QFINANCE

The Case for Continuous Auditing of Management Information Systems

by Robert E. Davis

This Chapter Covers

Managers should concentrate on making business decisions based on management information systems that reduce the risk of inappropriate responses to the entity's environment.
Since management is responsible for the entity's controls, it should have the means to determine, on an ongoing basis, whether selected controls are operating as designed.
Continuous auditing is an uninterrupted monitoring approach that allows IT auditors to examine controls on an ongoing basis and to gather selective audit evidence through the computer for timely opinions.

Introduction

Management information systems represent the aggregation of personnel, computer hardware and software, and associated policies and procedures, allowing data processing to generate information that can be used for decision-making. Corporations typically have management information systems with specific objectives designed to comply with external and internal business requirements. In this context, management information systems can exist at three configuration levels: decision support systems, expert systems, and continuous monitoring systems. Through an understanding of the development and deployment of these technologies, a case can be made for the continuous auditing of management information systems.

Considering the impact on decision processes, automated management information systems necessitate a higher degree of reliability and integrity than other information technology deployments. This is a result of the common need to extract system-generated information as opposed to manually created information to aid in making business decisions. Hence, corporate auditors need to convey timely opinions on both the quality of management information systems and the information produced by management information systems utilizing continuous assurance techniques. On the benefit side, employing continuous auditing can reduce the risk of management initiating inappropriate actions based on faulty logic and/or data.

Decision Support Systems as an Aid to Enterprise Governance

Control systems can be categorized as being either technical systems or decision systems. Classically, corporate technical systems represent specialized configurations that support business units in achieving objectives, whereas decision systems represent information systems, or analytic models, designed to effectively aid managers and professionals in decision-making. Nonetheless, assistance for the decision-making process may be contained in a technology-based decision support system (DSS).

Interpretatively, a technology-based information system represents an architectural component that collects data, processes transactions, and communicates operational results, while an analytical model is a set of relationships with variable continua of:

complexity, from one variable to many;
uncertainty, from deterministic to probabilistic;
time, from static to dynamic.

Thus, through proper system or model construction, an entity-centric DSS is deployed to enable the evaluation of alternative courses of action and efficient choice from the presented options to achieve the defined business objective.

Optimizing IT Assistance for Making Decisions

Reliable decision support systems should provide accurate and complete disclosure of available options, while maintaining the confidentiality and integrity required to enable effective responses. The "quality of management" depends heavily on having managers evaluate alternatives and select from the available options as many correct responses as possible. To ensure managerial quality, most managers are under observation for situational responses that impact the entity. Therefore, the ratio of decisional hits to misses must weigh favorably in the direction of hits for a manager to retain his status within most organizational formations. In other words, a regular pattern of failure to make appropriate decisions usually disqualifies an employee from retaining directional authority within an entity.

Generally, supporting decisions with software and hardware is wholly inadequate if there is no clear idea about the kinds of decisions that need to be made. Enterprise governance involves different types of decisions. The first type, *routine decisions*, is commonly treated within the entity's framework of policies and procedures. The second type, *nonroutine decisions*, typically requires one-time or nonrepetitive solutions based on environmental considerations. The third type, *nonroutine motley decisions*, is generally ill-structured and complex, arising from one-of-a-kind situations, and for an optimal response relies on scientific assessment. Nevertheless, decision techniques have become largely synonymous with quantitative approaches or mathematical analysis, which are well suited to IT processes. Some types of the latter are financial and statistical analysis that, depending on the circumstances, may be addressed through game theory, linear programming, simulation, and operations research.

At a minimum, governance decision support systems should include word processing, database, spreadsheet, and modeling capabilities. Of these, modeling is crucial to reducing uncertainty in the response to circumstances requiring a decision. Rudimentarily, a model comprises variables and objectives, where the structure must reflect the purpose for which it is constructed.

The variables in a quantitative model constitute a mathematical description of the relation between elements that can be classified as decision, intermediate, or output variables. The decision variables are usually controlled by the decision-maker and vary with the alternative selected. Intermediate variables link decisions to outcomes, thus functioning as consolidation variables. Output variables measure decision performance, and are referred to as "attributes."

