3. CASELET: ALL WORLD AIRWAYS

LEARNING OBJECTIVE

This case focuses on risk assessment.

Introduction

Don Geekbine, Chief Information Officer (CIO) of All World Airways, must perform a risk assessment of a proposal to outsource the IT operating environment.

BACKGROUND

Company

All World Airways (AWA) is an international airline with reservation centres in the US in Detroit, Michigan, and in Germany in Wiesbaden. AWA has posted losses for the past six quarters.

Industry

The airline industry has been significantly affected by the economic downturn, petroleum prices, labour disputes and the competition. Where IT was a core function, many of the large airlines have spun off their reservations and technical information systems to self-supporting companies and have entered into outsourcing agreements with their former support functions. This has removed investments and assets from the balance sheets, allowed the airlines to focus on their primary business of transportation, and permitted the newly independent IT functions to sell their services to other airlines because competition with the software owner is no longer a conflict of interest.

Key Players

The key players are:
• Don Geekbine, CIO
• Chief Financial Officer (CFO)
• Chief Executive Officer (CEO)

ISSUE

The company has built data centres in both locations, using IBM mainframes running the z/OS operating system and the Airline Control System (ALCS), a high-volume, high-speed transaction processor for the reservation industry. AWA also runs maintenance, scheduling, airfare sensitivity analysis and freight systems. Over the years, all IT activities have been managed and staffed internally.

The CFO and CEO have been reviewing IT costs and return on investment (ROI). Based on their analysis, they have determined that the cost of internal development and IT operations has become too expensive to justify continued support. In their review, they noted that other airlines have outsourced operations to industry-leading IT providers, including Galileo, Sabre®, Amadeus and Travelspan. AWA has decided that IT is not a core business and wants to outsource the IT function.

The CIO, Don Geekbine, was informed of the decision and was asked to perform a risk assessment of the outsourcing process. As part of his initial analysis, he prepared the following notes, in no particular order, which were incorporated into his briefing points:
• All applications were developed internally; reservations are fairly standard and could be easily outsourced; sensitivity analysis, flight and crew scheduling have some specific requirements that are only available with internally developed solutions.
• All systems were written in COBOL; many programmers are retiring, and those available command higher salaries.
• US programmers and operations are located in an economically depressed area; workers with eliminated positions will have problems finding new jobs.
• European work rules have long lead times for the elimination of jobs.
• There is a need to discuss transferring programming to low-cost locations such as India.
• The CFO indicated concern regarding compliance with the US Sarbanes-Oxley Act of 2002; Payment Card Industry Data Security Standard (PCI DSS) compliance is also a concern.
• Equipment and data centre facilities are currently leased. What becomes of the leases?
• Operational processes will require governance to ensure satisfactory performance of key project deliverables, key processes and system availability.
• Don has not performed risk assessments before and is unfamiliar with the issues that should be considered.
The CFO has requested that the risk assessment address the following:

- IT risks
- Financial risks
- Human resources risks
- Competitive risks
- Reputational risks

**Decision to Be Made**

Don has agreed to the assessment, but indicated that he would want to use COBIT as his analysis framework. He has decided that the following COBIT IT processes would be the basis for his risk assessment: PO9, DS1 and DS2. (See the exhibit after the questions for relevant COBIT control objectives.)

**QUESTIONS**

1. You have been requested to compile a list of risks for each of the five areas identified by the CFO for the risk assessment. Group your thoughts by section, using the details that Don has provided, your understanding of the COBIT risk management issues and your understanding of IT issues.

2. Using COBIT PO9, how would you perform a risk assessment of the risks identified in question 1 to provide an objective and subjective assessment for management’s consideration?

3. Using COBIT DS1 and DS2, identify what role the retained organisation should have in its interactions with the vendor for the outsourced IT function.

