system design.

Chapter 9

Getting Started With COBIT: Making the Case

9.1 Business Case

Common business practice dictates preparing a business case to analyze and justify the initiation of a large project and/or financial investment. This example is provided as a nonprescriptive, generic guide to encourage preparation ofa business case to justify investment in an EGIT implementation program. Every enterprise has its own reasons forimproving EGIT and its own approach to preparing business cases. This can range from a detailed approach with anemphasis on quantified benefits to a more high-level and qualitative perspective. Enterprises should follow existinginternal business case and investment justification approaches, if they exist. This example and the guidance in thispublication in provided to help focus on the issues that should be addressed in a business case.

The example scenario is Acme Corporation, a large multinational enterprise with a mixture of traditional, well-established business units as well as new Internet-based businesses adopting the very latest technologies.Many of the business units have been acquired and exist in various countries with different local political,cultural and economic environments. The central group's executive management team has been influenced bythe latest enterprise governance guidance, including COBIT, which they have used centrally for some time.They want to make sure that rapid expansion and adoption of advanced IT will deliver the value expected;they also intend to manage significant new risk. They have, therefore, mandated enterprisewide adoption of auniform EGIT approach. This approach includes involvement by the audit and risk functions and internalannual reporting by business unit management of the adequacy of controls in all entities.

Although the example is derived from actual situations, it does not reflect a specific, existing enterprise.

9.2 Executive Summary

This business case outlines the scope of the proposed EGIT program for Acme Corporation based on COBIT.

A proper business case is needed to ensure that the Acme Corporation board and the business units buy in to the initiative and identify the potential benefits. Acme Corporation will monitor the business case to ensure that the expected benefits are realized.

The scope, in terms of business entities that make up Acme Corporation, is all inclusive. It is acknowledged that some form of prioritization will be applied across all entities for initial coverage by the EGIT program due to limited program resources.

Various stakeholders have an interest in the outcomes of the EGIT program, from the Acme Corporation board of directors to local management at each entity, as well as external stakeholders such as shareholders and government agencies.

Consideration needs to be given to some significant challenges, as well as risk, in the implementation of the program on the required global scale. One of the more challenging aspects is the entrepreneurial nature of the Internet businesses, as well as the decentralized, or federated, business model that exists within Acme Corporation.

EGIT prioritized governance and management objectives that will receive focus at each entity will be identified

through athe governance system in relation to those that are defined in COBIT, relevant to each business unit. The

relevant andThe EGIT program will be achieved by focusing on the capability of the Acme processes and other

components of facilitated workshop approach by the members of the EGIT program. The objectives will start with

the strategy andenterprise goals of each unit, as well as the IT-related business risk scenarios that apply to the

specific business unit.

The objective of the EGIT program is to ensure that an adequate governance system, including governancestructures, is in place and to increase the level of capability and adequacy of the relevant IT processes. Theexpectation is that as the capability of an IT process increases, so too will its efficiencies and quality. Simultaneously,the associated risk will proportionally decrease. In this way, real business benefits can be realized by each businessunit.

Once the process of assessing the capability level within each business unit has been established, it is anticipated thatself-assessments will continue within each business unit as normal business practice.

The EGIT program will be delivered in two distinct phases. The first phase is a development phase, in which the team will develop and test the approach and tool set that will be used across the Acme Corporation. At the end of phase 1, the results will be presented to group management for final approval. Once the final approval has been obtained, in the form of an approved business case, the EGIT program will be rolled out across the entity in the agreed manner (implementation, phase 2).

It must be noted that it is not the responsibility of the EGIT program to implement the remedial actions identified at each business unit. The EGIT program will merely consolidate and report progress as supplied by each unit.

The final challenge that will need to be met by the EGIT program is that of reporting the results in a sustainable manner going forward. This aspect will take time and a significant amount of discussion and development. This discussion and development should result in an enhancement to the existing corporate reporting mechanisms and scorecards.

An initial budget for the development phase of the EGIT program has been prepared. The budget is detailed in a separate schedule. A detailed budget will also be completed for phase 2 of the project and submitted for approval by group management.

9.3 Background

EGIT is an integral part of overall enterprise governance and is focused on IT performance and the management of risk attributable to the enterprise's dependencies on IT.