Right-Sizing the Governance Model

Many types of detail variables can be associated with a mathematical model. Binary variables are employed for "go" and "no-go" decisions. Discrete variables are utilized for any of a finite number of values. Questions of "which" and "when" are represented as specific discrete values. Such data need not be continuous; however, continuous variables present an infinite number of possible values, and all the values will lie within a specific range. Among the other characteristics of detail variables, they can be random variables that model uncertainty and are expressed as probabilities. They can also be exogenous variables, ones that are external to the model and cannot be influenced by decision-makers.

DSS models are abstractions that operate as substitutes for the actual circumstances under evaluation. A model-driven DSS emphasizes access to and manipulation of statistical, financial, optimization, or simulation archetypes. Consequently, a model-driven DSS utilizes data and parameters provided by users to assist decision-makers in analyzing a situation; however, they are not necessarily data-intensive.

The construction of a DSS model for governance includes: making a large number of assumptions about the nature of the environment in which the entity's programs, systems, processes, activities and/or tasks operate; selecting the operating characteristics of components; and making paradigm suppositions about the way animate and/or inanimate objects are likely to behave. A model is ready for use by management when it matches the set of objectives and attributes that require analytical consideration.

The value of information assets is continuously increasing in this information age due to their integration into decision-making processes. Governance decisions are highly visible, often offer immediate results, tend to be goal-focused, and are directive. Although there are various techniques that can be applied to types of governance decisions, the final outcome is a matter of judgment. Normally, IT processes can be adapted to support judgmental decisions through the utilization of engineered business processes.

To ensure robustness for the intended application, DSS models must pass three tests: relevance, accuracy, and aggregation. Relevance is measured by the alignment of the defined condition to possible problem solutions. Accuracy can vary depending on the decision that is being made. Aggregation permits the grouping of a number of individual quantities into a larger quantity.

Impact of Decision Support Systems

Decision-making is the process of evaluating alternatives and choosing from among them. Information may drive leadership; however, data accuracy and completeness are prerequisites to ensuring that appropriate decisions are made. A DSS commonly assists middle-level and upper-level managers in long-term, non-routine, and often unstructured decision-making. Typically, the deployed system contains at least one decision model, and it is usually interactive, dedicated, and time-shared—although it need not be real-time. Thus, a DSS should be viewed as an aid to decision-making rather than simply the automation of decision processes. Managers should concentrate on making professional governance decisions based on a DSS that reduces the potential for inappropriate responses to the entity’s environment.

Expert Systems as an Aid to Compliance

Technology is an ever-changing tool driven by compliance requirements as well as entity-centric requirements to satisfy market demands. For compliance requirements, IT deployments tend to be reactionary rather than a continuous, proactive process. Consequently, IT compliance efforts are typically lacking in constancy and conformity. To combat this tendency, IT planners should focus design and transition efforts on three time frames that meet entity needs: the current state, the near-term state, and the long-term state of compliance requirements. Within this context, expert systems can be an invaluable tool for implementing mandates that satisfy immediate needs and simultaneously position the entity to meet the next potential compliance issue effectively.

Expert System Development Activities

IT usually pervades all organizational formations that are pursuing effective and efficient processing in response to compliance requirements, thus facilitating better decision-making through various information delivery mechanisms and offering opportunities for business model development that may lead to value creation as well as competitive advantage. To construct an expert compliance system a knowledge engineer—performing a function similar to a system or business analyst—is typically needed. A designated knowledge engineer is responsible for defining issues in manageable terms, soliciting the knowledge, skills, and abilities of experts, and translating these talents into electronically encoded formats.

The development of an expert system is usually a four-step process. It starts with the knowledge engineer gaining an understanding of a particular judgment issue. This is followed by the acquisition of the thought processes of experts in solving the issue. Next, if a shell program is not available, a computer model is programmed to reproduce the thought processes that have been adopted for defined situations. Finally, the system is tested and certified to ensure that the resulting decisions are appropriate and usable. These steps are commonly known as knowledge representation, knowledge acquisition, computational modeling, and model validation.

