Chapter 4

Audit of a CASE Environment

Mario Piattini
Universidad de Castilla-La Mancha, Spain

Jesús García-Tomás
Universidad Politécnica de Madrid, Spain

INTRODUCTION

The diffusion of CASE tools, along with the ever more pressing problems surrounding the management of the systems development department, has meant that themes related to internal control and audit of a CASE environment are of increasing interest.

In fact, the high cost of introducing CASE technology added to the potential improvement in productivity and quality have made it one of the most important areas for the Information Systems auditor.

In this paper we will deal with some of the questions that have to be taken into account when auditing a CASE environment. Our aim is not to offer exhaustive checklists of factors of influence in this kind of environment, but rather to reflect upon some themes that have been dealt with throughout the literature but from a different perspective to that of the information systems auditor.

In this paper we will deal with some of the questions that have to be taken into account when auditing a CASE environment. Our aim is not to offer exhaustive checklists of factors of influence in this kind of environment, but rather to reflect upon some themes that have been dealt with throughout the literature but from a different perspective to that of the information systems auditor. In order to do this we will begin by briefly introducing the basic concepts of the information systems audit, giving a brief explanation of the different methodologies that are used in this area. We will also analyze the risks that must be taken into account when installing a CASE tool.

This chapter appears in the book, Successful Software Reengineering by Sal Valenti. Copyright © 2002, IRM Press, an imprint of Idea Group Inc.
INFORMATION SYSTEMS AUDIT

By the term “internal control” we understand the policies, procedures and norms as a whole, which are established by the management group of a company in order to carry out its activities in an orderly and efficient way, safeguarding the assets and guaranteeing the completeness and reliability of its records. In the field of information technology, the aim of the internal control system is to guarantee the adaptation of the management of the computer assets and the reliability of the activities of the information systems (ISACF, 1998).

The concept “audit” can be defined as “the examination of an activity and the expressing of an opinion about the quality of the performance of an activity, undertaken by persons independent of the team responsible for the performance and supervision of the activity” (Clark et al., 1991).

Until a few years ago this function was related almost exclusively to the financial aspects and management of the companies; however due to their ever-increasing automation, the need has arisen for highly qualified technical personnel able to understand the risks that exist in the automated environment of information systems: these are the information system auditors (Piattini, 2000). Although at the beginning this person was considered as an “assistant” to the finance auditor, for whom he/she prepared programs which would make certain tests easier to carry out, nowadays they are increasingly more autonomous due to the growing complexity of information systems.

The computer audit can be defined, as according to Weber (1999), as “the process of collecting and evaluating evidence to determine whether a computer system safeguards assets. Maintains data integrity, allows organizational goals to be achieved effectively, and uses resources efficiently.”

Usually the information system audit is applied in two different ways; on the one hand the principal areas of the computer department are audited: the exploitation, the management, the development methodology, the operating system, telecommunications, databases, etc. and on the other hand the applications that work in the company are audited – internally developed, sub-contracted or acquired.

The audit of the CASE environment would form a part of the audit of the development process. The importance of the audit of the development environment arises from the fact that it is the starting point for the execution of the audit of the applications.

INFORMATION SYSTEM AUDIT METHODOLOGIES

Although different methodologies exist that can be applied in information system audit given that almost all firms of auditors and individual companies develop their own – these can be divided into two groups:
A Service-Based Approach for RBAC and MAC Security
www.igi-global.com/chapter/service-based-approach-rbac-mac/28961?camid=4v1a