Implementation of Service Integration in a Multiprovider Environment Using COBIT 5

By Martin Andenmatten, CISA, CGEIT, CRISC, ITIL Master

COBIT Focus | 28 September 2015

English | French | German | Portuguese | Spanish

We are living in a constantly changing world. While technology is getting smarter and easier to handle for users, governance and management of enterprise IT (GEIT) is becoming overly complex. Increasingly, cloud services are replacing traditional in-house solutions, and the risk associated with this new IT business model is difficult to manage. The role of the internal IT department is being questioned because its value is often not recognized at the board level. Because businesses can access IT services relatively easily via a cloud broker portal, long lasting program and project management is no longer needed for delivering equal services at unknown cost, time and risk. Well, we are not there yet, but the pathway is clear.

COBIT® 5 promotes the concept of differentiating governance and management. While appropriate, this approach does add to the challenge of knowing how to govern and manage these split, shared and distributed service towers (e.g., desktop, infrastructure, platform and application towers) from different vendors in order to fulfill the expectation regarding benefit realization, risk optimization and resource optimization. It will be even more interesting to see how this can be managed when there is not just a single service provider anymore, but many service providers, each delivering only parts of a service. The combination of providers is constantly changing through adding or removing service parts by the business process owners. The COBIT 5 Services, Infrastructure and Applications enabler is no longer a holistic delivery unit with a clear supply chain. It is more a compilation of service towers from independent service providers within a supply network. For example, how can availability or capacity requirements be ensured and managed end to end? How will incidents and problems be coordinated among the different suppliers? How will security operations and cyberresilience be ensured when service partners are dynamically changing? Is a dedicated supplier management process with contracting and monitoring activities sufficient for overlooking the whole situation and ensuring compliance? Is service orchestration and automation the only solution and should we rely primarily on trust that everything will work just fine? Do we need a much stronger governance and management system in such an agile and ever-changing supplier landscape? And what should that look like?

COBIT 5 is still the basic framework for building a governance and management system in a multivendor and extensive cloud service environment.

COBIT 5 is still the basic framework for building a governance and management system in a multivendor and extensive cloud service environment. ISACA® has published several different COBIT 5 practical guidance volumes; *Vendor Management Using COBIT® 5* and *Controls and Assurance in the Cloud: Using COBIT® 5* are especially suited for use in this context. But neither publication takes into account the dynamics that have to be considered when governing and managing such an environment. A service integration concept is needed, which supports the shift to shorter contracts and the increased push toward the use of sourcing and cloud services from multiple external sourcing partners.

Today, such a model exists: Service Integration and Management (SIAM). This is a concept with a clear role of providing overall direction, management and coordination for the delivery of end-to-end IT services. SIAM is not a new framework, but since the typical best-of-breed approach in evaluating service partners is leading to a lack of interoperability and portability and difficulties in coordination of service issues, the framework is increasingly used in service management environments. It helps to build the capabilities required to get control over the entire service delivery network. And it is a great opportunity for internal IT organizations to reposition their role and play their part between the business and the various suppliers as the custodian for the management body of IT-related inquiries within the enterprise. This is very important in order to keep the accountability of processes and services within the organization.

SIAM is not a tool and not a process. It is more of a fundamental capability for a target operation model in order to be able to reflect the particular requirements of the business units and the particular nature of the supplier landscape. In order to efficiently manage service integration within an organization, it is useful to use the COBIT 5 structure with the 7 enablers and adapt it to the special requirements.

COBIT 5 Enabler: Policies, Principles and Frameworks

Clear policies and direction are needed to define how external cloud services and sourcing providers are brought into an organization. Moreover, there must be defined service design standards that clearly describe the interfaces, roles and responsibilities within the service ecosystem. When an end-to-end service warranty has to be delivered, it is essential to have all partners on the same page. It is necessary to clarify how priorities are handled and escalation is invoked.

SIAM needs to build clear policies and principles that define service integration standards. Even when it has to be accepted that different partners are using different tools and process definitions, a minimum set of requirements describing the principles of working together has to be defined.

As is the nature of outsourcing and cloud sourcing services, parts of processes will be managed at the supplier site (**figure 1**). However, the end-user organization is still accountable for service outcome, cost and risk. A clear policy and direction with the authority to require adherence to each management process has to be in place, e.g., establishing the information security policy, using controls, detecting breaches and initiating corrective actions.