Populating the Expert System

A knowledge engineer can obtain knowledge in several ways. One option is to go through textbooks and professional journals to extract definitions, axioms, and rules that apply to the issue. This type of knowledge acquisition is especially useful for teaching and reference situations because the question–response paths are direct. However, the way in which questions are posed to the expert system can lead to misleading results. Another method of acquiring knowledge is to ask human experts to explain their thought processes and ways of solving problem scenarios; this is sometimes referred to as verbal protocol analysis. Last, a human expert can enhance the information obtained from literary resources and will often bring unpublished knowledge, gained through experience, to the decision process paths. This combinational knowledge makes human-based expert systems a valuable technology.

To incorporate human expert knowledge into a technology-based expert system, the right individuals must be identified and selected. Specialists tend to be trained in rather narrow domains and are best at solving problems within their defined realms of expertise. Assuming that experts do exist and are willing to participate, good experts are those who are able to solve particular types of problem scenarios that few others can solve with the same efficiency and/or effectiveness. Additionally, considerable time can be saved in developing an expert compliance system if the knowledge engineer has experience in the area that is being modeled.

After experts have been selected, the knowledge engineer must take the expert knowledge and transform it into a computational model. However, issues may arise because an expert discovers that he or she is unable to describe how a situation is resolved. Typically, this is due to the way they may operate at a subconscious level while performing some tasks to address a scenario. In view of the possibility that undefined steps may generate misaligned logic paths in the inference engine, it is common for interdisciplinary teams of specialists to work together to formulate deductive reasoning processes for defined problems.

To assist in assessing decisional acumen, most managers are under observation for situational responses that may impact the entity. The reliability of business-related information used in making decisions is therefore critical. During the final stage of preparation for deployment, an expert system has to be validated to ascertain the reliability and scope of its decisional processes. In the model validation step a knowledge engineer and/or IT assurance professional identifies errors, omissions, and mistakes in the knowledge base. Furthermore, since the constructed system is designed to simulate an expert’s decision-making process, it should be tested against the opinions of subject matter experts. Finally, if the system is later updated to keep the knowledge base current, reevaluation of the model is necessary to ensure its continued decisional reliability.

Impact of Expert Systems

From a technical perspective, the typical expert system can be divided into two essential parts: the knowledge base, and the inference engine. The knowledge base contains the body of knowledge, or set of facts and relationships, obtained in the knowledge acquisition phase. The rules associated with a knowledge base tend to be heuristic and take the form of conditional statements, whereas the inference engine is a collection of computer routines that control the system paths through the knowledge base to enable recommendations. In addition, the inference engine serves as a bridge between the knowledge base and the user.

Methodologically, for expert systems the knowledge engineer defines the ambit of issues that the system will address. A logic path that is too broad may result in a system that is too difficult to manage and it may cause a system crash. Contrastingly, the knowledge engineer must be careful not to limit an issue overly because a logic path that is too narrow will produce a system so rudimentary that the results will be worthless.

Continuous Monitoring Systems as a Risk Management Aid

A management information system is often deployed to permit performance monitoring to assess compliance with adopted standards and enable corrective actions and/or process improvements to an entity’s control systems. A generally accepted key element that enables the risks inherent in many control systems to be successfully managed is the ability to monitor processes independently and continuously as close to the execution point as possible. Yet, analytic technologies capable of continuous monitoring are typically lacking in management information system deployments. Therefore, a continuous monitoring system that is conjointly implemented within management information systems can enhance the detection of variance as well as improve compliance verification and exception reporting systems.

“Monitoring encompasses the tracking of individual processes, so that information on their state can be easily seen, and statistics on the performance of one or more processes can be provided.” From Wikipedia entry, “Business process management.”

Foundations for Managing Processes

Prespecified and routine decisions, which form the policies and procedures that are typically documented by an entity, are designed to provide time for managers to address non-routine activities and consider improvements to the currently deployed control processes by removing them from the more mundane aspects of day-to-day operations. However, process monitoring is required to ensure that expected outcomes are achieved for assigned functional responsibilities and that irregular activities are detected on a timely basis.

