Extending COBIT 5 Data Security and Governance Guidance

By Myles Suer, ITIL, and Les McMonagle, CISA, CISSP, ITIL

COBIT Focus | 30 January 2017

COBIT® 5 contains highly relevant guidance for IT practitioners and business leaders regarding governing and protecting data and information. However, the question of whether COBIT 5 is enough should be asked. This article explores what COBIT 5 provides and does not provide, then suggests a series of appropriate additions.

COBIT 5 does correctly start with an overarching set of business recommendations. For example, COBIT 5 suggests that business leaders include compliance with external laws and regulations, management of business risk, and compliance with internal enterprise policies in their balanced scorecard (BSC). For each of these, relevant metrics exist, including:

- The use and application of risk assessments
- The cost of regulatory noncompliance
- The measurement of noncompliance incidents
- The percentage of stakeholders who understand policies
- The percentage of policies supported by effective standards and working practices

These enterprise goals flow into a set of IT processes for information and data governance and security. COBIT 5 suggests that key elements of risk are securing information, processing infrastructure and applications. Here COBIT 5 currently relies on backward facing indicators. It looks, for example, at the number of security incidents that have caused financial loss or public embarrassment and at the number of IT services without standing security requirements. This is really important. It looks at the time to grant, change and remove access privileges and compares these against agreed-on services levels. COBIT 5 also looks at the frequency of security or risk assessments compared against the latest standards and policies.

COBIT Recommendations for Enterprise Security Process

COBIT 5 encourages each enterprise to adapt the COBIT content to the enterprise’s own priorities and circumstances. However, among the processes COBIT 5 recommends are 3 especially suited for security, and the metrics suggested for each are only a subset of measurements that might be meaningful to the enterprise. First is that a system is in place that considers and effectively addresses enterprise information security requirements. This appears overarching (a good thing), and the measures suggested for it include the number of key security roles that have been clearly defined and the number of security-related incidents. Most enterprises would wish to add other measures to the list in keeping with their own situation.

Second is a security plan that has been established, accepted and communicated throughout the enterprise. Here COBIT 5 looks at the level of stakeholder satisfaction with the security plan, the number of security solutions deviating from the agreed-on plan and the number of security solutions deviating from the enterprise security architecture. Architecture clearly compromises pain points in 2 ways: by leading to security gaps and by potentially lengthening the time to fix
security or compliance issues.

Third is that information security solutions are implemented throughout the enterprise. Here COBIT 5 metrics look at the number of services and solutions with confirmed alignment to the security plan at the same time as security incidents caused by nonadherence to the security plan. These are all great metrics to track and provide useful illustrative examples, but today’s enterprises will likely wish to add more, with greater specificity.

How Does the Real World of Information Look?

Today’s chief information officers (CIOs) insist that by focusing on an application view of security, COBIT® misses a major challenge with today’s enterprise architecture and that what is needed is a more holistic ecosystem approach to protecting enterprise data. CIOs say that security needs to move from perimeters and applications to the point of data consumption and protecting data to be effective now that, basically, the entire world is the organization’s perimeter. In contrast with the “big iron days,” where all data were in 1 secure place, today’s hybrid cloud/Software as a Service (SaaS) networks have blurred perimeters, and CIOs say the focus needs to shift from the systems to the data.¹

This is seen by CIOs as harder to put in place, but, ultimately, is required. A CIO put the problem this way: “You know those flight maps in the airline magazines? Those are our data flow maps, we have in our environment data flying all over the place. Today protecting data needs to become a bigger discussion. It needs written policies, user transparency, and data protection. And attention needs to be given not just to the pieces, but to the whole enchilada.”²