Figure 1—Process Domains
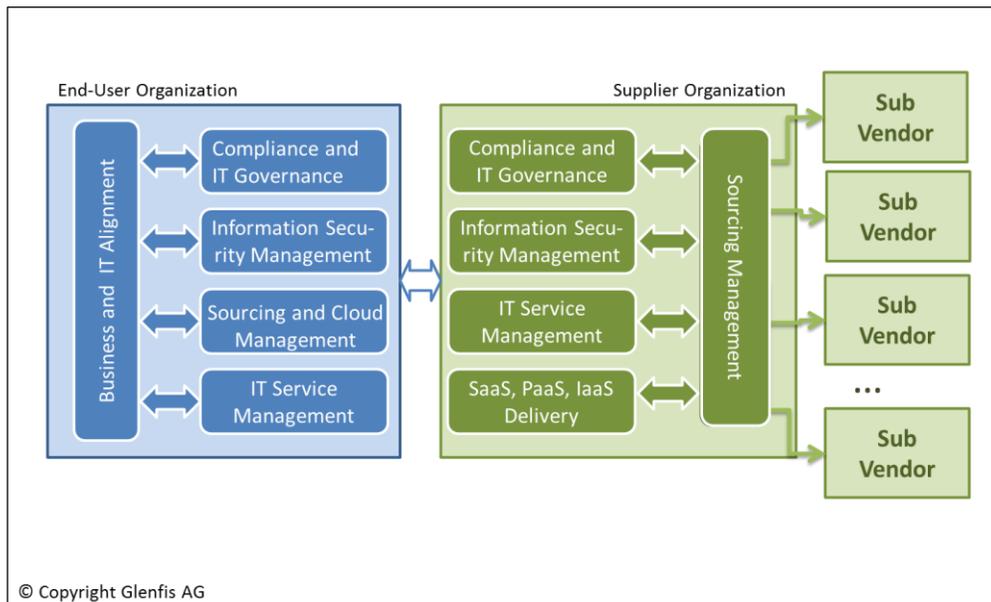
Source: Glenfis AG. Reprinted with permission.

COBIT 5 Enabler: Processes

Process practices and activities are the most important vehicles for executing policies and directives. It is known that organizations need an overall process owner who is accountable for all process activities end to end. In a multivendor environment, it has to be taken into account that every supplier will have a corresponding process owner on its side who is acting according to his/her responsibilities as well. For example, a problem manager from the end-user organization needs to coordinate definitions and process activities with each corresponding process owner from the critical service provider.

In a multiprovider environment, there are service integration and management systems to be built up. There are specific core components needed, as illustrated in **figure 2**, with the purposes coordinating work between the different stakeholders involved. For example "Service Design" becomes a core component in defining the process and tool standards and interfaces for suppliers to work with the customer.