Conceptually, continuous monitoring systems generally consist of three levels: data provisioning, information management, and information presentation. Data provisioning is enabled by the collection and storage of specified items in an assigned location. Information management utilizes the combination of knowledge of IT architecture, analytic knowledge, and collected data to assess processing. Information presentation provides results from the conditions that are being monitored.

To enable effective deployment, the three levels of continuous monitoring must operate harmoniously. The data provisioning level supplies raw data for analysis after the collection process has been completed. These collected data can be extracted from processed and formatted output that is produced by defined processes and/or through direct data access. The extracted data are commonly stored in a data repository and/or retained in original form. However, certain data may also need to be stored at the information management level. This includes information about the structure of the systems that are being monitored as well as analytic definitions, such as conditional statements. Analysis of the data is performed using various tools, and the output is sent to the presentation level for evaluation by designated users.

Path to Continuous Monitoring

According to the Institute of Internal Auditors (2005), “Continuous monitoring of controls is a process that management puts in place to ensure that its policies and procedures are adhered to, and that business processes are operating effectively.” Though manual performance monitoring may suffice in low-technology situations, in most high-technology environments automated controls become a necessary part of the IT architecture for ensuring information reliability and integrity. As suggested by John Verver (2003), the technology underpinnings to enable an effective continuous monitoring strategy should include several key components: independence from the system that processes the data; the ability to compare data and information across multiple platforms; the ability to process large volumes of data; and prompt notification to management of items that represent control exceptions.

To ensure effective continuous monitoring, adequate segregation of functions must be sustained. Continuous monitoring and segregation of functions are not new control concepts. Yet technological integration issues can be a barrier to implementing continuous monitoring systems that are independent of operational processes and capable of easy configuration for specific risk tolerance requirements. Procedurally, achieving appropriate functional independence in an automated system necessitates defining IT and operational user work units with consideration of the control context. As a result, when properly implemented, the segregation of functions assures that organizational responsibilities do not impinge on the independence or corrupt the integrity of information system assets while data on individual processes are being tracked and collected.

Continuous monitoring allows management to have greater insight into the entity’s current state of compliance. Typically, for IT, continuous monitoring involves ongoing automated testing of selected data within a given process area against a suite of control protocols. Management can utilize this information to set or reset process guidelines, rules, and tests via applied analytics that identify performance gaps or unusual events that may suggest control failures. This type of continuous monitoring can exist in IT hardware, firmware, or software that is enabled to observe and record automated activities. Therefore, automated continuous monitoring provides a timely feedback mechanism for management to ensure that configuration items and controls are operating as designed and that data are processed appropriately.

Impact of Continuous Monitoring

Since management is responsible for the entity’s controls, they should have the means to determine, on an ongoing basis, whether selected controls are operating as designed. Continuous monitoring typically addresses management’s responsibility to assess the adequacy and effectiveness of controls in a timely manner. It enhances managerial capabilities and entity-level controls, while striving to facilitate the maintenance of acceptable performance levels. Furthermore, with the ability to identify and correct control problems on a timely basis, automated continuous monitoring enriches an entity’s compliance program. Nonetheless, the key to a successful deployment of automated continuous monitoring is process ownership by personnel who are assigned responsibility for responding to reported exception conditions.

Case Study

In this information age the value of information assets is continuously increasing due to their integration into decision-making processes. Assistance in the decision-making process may be contained in an IT DSS. Thus, utilizable decision support information should provide accurate and complete disclosure of available data while maintaining the expected confidentiality and integrity.

Technology deployment and associated management information systems can provide a competitive advantage as well as increased control requirements. Considering the adamant demands for continuous process improvements, a focus on overall information protection and security delivery value in terms of enabled services has become the managerial norm. Information security service management is a set of processes that enable and potentially optimize IT security services for an entity to satisfy business requirements, while simultaneously providing strategic and tactical management of the IT security infrastructure. In this context, information security service level management should be considered a quality of service administration that makes demonstrable contributions to process improvement.