The authors of The Privacy Engineer’s Manifesto summarize this change well in their description of how data protection has changed. With the advent of firewalls, the emphasis was on keeping data within the firewall. This was followed by protecting data inside and outside of the firewall, and then came managing data through identity management and access control. The problem with access control, according to the authors, is that it became too easy to share information and violate privacy concerns. Another emerging issue is what enterprises need to do to safely exploit ever larger, more complex, distributed and disbursed data sets about individuals. According to The Privacy Engineer’s Manifesto, the “intelligence stage,” which is where the world is headed now, is about people, devices and systems making handshakes, connecting, processing information and providing services: “Whereas the hallmark of the access stage was the sharing of information, the intelligence stage may be considered as far more person and data centric rather than tool [application] centric.”³

Data Security by Design

Privacy by Design provides great guidance to everyone involved in protecting data today with the following 6 foundational principles:

1. Proactive, not reactive; preventive, not remedial
2. Privacy as the default setting
3. Privacy embedded into design
4. End-to-end security
5. Visibility and transparency
6. Respect for user privacy

Proactive, Not Reactive

To move from a reactive to proactive mode needs foresight with regard to data use. Privacy should not be an afterthought and data security needs to be related to the use of information, meaning that enterprise security requirements should worry about data at all touch points. Part of this means that organizations need to become internally and externally focused on what data security and privacy mean to them and consider the entire data flow. It cannot be stressed enough how much information is input and output between multiple applications and not just between people; therefore, once data flows have been mapped, CIOs need to create and manage access and use according to clearly defined data security policies.

Privacy as the Default Setting
Enterprises need to start acting more like the military and compartmentalize data access. They also need to set privacy protection as the default setting even before building more finely grained access control. In terms of providing access, CIOs ask many questions in advance of data owners, such as: What can happen if data are exposed? What are the financial liabilities of such exposure? And what about reputational impact? By asking these questions, appropriate safeguards can be made up front with the shared development of privacy policies by IT and the business, combined with technical solutions.

**Embedded Into Design**
Privacy should proactively be built into projects and processes from the start rather than initiated as a response to an audit finding or new compliance requirement. Privacy is best when it is “baked in” from inception vs. bolted on later. Privacy design needs to occur during the requirements gathering and design phase of a project, like quality assurance (QA).

**End to End**
Today, data protection is bigger than any one project or application and needs to consider the use of information wherever it goes. The emphasis needs to be placed on creating requirements that relate to the data as well as all data touch points. Doing this well means discovering where all data exist within enterprises so they can be thoroughly accounted for and protected appropriately. One CIO said recently, “Organizations need to collect only as much information as is required, store it only as long as it needs to be stored and anonymize as much of it as you can, and do this in an automated, policy based fashion.” While this makes sense, there is risk in thinking about protecting data in a piecemeal fashion. Data protection governance needs a composite view of systems as a whole; otherwise, compliance and governance holes will exist. Data need to be protected everywhere, all the time—unauthorized users or hackers need to find only one weak point in the data flow to exploit it.

**Visibility and Transparency**
Transparency about the collection and use of data is a part of privacy by design that is essential to data subject trust as well as compliance. Organizations need privacy policies that hold business units accountable for information usage and processing. It is considered vital for organizations to implement data governance that provides visibility and control over data wherever they go and at all times.

**Respect for User Privacy**
Finally, organizations need to make data security and privacy business priorities and be clear, both internally and externally, what privacy means while integrating it into enterprise culture and management. Part of this process is establishing explicit data owners and involving them in the implementation of policies that have, at their core, respect for the sources of personally identifiable information (PII). This involves encouraging data subjects to actively manage their own data by offering consent, accuracy and access, then “determining which elements make a collection of information personal or identifying” and may need to be depersonalized or deidentified.

**What Else Is Needed?**
The world consists of complex business ecosystems, where ensuring data security and regulatory compliance will be increasingly difficult if ad hoc application or environment-centric data protection continues. Data protection needs to enable everyone involved with data—from the data stewards creating policies governing access and use of data, to the chief information security officer (CISO) securing and protecting data assets and the analysts seeking data insights—to securely perform their duties. Organizations need the ability to seamlessly enforce security policies across the enterprise to protect sensitive data and control access to those data, regardless of where the data flow, how they are used or where they rest.