**EXHIBIT**

**Supporting Documentation—Relevant COBIT Control Objectives**

- PO9.1 IT risk management framework—Establish an IT risk management framework that is aligned to the organisation’s (enterprise’s) risk management framework.
- PO9.2 Establishment of risk context—Establish the context in which the risk assessment framework is applied to ensure appropriate outcomes. This should include determining the internal and external context of each risk assessment, the goal of the assessment, and the criteria against which risks are evaluated.
- PO9.3 Event identification—Identify events (an important realistic threat that exploits a significant applicable vulnerability) with a potential negative impact on the goals or operations of the enterprise, including business, regulatory, legal, technology, trading partner, human resources and operational aspects. Determine the nature of the impact and maintain this information. Record and maintain relevant risks in a risk registry.
- PO9.4 Risk assessment—Assess on a recurrent basis the likelihood and impact of all identified risks, using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk should be determined individually, by category and on a portfolio basis.
- PO9.5 Risk response—Develop and maintain a risk response process designed to ensure that cost-effective controls mitigate exposure to risks on a continuing basis. The risk response process should identify risk strategies such as avoidance, reduction, sharing or acceptance; determine associated responsibilities; and consider risk tolerance levels.
- PO9.6 Maintenance and monitoring of a risk action plan—Prioritise and plan the control activities at all levels to implement the risk responses identified as necessary, including identification of costs, benefits and responsibility for execution. Obtain approval for recommended actions and acceptance of any residual risks, and ensure that committed actions are owned by the affected process owner(s). Monitor execution of the plans, and report on any deviations to senior management.
- DS1.1 Service level management framework—Define a framework that provides a formalised service level management process between the customer and service provider. The framework should maintain continuous alignment with business requirements and priorities and facilitate common understanding between the customer and provider(s). The framework should include processes for creating service requirements, service definitions, service level agreements (SLAs), operational level agreements (OLAs) and funding sources. These attributes should be organised in a service catalogue. The framework should define the organisational structure for service level management, covering the roles, tasks and responsibilities of internal and external service providers and customers.
- DS1.2 Definition of services—Base definitions of IT services on service characteristics and business requirements. Ensure that they are organised and stored centrally via the implementation of a service catalogue portfolio approach.
3. CASELET: ALL WORLD AIRWAYS

- DS1.3 Service level agreements—Define and agree to SLAs for all critical IT services based on customer requirements and IT capabilities. This should cover customer commitments; service support requirements; quantitative and qualitative metrics for measuring the service signed off on by the stakeholders; funding and commercial arrangements, if applicable; and roles and responsibilities, including oversight of the SLA. Consider items such as availability, reliability, performance, capacity for growth, levels of support, continuity planning, security and demand constraints.
- DS1.4 Operating level agreements—Define OLAs that explain how the services will be technically delivered to support the SLAs in an optimal manner. The OLAs should specify the technical processes in terms meaningful to the provider and may support several SLAs.
- DS1.5 Monitoring and reporting of service level achievements—Continuously monitor specified service level performance criteria. Reports on achievement of service levels should be provided in a format that is meaningful to the stakeholders. The monitoring statistics should be analysed and acted upon to identify negative and positive trends for individual services as well as for services overall.
- DS1.6 Review of service level agreements and contracts—Regularly review SLAs and underpinning contracts (UCs) with internal and external service providers to ensure that they are effective and up to date and that changes in requirements have been taken into account.
- DS2.1 Identification of all supplier relationships—Identify all supplier services, and categorise them according to supplier type, significance and criticality. Maintain formal documentation of technical and organisational relationships covering the roles and responsibilities, goals, expected deliverables, and credentials of representatives of these suppliers.
- DS2.2 Supplier relationship management—Formalise the supplier relationship management process for each supplier. The relationship owners should liaise on customer and supplier issues and ensure the quality of the relationship based on trust and transparency (e.g., through SLAs).
- DS2.3 Supplier risk management—Identify and mitigate risks relating to suppliers’ ability to continue effective service delivery in a secure and efficient manner on a continual basis. Ensure that contracts conform to universal business standards in accordance with legal and regulatory requirements. Risk management should further consider nondisclosure agreements (NDAs), escrow contracts, continued supplier viability, conformance with security requirements, alternative suppliers, penalties and rewards, etc.
- DS2.4 Supplier performance monitoring—Establish a process to monitor service delivery to ensure that the supplier is meeting current business requirements and continuing to adhere to the contract agreements and SLAs, and that performance is competitive with alternative suppliers and market conditions.