Figure 2—SIAM: Components and Process Landscape
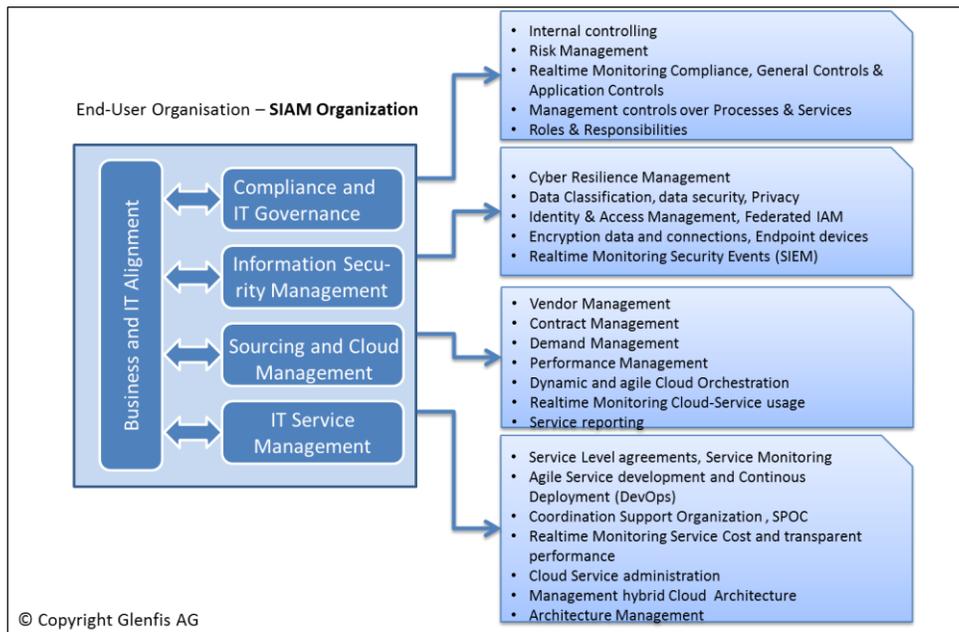
SIAM – Components and Process Landscape
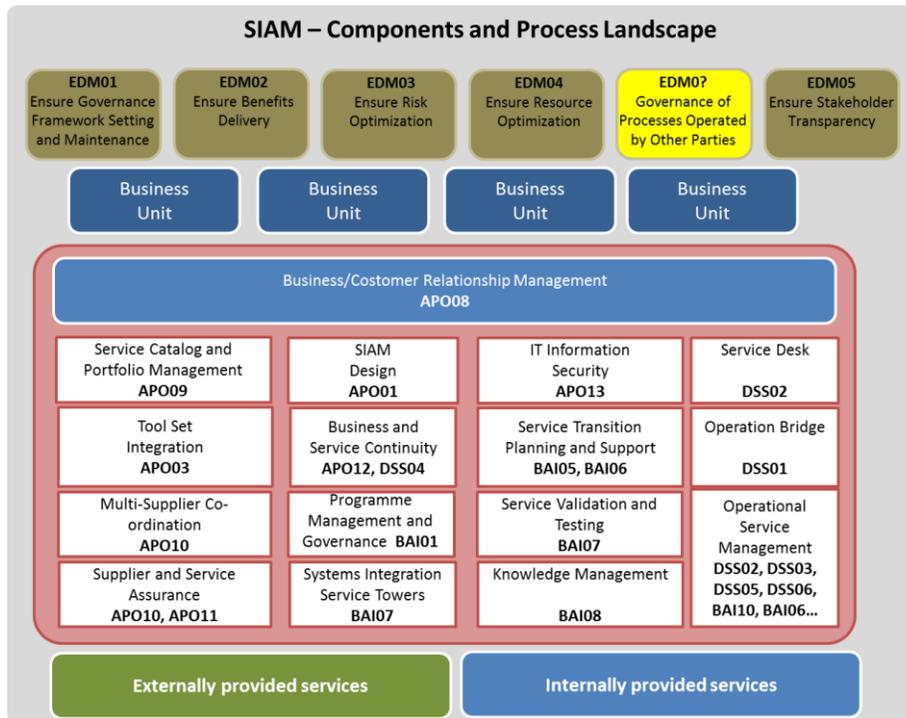
Source: Glenfis AG. Reprinted with permission.

As such, a clear picture of all involved service partners has to be painted within the service portfolio and service catalog (APO09). Different definitions of priorities, classification schemes, service levels or information handover have to be defined within the service design framework (APO01).

COBIT 5 Enabler: Organizational Structures

As service integration is a specific capability with specific skills in coordination, supplier and contract management, and relationship building with all involved parties, it is advisable to establish a specific SIAM team. This team can coach or even take over some accountabilities for process coordination and consistent service reporting. It can act as a knowledge pool for governance and management processes and defining service integration standards (**figure 3**).

Figure 3—Organization and Processes Within the SIAM Concept

End-User Organisation – **SIAM Organization**

Business and IT Alignment

- Compliance and IT Governance
- Information Security Management
- Sourcing and Cloud Management
- IT Service Management

- Internal controlling
- Risk Management
- Realtime Monitoring Compliance, General Controls & Application Controls
- Management controls over Processes & Services
- Roles & Responsibilities

- Cyber Resilience Management
- Data Classification, data security, Privacy
- Identity & Access Management, Federated IAM
- Encryption data and connections, Endpoint devices
- Realtime Monitoring Security Events (SIEM)

- Vendor Management
- Contract Management
- Demand Management
- Performance Management
- Dynamic and agile Cloud Orchestration
- Realtime Monitoring Cloud-Service usage
- Service reporting

- Service Level agreements, Service Monitoring
- Agile Service development and Continous Deployment (DevOps)
- Coordination Support Organization , SPOC
- Realtime Monitoring Service Cost and transparent performance
- Cloud Service administration
- Management hybrid Cloud Architecture
- Architecture Management

© Copyright Glenfis AG

Source: Glenfis AG. Reprinted with permission.

As such, a SIAM function can be in-house or delivered from a specific SIAM provider. This article suggests that this team should remain with the end-user organization because the core of coordination and management work is done there. But if the necessary skills and experience cannot be found in-house, outsourcing is always an option.

