Supporting Assurance and Compliance Monitoring

Peter Goldschmidt
The University of Western Australia, Australia

INTRODUCTION

Governments and commercial organizations typically use monitoring facilities that depend on data that identify source agents and their relationships, to detect and draw attention to possible anomalies and potential non-compliance.

The assurance of compliance monitoring requires decision support and appropriate domain knowledge, relevant to the level of user, to manage the results of the surveillance. This is required in order to fulfill the necessary and sufficient evidence verifying or refuting this output.

BACKGROUND

This article discusses methods to support assurance of surveillance monitoring and output verification knowledge management (CV-KM), including a brief discussion on primary monitoring systems; the different environments in which they operate; the verification problem solving and decision making tasks; the problem structure and the coordination of the review process to facilitate truth maintenance. The surveillance operation is considered a primary monitoring function, with the analysis of the resulting output the secondary monitoring function - the assurance component.

Examples of monitoring systems range from standard data processing routines that ensure internal control, such as data input, processing and output compliance. Weber (1999) provides a comprehensive discussion on these processes, to the monitoring of events transacted in more complex environments, such as fraud detection, intrusion detection, data mining systems and the like, via sophisticated statistical, artificial intelligence and neural computing techniques, or hybrid combinations. These devices are termed primary monitoring systems (PSS).

Assuring, verifying and managing PSS information quality and integrity is fundamental to the success of modern information-dependent organizations. Concurrent with the need for surveillance is a need to maintain personal privacy, due diligence, and accountability (Cillufo, 2000).

Clarke (1988) highlights the inherent dangers of drawing conclusions resulting from the electronic monitoring of data related to individuals and groups of individuals, and points out that a major problem in “dataveillance” is the high noise to signal ratio, which may be misleading. Davis and Ord (1990) acknowledge the problem of setting threshold levels in an ever-changing environment. With any set of tolerance levels, deviant (even fraudulently motivated) behaviour may escape detection. Tightening tolerance levels limits increases the likelihood that exception conditions will trigger an alert but also increases false positive alerts since the number of instances that fall outside the tolerance increases. The cost for the analyst (the decision-maker) to review the additional non-exception condition alerts must be assessed in relation to the imputed value of identifying the additional true exceptions detected by more stringent limits (Davis & Ord, 1990).

Advances have, in general, reduced the problem of misleading results produced from “noisy data,” including improvements in data processing and the increased use of sophisticated computational techniques such as statistical, knowledge-based and artificial neural computational methods. These systems are centered on the events being monitored and the events’ source agents. Their results, however, may still require human judgment to determine their validity (Goldschmidt, 2001). CV-KM systems act as a secondary monitoring facility supporting, verifying and assuring data and information compliance by assisting in analyzing and categorizing exceptions, or results, generated by PSS. CV-KMs assist in assuring the fulfillment of the necessary and sufficient evidence supporting (true positive/negative) or refuting (false positive) hypotheses of non-compliance. The input to CV-KMs requires the output resulting from the organization’s domain-specific PSS plus related information. Operationally, the CV-KMs are a bolt-on addition to the PSS.

WHAT ARE PRIMARY SYSTEMS?

Typically, these systems examine the integrity of transaction data as well as the entire transaction, or event, to ensure compliance with predetermined conditions. An exception report identifies any variances. This identification either fulfills the conditions of necessary and sufficient evidence and determines an instance of non-compliance, or indicates possible non-compliance. In the latter case further evidence may be sought to substantiate the hypothesis of non-compliance.

The function of PSS is twofold: identifying a variance, and producing and accumulating supporting evidence. When both these conditions are met, the evidence points to the detective, corrective or preventative actions required.

The detective function is fulfilled by recognition of the variance; correction can then be made to the data or the event, which is then reprocessed. The preventative function is fulfilled by the recognition of the variance resulting in the rejection of the event. Decision-makers must interpret ambiguous evidence to determine what action is required, or if the non-compliant indicator is a true or a false positive directive.

Examples of PSS range from standard data processing routines that ensure internal control, such as data input, processing and output compliance, to the use of sophisticated statistical (procedural) techniques, artificial intelligent (declarative) techniques and neural (associative) techniques, or hybrid combinations. In general, computational techniques are either demons or objects (O'Leary, 1991; Vasarhelyi & Halper, 1991). Demons are computerized routines that are instantiated by data or events received, as opposed to being requested by some program. "Demons add knowledge to a system without specification of where they will be used ... like competent assistants they do not need to be told when to act" (Winston, 1977, p. 380). They are data or event dependent, rather than program dependent, and provide intelligent self-activation for monitoring data triggered by compliance threshold levels. O'Leary points out that demons have been developed to monitor patterns for the purpose of auditing activities conducted on computer-based systems. Vasarhelyi and Halper describe an alternate: CPAS, Continuous Process Audit System. CPAS allows for the continuous audit of on-line systems by monitoring transactions to determine variance between monitored information and expected information.

THE PSS AND CV-KM ENVIRONMENT

PSS and CV-KM can be classified by levels of complexity, characterized by their place on the simple or complex environmental continuum in which they operate and the decisions required to determine instances of non-compliance. Constraints may take the form of an organization's predetermined policies and procedures, needed to ensure data and event integrity, contractual agreements, and statutory requirements. These constraints are not mutually exclusive and can be seen as bounds or threshold levels. The parameters used to construct these levels may change with modifications to threshold requirements such as evolutionary changes in constraints and changes in data and event requirements. A simple environment is so-called because: 1) the threshold levels either seldom change or only change over the longer term; 2) the identification of the variance fulfils the conditions of necessary and sufficient evidence to determine an instance of non-compliance; and 3) the decisions, needed to determine if events comply, lie on the structured to highly structured portion of the decision-making continuum. The degree to which the bounds of the threshold levels are set, very narrow to very broad, determines the type of decision required. Under a simple environment the bounds or threshold limits are narrow, characteristic of structured decisions such as data input integrity and customer credit checks. Decision-making in this environment is ex-ante, made of a single step, and the constraints are all predetermined.

In a complex environment, decision-making is ex-post, complex and may require multiple steps. Initial monitoring uses a priori thresholds broader than in a simple environment, that is, more granular and produces exceptions that identify suspected non-compliant events (SNCEs). Once these exceptions have been produced, the decision-maker must substantiate true positive exceptions. This task must be broken down into smaller components and subgoals must be developed (Simon, 1973) to identify, categorise and discard any false positive exceptions. False negatives do not generate an exception, and allow possible suspect events to slip through the surveillance sieve. If the threshold limits are stringent enough, marginal false negatives could be subsumed and later considered. Nevertheless, this would not necessarily reduce the occurrences of *true* false negatives, as their characteristics may not be known. True positives are those exceptions that the decision-maker has determined are indeed anomalous. Evidence for this decision uses the results of the initial monitoring as well as important information related to the event, characterized by a need for judgmental expertise. Examples of these approaches to complex environments include: Byrnes et al. (1990), Major and Riedinger (1992), Senator et al. (1995), and Kirkland et al. (1999).