In this cloud-first era, data protection needs to move from the perimeter to the data and points of use to be effective. In a world with only virtual boundaries, security needs to shift from the systems to the data as they move to and from all forms of cloud services.

Data privacy and security policies need central management to ensure data protection is consistently applied wherever
data flow. Application-by-application security and privacy no longer work because of the blurring of network boundaries and free flow of data from machine to machine and system to system. Taking this step is the only way that organizations can consistently protect sensitive information throughout its entire life cycle.

Today, data protection capabilities are needed that can, depending upon required access, make sensitive data fully visible, partially visible or completely protected, depending on each user’s role in the organization. This permits the analysis of protected health information (PHI) and PII data while preserving privacy and security for all applications and parties. The foundation for protecting sensitive information is the data security policies each organization creates. These should be based on data security business cases and answer, at minimum, the following business questions:

- What data shall be protected?
- Who shall have access to the data?
- Which days and times shall the data be accessible?
- Where in the enterprise shall the policy be enforced?
- Who will undertake audit of access and process attempts? To what data, where and when?

Today's enterprises need to seamlessly integrate and protect sensitive data within all existing business applications and business processes. They need to allow authorized personnel appropriate, quick and easy access to critical data (security of inclusion), while ensuring internal or external unauthorized users do not have access to data (security of exclusion). Enterprises increasingly need to provide equal defense against insider threats, external attacks and data privacy violations.

**Good Security Governance Takes Time and Effort**

COBIT 5 recommends that organizations take specific actions to govern and protect their data and information and provides a set of IT-enabling processes for information and data governance. Some enterprises may already be using some, if not all, of the COBIT 5 process recommendations. For those that are not, this article lays out a set of steps that enterprises can take to better govern and manage information and recommends additional steps to move from application-centric to data-centric protection.

As with most improvement methodologies, the key is to start by taking one step at one time—Rome was not built in a day and neither is good data governance. The point is to start the improvement journey today. COBIT provides sound and comprehensive improvement recommendations to kick things off, but organizations clearly need to move beyond reactive compliance and security to a more proactive stance by mandating the need for data privacy and security to be enterprisewide. In other words, data must be protected consistently wherever they flow.

**Myles Suer, ITIL**

Is a director of solutions and industry marketing at Protegrity. He was recently named the number 9 influencer of CIOs on Twitter by Leadtail Insights. Much of his experience has been as a business intelligence (BI) practitioner. Suer worked at Hewlett Packard and Peregrine, where he led the product management team applying BI and scorecard technology to IT management products. Prior to HP, he led new product initiatives at start-ups and large companies. This included a restart of a business activity monitoring company. He has also been employed as a software industry analyst.

**Les McMonagle, CISA, CISSP, ITIL**

Has more than 20 years of experience in information security. He has held the position of CISO for a credit card company and Industrial Loan Company Bank, founded a computer training and IT outsourcing company in Europe, directed the security and network technology practice for Cambridge Technology Partners across Europe and helped several security technology firms develop their initial product strategy. McMonagle founded and managed Teradata’s Information Security, Data Privacy and Regulatory Compliance Center of Excellence and is currently chief security strategist at Protegrity.
Endnotes

1 Jack Gold, Principal Analyst and Founder, J. Gold Associates, #CIOChat, Twitter feed, 28 April 2016
2 Josh Olson, Chief Information Officer, Michigan Technological University, USA, #CIOChat, Twitter feed, 18 August 2016
3 Dennedy, M.; J. Fox; T. Finneran; The Privacy Engineer’s Manifesto, Appress, USA, 2014
4 Ryan Fay, ACI Specialty, #CIOChat, Twitter feed, 7 July 2016
5 Op cit Dennedy, Fox and Finneran