Developing a Governance Framework for the Global Support Organisation at GlaxoSmithKline, Using COBIT

By Steve Williamson

Like most innovation-led organisations, GlaxoSmithKline (GSK) is highly dependent on IT. Its large, centralised IT support group has used COBIT\textregistered\ 4.1 as the basis for developing an organisational IT governance framework. GSK is beginning its transition to COBIT\textregistered\ 5.

The mission of GSK is ‘to improve the quality of human life by enabling people to do more, feel better and live longer’. In support of this mission, GSK develops and makes pharmaceuticals to treat a range of conditions including respiratory diseases, cancer, heart disease and epilepsy. GSK researches and makes vaccines that protect against infectious diseases, including influenza, rotavirus, cervical cancer, measles, mumps and rubella. It makes innovative consumer health care products, with a portfolio that includes well-known brands such as Horlicks, Panadol and Sensodyne. GSK is a global company operating in more than 115 countries with approximately 100,000 employees.

One of GSK’s strategic priorities is to simplify its operating model by reducing complexity and thereby becoming more efficient. This will free up resources to invest in other, more productive, areas of the business. One of the outcomes of this strategy is a more centralised IT organisation, offering standard IT support services to all business areas.

The application support group was formed by merging a number of autonomous, business-facing IT groups and is responsible for a portfolio of more than 2,000 applications supporting every stage of the value chain (research, development, manufacturing, commercial and corporate functions). This department has several hundred permanent staff, based at different locations worldwide. Additional technical support is provided from two offshore business partners.

The application support department has developed a governance framework for GSK.

Governance for an IT Support Function

Shortly after the formation of the new global support department, the need for an evaluation of governance processes was identified. The aim was to verify that the newly formed organisation has the right structures, processes and controls in place to enable successful execution of its strategy, and to ensure alignment with the enterprise strategy.

Organisational governance is a commonly accepted management term, which most people loosely understand. However, trying to define precisely what IT governance is and how it applies to an IT organisation is in itself a challenge. Thus, reference to commonly accepted industry frameworks is useful. In this case, GSK’s application support department utilized COBIT\textregistered\ (version 4.1 was used for this exercise).

ISACA defines IT governance as, ‘The responsibility of executives and the board of directors; consists of the leadership, organizational structures and processes that ensure that the enterprise’s IT sustains and extends the enterprise’s strategies and objectives’.¹

Why COBIT?

One of the advantages of COBIT 4.1 is that it is a framework that is strongly focused on control rather than execution. It covers a broad range of governance areas (e.g., human resources, finance, strategic alignment, risk management, service
management) and can be mapped to other industry standards, such as ISO 27001 for security and ITIL for service management, which made it a good fit for GSK.

How GSK Used COBIT 4.1

COBIT 4.1 is comprehensive, yet simply structured, with each process area sub-divided into process description, control objectives, management guidelines and maturity models. This makes it easy to select the processes that are most applicable to the organisation’s goals and ignore those that are either not relevant or of lesser importance. For example, the COBIT processes PO2 Define the information architecture and PO3 Determine technological direction are the primary responsibility of another department within the enterprise, so these were excluded from the application support department’s framework, and other COBIT 4.1 processes had only partial applicability.

The application support department took the following steps to create its governance framework:

1. Identify the applicable process areas from COBIT 4.1.
2. Identify the applicable control objectives within each process area.
3. Perform the risk assessment, i.e., ascertain the impact to the organisation of control failures in each process.
4. Identify which existing processes, procedures or working practices address this process area, and evaluate against the control objectives.
5. Review with subject matter experts and senior management, including those responsible for implementing the controls.
6. Document any gaps or weak controls, describing the risk and input this information into the relevant process improvement work stream.

When control weaknesses are identified, it normally indicates that a policy is not being implemented effectively. This identifies the need for corrective action, which is the responsibility of management. This type of analysis could reveal a more fundamental problem, such as a previously unrecognised or an inadequately mitigated risk. In such a situation, the corrective action would be changes to the policy framework. Such actions would not be addressed by management, but by the compliance board. This could result in new or amended policies and/or decisions relating to the risk tolerance.

The governance framework is structured by IT governance focus areas (mapped to COBIT process areas) and includes the following:
- IT organisation and relationship governance
- The strategic alignment of business and IT objectives
- Quality, risk and control policies framework
- Communications, training and knowledge management
- Investment portfolio, financial management and value delivery governance
- System development, deployment and maintenance
- Third-party services/supplier management

For each governance focus area, control objectives, key risk factors and implementation were defined (figure 1).

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control objectives</td>
<td>These were taken directly from COBIT 4.1. Applicable control objectives were selected (excluding those that had only a tenuous association).</td>
</tr>
<tr>
<td>Key risk factors</td>
<td>This is the analysis of organisational impacts from failure to effectively meet control objectives. Example risk impacts include operational inefficiencies, increased likelihood of security breaches, regulatory failure and legal penalties.</td>
</tr>
<tr>
<td>Implementation</td>
<td>This section described the procedures, controls and organisational structures that were currently in place and addressed the control objectives. This revealed gaps and weaknesses.</td>
</tr>
</tbody>
</table>

One may ask, why go to the trouble of creating a separate document rather than using the COBIT material directly? The reason is that having a framework with familiar business context allows it to be more intuitive to those who need to use it. Its purpose is to evaluate GSK’s processes against a commonly accepted standard for governance, not to redefine metrics or introduce new ways of working. This ensured the document is meaningful to a wide range of people, most of whom have little or no experience using COBIT.
Findings and Derived Value

Control objectives can be met by a procedure (e.g., change control process) or through effective organisational structures (e.g., representation on leadership teams), which clearly demonstrated accountability and control. However, during the analysis, the application support department found that some control objectives are being effectively met through nonprocedural methods. Although less formal than a management-approved procedure, most of these methods were documented or implied as part of job descriptions, thus demonstrating accountability.

Determining whether or not a procedure addresses the needs of the control objective is relatively easy. Judging the overall effectiveness of a procedure across a newly consolidated IT department is more difficult without extensive data gathering or audit. As a means of addressing this, newly implemented monitoring activities were used to assess the effectiveness of the mitigation techniques and they were the key source of information, making possible ongoing programme improvement.

In 2013, a department-wide governance audit was performed. This framework document was the basis for audit preparedness. It did not cover everything the auditors assessed, but it helped demonstrate the adequacy of the controls structures in place.

Next Steps

The framework gives a point-in-time evaluation of the application support department’s controls and allows for the identification of threats, vulnerabilities and inefficiencies, risk factors, and issues (which would have otherwise gone unnoticed). It will be maintained in line with organisational changes (e.g., if the organisation starts to offer a broader range of IT services, the framework can easily be expanded).

The next evolution of this governance model will include process capability assessment models for key process areas. The COBIT 5 process assessment model will be the basis for designing and implementing these models. This also marks the transition to COBIT 5. The process areas selected for capability assessments are those that would have the greatest risk impact if they failed to operate effectively. As before, the models will be based on COBIT, but will reference GSK’s metrics and processes. The first step is to perform a baseline assessment to determine current maturity levels, and then long-term improvement objectives will be established to ensure continued process improvement over the next five years.

Steve Williamson

Is the director, IT risk management, at GlaxoSmithKline, responsible for information security, regulatory compliance and quality management. Williamson started his IT career 25 years ago as a software tester in the banking industry. Williamson has been with GSK for the last 16 years in various project management and governance, risk and compliance roles.

Endnotes

1 ISACA, Glossary

©2014 ISACA. All rights reserved.