IT is integrated into the operations of Acme Corporation businesses. For many, the Internet is at the core of their operations. EGIT, therefore, follows the management structure of the group: a decentralized format. Management of each subsidiary/business unit is responsible for ensuring that proper processes are implemented relevant to EGIT.

scheduled meeting of the appropriate risk committee.has implemented the EGIT policy during the financial year. Significant exceptions are to be reported at eachappropriate risk committee, which is a subset of the board of directors. This report will detail the extent to which itAnnually, the management of each significant subsidiary company is required to submit a formal written report to the

management of each significant subsidiary company. It will provide both internal and external stakeholders withThe

statement will be based on reports obtained from the risk, compliance and internal audit teams and theassessed,

monitored, reported and disclosed in an EGIT statement as part of the enterprise's integrated annual report.The board

of directors, assisted by the risk and audit committees, will ensure that the group's EGIT performance is relevant and

reliable information about the quality of the group's EGIT performance.

effectiveness of EGIT.Internal audit services will provide assurance to management and to the audit committee on the adequacy and IT-related business risk will be reported on and discussed as part of the risk management process in the risk registerspresented to the relevant risk committee.

9.4 Business Challenges

Due to the pervasive nature of IT and the pace of technology change, a reliable framework is required to adequatelycontrol the full IT environment and avoid control gaps that may expose the enterprise to unacceptable risk.

The intention is not to impede the IT operations of the various operating entities. Instead, it is to improve the riskprofile of the entities in a manner that makes business sense and provides increased quality of service andefficiencies, while explicitly achieving compliance not only with the Acme Corporation's group EGIT charter, butalso with any other legislative, regulatory and/or contractual requirements.

Some examples of likely pain points include:[25]

- Complicated IT assurance efforts due to the entrepreneurial nature of many of the business units
- Complex IT operating models due to the Internet service-based business models in use
- Geographically dispersed entities made up of diverse cultures and languages
- The decentralized/federated and largely autonomous business control model employed within the group
- Implementation of reasonable levels of IT management, given a highly technical and, at times, volatile ITworkforce
- IT's balancing of the enterprise's drive for innovation capabilities and business agility with the need to manage riskand have adequate control
- The setting of risk and tolerance levels for each business unit
- An increasing need to focus on meeting regulatory (privacy) and contractual (Payment Card Industry [PCI])compliance requirements
- Regular audit findings about poor IT controls and reported problems related to IT quality of service
- Successful and on-time delivery of new and innovative services in a highly competitive market

9.4.1 Gap Analysis and Goal

There is currently no groupwide approach or framework for EGIT or use of IT good practices and standards.

Among local business units, there are variable levels of adoption of good practice with regard to EGIT. As a result, very littleattention has traditionally been paid to the level of IT process capability. Based on experience, the levels aregenerally low.

processes and controls appropriate to each business unit, in a prioritized manner.The objective of the EGIT program is, therefore, to increase the level of capability and adequacy of IT-related

proportionally as well and the IT-related business risk profile of each entity should decrease.and report on its status. As the capability level of each business unit increases, quality and efficiency should increase The outcome should be that significant risk has been identified and articulated, and management can address the risk

Ultimately, business value should increase as a result of effective EGIT.[26]

[2526] This enumeration is a subset of the one in section 4.5 (Design Factors) and is also discussed in the Empirical research exists to support the statement. For example, see *op cit* De Haes, Joshi and van Grembergen.*COBIT® 2019 Implementation Guide*.

9.4.2 Alternatives Considered

Many IT frameworks exist, each intended to control specific aspects of IT. The COBIT framework is regarded by many as the world's leading EGIT and control framework. It has already been implemented by some subsidiaries ofAcme Corporation.

COBIT was chosen by Acme as the preferred framework for EGIT implementation and should, therefore, be adoptedby all subsidiaries.

COBIT does not have to be implemented in its entirety; only those areas relevant to the specific subsidiary orbusiness unit need to be implemented, taking into account the following:

1. The development stage of each entity in the business life cycle
2. The business objectives of each entity
3. The importance of IT for the business unit
4. The IT-related business risk faced by each entity
5. Legal and contractual requirements **6.** Any other pertinent reasons

If a specific subsidiary or business unit has already implemented another framework, or an implementation is planned in the future, the implementation should be mapped to COBIT for reasons of reporting, audit and clarity ofinternal control.

9.5 Proposed Solution

The EGIT program is being planned in two distinct phases.

9.5.1 Phase 1. Pre-planning

Phase 1 of the EGIT program is the development stage. During this stage of the program, the following steps areundertaken:

1. The core team structure is finalized among the stakeholders and participants on the project.
2. The core team completes COBIT foundation training.
3. Workshops with the core team are conducted to define an approach for the group.
4. An online community is created within Acme Corporation to act as a repository for knowledge sharing.
5. All stakeholders and their needs are identified.
6. and realigned, if required. Current committee structures, roles and responsibilities, decision rules, and reporting arrangements are clarified
7. implementation of the program.A business case for the EGIT program is developed and maintained, as a foundation for the successful
8. A communication plan is created for guiding principles, policies and expected benefits throughout the program.
9. The assessment and reporting tools for use during the life of the program and beyond are developed.
10. the approach and tools. The approach is tested at one local entity. This activity is for ease of logistics and to facilitate the refinement of
11. running the EGIT program assessment phase under more challenging business conditions. The refined approach is piloted at one of the foreign entities. This is to understand and quantify the difficulties of
12. The final business case and approach are presented, including a roll-out plan to Acme Corporation executivemanagement for approval.

