COBIT and a comment was made about how COBIT® 4.1 was "better" than COBIT 5 as it could just be "picked up and used." I had completed COBIT 5 Foundation[25] training at the end of 2015 and so felt comfortable enough to answer.

COBIT 5, as opposed to COBIT 4.1, addresses all stakeholders' needs: benefits realization, risk optimization and resource optimization. By following the goals cascade or, where this is not in place, mapping upward to generic goals, enablers that truly add value to the enterprise, including processes, can be added to the audit universe. The approach also ensures that the objectives and results of the assurance engagement can be put into an enterprise and IT context. This, ultimately, allows audit to add value to what is valued.

Endnotes

1 ISACA, COBIT® 5, USA, 2012, *www.isaca.org/COBIT/pages/default.aspx*
2 *Ibid*., p.17
3 *Ibid*.
4 Kaplan, R. S.; D. P. Norton; *The Balanced Scorecard: Translating Strategy Into Action*, Harvard University Press, USA, 1996
5 *Op cit* COBIT 5, p. 17. The goals cascade is covered in greater detail in COBIT 5.
6 *Ibid*., p. 27
7 ISACA Glossary, Audit, *www.isaca.org/Glossary*
8 *Op cit* COBIT 5, figure 16, p. 33
9 ISACA, *COBIT® 5: Enabling Processes*, USA, 2012, figure 18, p. 227-229, *www.isaca.org/COBIT/Pages/COBIT-5-Enabling-Processes-product-page.aspx*. Map between the IT processes and IT-related goals.
10 *Ibid*., figure 17, p. 226. Map between the IT-related goals and enterprise goals.
11 *Op cit* COBIT 5, p. 27
12 Cooke, I.; "Audit Programs," *ISACA® Journal*, vol. 4, 2017, *www.isaca.org/archives*
13 Cooke, I.; "Auditing Mobile Devices," *ISACA Journal*, vol. 6, 2017, *www.isaca.org/archives*
14 Cooke, I.; "Auditing Data Privacy," *ISACA Journal*, vol. 3, 2018, *www.isaca.org/archives*
15 ISACA, *Information Systems Auditing: Tools and Techniques—Creating Audit Programs*, USA, 2016, *www.isaca.org/Knowledge-Center/Research/Documents/IS-auditing-creating-audit-programs_whp_eng_0316.PDF*
16 *Op cit* ISACA, *Information Systems Auditing: Tools and Techniques—Creating Audit Programs*, p. 8

17 ISACA, *COBIT® 5 for Assurance*, USA, 2013, p. 59, *www.isaca.org/COBIT/Pages/Assurance-product-page.aspx*

18 *Ibid.*, p. 55-82

19 *Op cit* ISACA, *Information Systems Auditing: Tools and Techniques—Creating Audit Programs*

20 *Op cit* ISACA, *COBIT 5 for Assurance*, p. 56

21 *Ibid.*, Section 2B, Assessment Perspective: Providing Assurance Over a Subject Matter, p. 53

22 ISACA, COBIT® 5 Process Audit/Assurance Programs, *www.isaca.org/KNOWLEDGE-CENTER/RESEARCH/Pages/Audit-Assurance-Programs.aspx#cobit5app*

23 Cooke, I.; "Innovation in the IT Audit Process," *ISACA Journal*, vol. 2, 2018, *https://www.isaca.org/archives*

24 European Computer Audit, Control and Security Conference, *https://www.isaca.org/ecommerce/Pages/european-cacs-europe.aspx*

25 I would like to take this opportunity to publicly thank the gentleman in question, Everett Breakey, CISA, CRISC, CISM, CGEIT, of the ISACA Ireland Chapter, who has made it his mission to bring COBIT 5 training to the population of Ireland.