Noncompliance risks are an irrefutable fact, where the consequences range from significant financial penalties to the threat of damage to an entity’s reputation. Fielding an appropriate response to a security incident is typically a crucial business requirement. To enable effective management, a security MIS should correlate data to intended usage to determine the repercussions of a security failure. Considering that the primary contingency management objective is to provide solutions through an understanding of risk, an adequate response to an IT security incident depends on timely, reliable information to assess the risks and subsequently apply resources.

Auditors are indirectly, if not directly, an entity control mechanism which assures that mandated compliance expectations are adequately addressed by management. Amplifying the criticality of information security is the number of laws related to the protection of information assets and regulations that impact compliance expectations. In one form or another, assuring compliance serves as a significant information security audit objective for most entities which can best be served through continuous auditing of information security incidents. Therefore, an auditor should continuously audit whether effective procedures for the protection of information assets are implemented to manage and maintain the confidentiality and integrity of information throughout the information lifecycle.

Making It Happen

Survey the deployment of computerized management information systems.
Acquire support for the investigation of continuous auditing options.
Assess the risk of inappropriate decision-making based on unreliable and inaccurate information.
Present a transparent case for establishing continuous auditing of high-risk management information systems.
If necessary, confer with the IT department to establish service-level agreements for continuous auditing systems.

Summary

Continuous auditing is an uninterrupted monitoring approach that allows IT auditors to examine controls on an ongoing basis and to gather selective audit evidence through the computer. Theoretically, in some environments it should be possible to significantly shorten the audit reporting time frame to render nearly instantaneous or truly continuous assurance. In particular, continuous assurance is well suited for use in high-risk, high-volume, paperless environments. As a technique, continuous auditing is designed to enable IT auditors to report on subject matter within a much shorter time frame than under other audit models. As a process, continuous auditing can be employed to enable timely reporting by IT auditors through continuous testing.

More Info

Books:

- Akerkar, Rajendra, and Priti Sajja. *Knowledge-Based Systems*. Sudbury, MA: Jones & Bartlett, 2009.
- Davis, Robert E. *Assuring IT Legal Compliance*. Los Gatos, CA: Smashwords, 2011.
- Higson, Andrew. “Effective financial reporting and auditing: Importance and limitations.” In *QFINANCE: The Ultimate Resource*. 3rd ed. London: Bloomsbury, 2012; pp. 338–340. Online at: tinyurl.com/6mw6qe6
- Laudon, Ken, and Jane Laudon. *Management Information Systems*. 11th ed. Upper Saddle River, NJ: Prentice Hall, 2009.
- Mainardi, Robert L. *Harnessing the Power of Continuous Auditing: Developing and Implementing a Practical Methodology*. Hoboken, NJ: Wiley, 2011.
- O’Brien, James, and George Marakas. *Management Information Systems*. 9th ed. New York: McGraw-Hill, 2008.
- Seref, Michelle M. H., Ravindra A. Ahuja, and Wayne L. Winston. *Developing Spreadsheet-Based Decision Support Systems*. Charlestown, MA: Dynamic Ideas. 2007.

Article:

- Verver, John. “Risk management and continuous monitoring.” *AuditNet* (March 2003). Online at: tinyurl.com/6vmqu4p [PDF].

Report:

- Institute of Internal Auditors. “Continuous auditing: Implications for assurance, monitoring, and risk assessment.” White paper. 2005. Online at: tinyurl.com/cheh2wn [PDF].

Websites:

- Information Systems Audit and Control Association (ISACA): www.isaca.org
- Institute of Internal Auditors (IIA): www.theiia.org
- International Federation of Accountants (IFAC): www.ifac.org

See Also

Best Practice

- Continuous Auditing: Putting Theory into Practice
- Reducing Costs and Improving Efficiency with New Management Information Systems

Checklists

- Auditing Information Technology and Information Systems

To see this article on-line, please visit http://www.qfinance.com/performance-management-best-practice/the-case-for-continuous-auditing-of-management-information-systems?full