9.5.2 Phase 2. Program Implementation

The EGIT program is designed to start an ongoing program of continual improvement, based on a facilitated,iterative life cycle by following these steps:

1. Determine the drivers for improving EGIT, from both an Acme Corporation group perspective and at thebusiness unit level.

2. Determine the current status of EGIT.
3. Determine the desired state of EGIT (both short- and long-term).
4. Determine what needs to be implemented at the business unit level to enable local business objectives, andthereby align with group expectations.
5. Implement the identified and agreed improvement projects at the local business unit level.
6. Realize and monitor the benefits.
7. Sustain the new way of working by keeping the momentum going.

9.5.3 Program Scope

The EGIT program will cover:

1. All of the group entities. However, the entities will be prioritized for interaction due to limited programresources.
2. The method of prioritization. It will need to be agreed with Acme Corporation management, but could be doneon the following basis: **a.** Size of investment
   b. Earnings/contribution to the group
   c. Risk profile from a group perspective
   d. A combination of these criteria **3.** The list of entities to be covered during the current financial year. This should be finalized and agreed withAcme Corporation management.

9.5.4 Program Methodology and Alignment

entities.The EGIT program will achieve its mandate by using a facilitated, interactive workshop approach with all the outcomes and priorities.officer (CFO). This approach should ensure that the program outcomes are closely aligned to the expected businessThe approach starts with the business objectives and the objective owners, typically the CEO

and chief financial IT-related business risk and objectives are considered.chief technology officer (CTO) or chief

information officer (CIO). At the IT operations level, further details of theOnce the business objectives have been

covered, the focus shifts to IT operations, typically under the control of the The business and IT objectives, as well as

the IT-related business risk, are then combined in a tool (based on COBIT guidance) that will provide a set of focus

areas within the COBIT processes for consideration by the business unit. Inthis fashion, the business unit can

prioritize its remediation efforts to address the areas of IT risk.

9.5.5 Program Deliverables

As mentioned earlier, an overall goal of the EGIT program is to embed the good practices of EGIT into thecontinuing operations of the various group entities.

Specific outcomes will be produced by the EGIT program to enable Acme Corporation to gauge the delivery of theintended outcomes. These include the following:

1. The EGIT program will facilitate internal knowledge sharing via the intranet platform and leverage existingrelationships with vendors to the advantage of the individual business units.

2. Detailed reports on each facilitation with the business units will be created derived from the EGIT programassessment tool. The reports will include:

   a. The current prioritized business objectives, and consequent IT objectives, based on COBIT

   b. The IT-related risk identified by the business unit in a standardized format, and the agreed focus areas forattention by the business unit based on COBIT processes and practices and other recommended components

3. Overall progress reports on the intended coverage of the Acme Corporation business units by the EGIT programwill be created.

4. Consolidated group reporting will cover:

   a. Progress from business units engaged with their agreed implementation projects based on monitoring agreedperformance metrics

   b. Consolidated IT risk view across the Acme Corporation entities
   c. Specific requirements of the risk committee(s)
5. Financial reporting on the program budget vs. actual amount spent will be generated.
6. Benefit monitoring and reporting against business-unit-defined value objectives and metrics will be created.

9.5.6 Program Risk

The following are considered potential types of risk to the successful initiation and ongoing success of the AcmeCorporation EGIT program. Risk will be mitigated by focusing on change enablement and will be monitored andaddressed continually via program reviews and a risk register. These types of risk are:

1. level Management commitment and support for the program, both at the group level as well as the local business unit

2. local entities should want to adopt the process for the value it will deliver, rather than doing it because of the

   Demonstrating actual value delivery and benefits to each local entity through the adoption of the program. The

   policy in place.

3. Local management's active participation in the implementation of the program
4. Identifying key stakeholders at each entity for participation in the program
5. Business insight within the IT management ranks
6. Successful integration with any governance or compliance initiatives that exist within the group

7. This could be replicated geographically, as well as at the local holding company level, where appropriate.could become an agenda item of the IT executive committee. Local equivalents would also need to be constituted. The appropriate committee structures to oversee the program. For example, the progress of the EGIT program overall

9.5.7 Stakeholders

The following have been identified as stakeholders in the outcome of the EGIT program:

1. Risk committee
2. IT executive committee
3. Governance team
4. Compliance staff
5. Regional management
6. Local entity-level executive management (including IT management)
7. Internal audit services

A final structure containing the individual names of stakeholders will be compiled and published after

consultationwith group management. The EGIT program needs the identified stakeholders to provide the following:

1. Guidance as to the overall direction of the EGIT program. This includes decisions on significant governance-related topics defined in a group RACI chart according to COBIT guidance. It further includes setting priorities,agreeing on funding and approving value objectives.