COBIT 5 Enabler: Culture, Ethics and Behaviour

As always, people run the processes and make everything happen. A supportive and open-minded culture is needed for building effective personal relationships at all levels among process owners, service owners, the SIAM team and the suppliers, where ever they are located. There should be regular one-to-one meetings between the corresponding process and service owners.

In the end, this helps to build a supportive and collaborative work environment across the suppliers and aids in building a value network within the service delivery landscape.

COBIT 5 Enabler: Information

Information is crucial. Information must flow between the end-user organization and the suppliers. Incidents, events, changes, known errors and service achievements have to be transparent and easily accessible. The service design as discussed under Enabler Processes will deliver the standards and interfaces between the involved parties.

COBIT 5 Enabler: Services, Infrastructure and Applications

Because IT services are a combination of different service towers delivered by internal and external suppliers, a good service architecture based on an architecture development method (ADM) (e.g., in **The Open Group Architecture Framework** [TOGAF]) should be implemented. The service design standards should be part of such a model.

A big challenge is collaboration among the different tools used by the different suppliers. It is wishful thinking to ask the suppliers to use the same tool the end-user organizations use and it would drive increased costs. It is challenging enough to get some technical integration of the different tool sets based on standard interfaces. More challenging is the definition of common information standards for the interchange (severity level, priorities, process

status, etc.) (**figure 4**).

Figure 4—The SIAM Tool Set As the Enterprise Resource Planning Tool for Internal IT
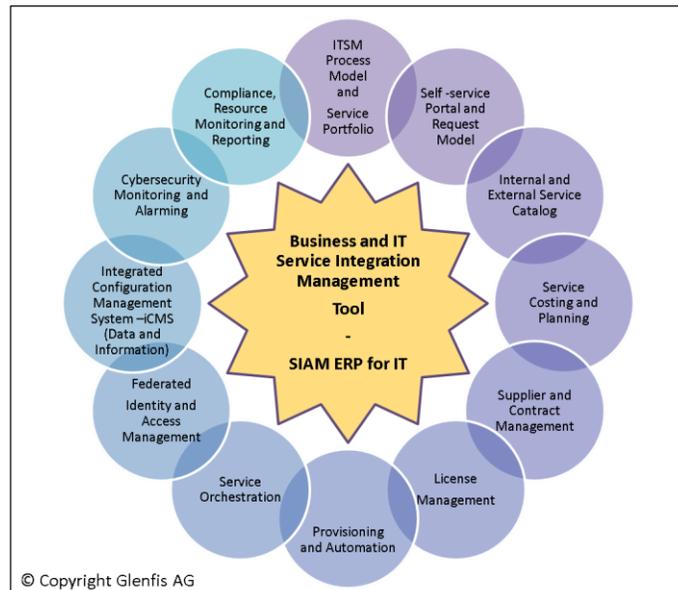
Source: Glenfis AG. Reprinted with permission.

COBIT 5 Enabler: People, Skills and Competencies

The SIAM key staff needs to be at least as qualified and knowledgeable in GEIT services and related techniques as the supplier's staff. This is crucial for being able to effectively design and govern the processes and activities. In addition to technical and process skills, soft skills will be needed, especially in:

- Relationship management
- Conflict management
- Influence
- Negotiation
- Stakeholder management

The key SIAM staff will spend most of its time with the supplier staff, outside of direct internal management control. The existence and maturity of these soft skills will be critical for successful SIAM implementation.

Implementation and Transition to a New SIAM Operation Model

Similar to implementation of a governance and management system, the SIAM target operation model will be an organizational change that has to be treated as a business change. The 7-step implementation model of COBIT 5 can be used as a guideline, but a detailed SIAM model must be fully understood in order to define the vision and the target state.

Author's Note

More Information about SIAM can be found in 2 white papers by Axelos:

- *An Introduction to Service Integration and Management and ITIL*
- *An Example ITIL-based Model for Effective Service Integration and Management*

Martin Andenmatten, CISA, CGEIT, CRISC, ITIL Master

Is founder and managing director of Glenfis AG, a consulting and training organization located in Switzerland. He and his team help organizations build their sourcing and service management strategies and support them in the selection and transition phase. He leads demanding sourcing and service management programs for a range of customers. Since 2002, he has also been a course instructor in ITIL, ISO 20000 and COBIT and Sourcing Governance. As an editor and writer, he has described his practical experience in the books *ISO 20000: Praxishandbuch für Servicemanagement und IT-Governance – Managing Services with ITIL* (*Practical Handbook for Service Management and IT Governance – Managing Services with ITIL*) and *COBIT 5 Grundlagen* (*COBIT 5 Basics*).