2. Acceptance of the deliverables and monitoring the expected benefits of the EGIT program

9.5.8 Cost-Benefit Analysis

The program should identify the expected benefits and monitor to ensure that real business value is being generatedfrom the investment. Local management should motivate and sustain the program. Sound EGIT should result inbenefits that will be set as specific targets for each business unit and monitored and measured during implementationto ensure that they are realized. The benefits include:

1. Maximizing the realization of business opportunities through IT, while mitigating IT-related business risk toacceptable levels, thus ensuring that risk is responsibly weighed against opportunity in all business initiatives

2. Support of the business objectives by key investments and optimum returns on those investments, thus aligningIT initiatives and objectives directly with business strategy

3. Legislative, regulatory and contractual compliance as well as internal policy and procedural compliance
4. A consistent approach to measuring and monitoring progress, efficiency and effectiveness
5. Improved quality of service delivery
6. time and with fewer resources Lowered cost of IT operations and/or increased IT productivity by accomplishing more work consistently in less

be funded locally and an estimate provided. Specific project improvement initiatives for each business unit will beindividual business unit management and process owners (attendance, venue, facilitators and other related costs) willtraining courses. These central costs have been estimated for phase 1. The cost of assessment workshops forCentral costs will include the time required for group program management, external advisory resources and initial

efficiency and standardization.estimated in phase 2 and considered on a case-by-case basis and overall. This will enable the group to maximize

9.5.9 Challenges and Success Factors

Figure 9.1program and the critical success factors that should be addressed to ensure a successful outcome.summarizes the challenges that could affect the EGIT program during the implementation period of the

Challenge	Critical Success Factor—Actions Planned
improvement objectivesInability to gain and sustain support for	● Mitigate through committee structures within the group (to be agreedand constituted).
businessCommunication gap between IT and the	● Involve all stakeholders.
Cost of improvements outweighing perceivedbenefits	● Focus on benefit identification.
and the enterpriseLack of trust and good relationships between IT	● Foster open and transparent communication about performance, withlinks to corporate performance management. ● Focus on business interfaces and service mentality. Publish positive outcomes and lessons learned to help establish and maintain credibility. ● Ensure the CIO maintains credibility and leadership in building trust and relations. ● Formalize governance roles and responsibilities in the business soaccountability for decisions is clear. ● Identify and communicate evidence of real issues, risk that needs to beavoided and benefits to be gained (in business terms) relating to Focus on change enablement planning. proposed improvements. ●
Lack of understanding of the Acme environmentby those responsible for the EGIT program	● Apply a consistent assessment methodology.
Various levels of complexity (technical,organizational, operating model)	● Treat the entities on a case-by-case basis. Benefit from lessonslearned and sharing knowledge.
Understanding of EGIT frameworks, proceduresand practices	● Train and mentor.
Resistance to change	● Ensure that implementation of the life cycle also includes changeenablement activities.
Adoption of improvements	● Enable local empowerment at the entity level.
Difficulty in integrating EGIT with the governance models of outsourcing partners	● Involve suppliers/third parties in EGIT activities. Incorporate conditions and right to audit in contracts. ●

Failure to realize EGIT implementationcommitments	• Manage expectations. Keep it simple, realistic and practical. Break down the overall project into small achievable projects, buildingexperience and benefits. • •
Trying to do too much at once; IT tackling overlycomplex and/or difficult problems	• • Apply program and project management principles. Use milestones. Prioritize 80/20 tasks (80 percent of the benefit with 20 percent of theeffort) and be careful about sequencing in the correct order. Capitalizeon quick wins. Build trust/confidence. Have skills and experience to keep it simple • • Reuse what is there as a base. and practical. •
IT in fire-fighting mode and/or not prioritizingwell and unable to focus on EGIT	• Apply good leadership skills. Gain commitment and drive from top management so people aremade available to focus on EGIT. • • Apply tighter discipline over/management of business requests. Address root causes in the operational environment (externalintervention, management prioritizing IT). Obtain external assistance. • •

Challenge	Critical Success Factor—Actions Planned
Absence of required IT skills and competencies,such as understanding of the business, processes, soft skills	■ ■ ● Focus on change enablement planning: Development TrainingCoaching Mentoring Feedback into recruitment process Cross-training ■ ■ ■ ■
Improvements not adopted or applied	● Use a case-by-case approach with agreed principles for the local entity. It must be practical to implement.
Benefits difficult to show or prove	● Identify performance metrics.
Loss of interest and momentum	● Build group-level commitment, including communication.