Continuous Auditing

Continuous auditing is an approach used by an IT auditor to monitor system reliability on a continuous basis and gather selective audit evidence through the computer. A distinctive characteristic is the short time lapse between the facts to be audited, the collection of evidence and audit reporting.

This enables an IT auditor to perform tests and assessments in a real-time or near-real-time environment, reporting results on the audit subject matter within a much shorter time frame than under a traditional audit approach. Click the links below to review more information about continuous auditing

- Continuous audit uses
- Continuous audit techniques
- Other continuous audit techniques

Continuous audit uses

Continuous auditing efforts often incorporate new IT developments; increased processing capabilities of current hardware, software, standards and AI tools; and attempts to collect and analyze data at the moment of the transaction. Continuous auditing aims to provide a more secure platform to avoid fraud and a real-time process aimed at ensuring a high level of financial control.

To accomplish this, data must be gathered from different applications working within different environments, transactions must be screened, the transaction environment has to be analyzed to detect trends and exceptions, and atypical patterns (i.e., a transaction with significantly higher or lower value than typical for a given business partner) must be exposed.

If all this must happen in real time, perhaps even before final sign-off of a transaction, it is mandatory to adopt and combine various top-level IT techniques. The IT environment is a natural enabler for the application of continuous auditing because of the intrinsic automated nature of its underlying processes.

Continuous auditing tools are often built into many enterprise resource planning packages and most OS and network security packages. These environments, if appropriately configured and populated with rules, parameters, and formulas, can output exception lists on request while operating against actual data. Therefore, they represent an instance of continuous auditing. The difficulty, but significant added value, of using these features is that they postulate a definition of what would be a “dangerous” or exception condition.

For example, whether a set of granted IT system access permissions is to be deemed risk-free will depend on having well-defined separation of duties. On the other hand, it may be much harder to decide if a given sequence of steps taken to modify and maintain a database record points to a potential risk. It is important to validate the source of the data used for continuous auditing and note the possibility of manual changes.

Continuous audit techniques

Continuous audit techniques are important IT audit tools that improve the security of a system by permitting an IT auditor to evaluate operating controls without disrupting the enterprise's usual operations. This can be valuable when these tools are used in time-sharing environments that process many transactions but leave a scarce paper trail. For example, when a system is misused by someone withdrawing money from an inoperative account, a continuous audit technique will report this withdrawal in a timely manner to an IT auditor. This can reduce the time lag between the misuse of the system and the detection of that misuse.

The use of continuous audit procedures gives an IT auditor and management greater confidence in an IT system's reliability because failures, improper manipulation and lack of controls will be detected on a timely basis. There are five types of automated evaluation techniques applicable to continuous auditing.

Systems control audit review file and embedded audit modules (SCARF/EAM)
Involves embedding specially written audit software in the enterprise's host application system so the application systems are monitored on a selective basis.

- Complexity: very high
- Useful when: regular processing cannot be interrupted.

Snapshots
Involves taking "pictures" of the processing path that a transaction follows, from the input to the output stage. With the use of this technique, transactions are tagged by applying identifiers to input data and recording selected information about what occurs for an IT auditor's subsequent review.

- Complexity: medium
- Useful when: an audit trail is required

Audit hooks
This technique involves embedding hooks in application systems to function as red flags and induce IT auditors to act before an error or irregularity gets out of hand.

- Complexity: low
- Useful when: only select transactions or processes need to be examined

Integrated test facility (ITF)
In this technique, dummy entities are set up and included in an auditee's production files. An IT auditor can make the system either process live transactions or test transactions during regular processing runs and have these transactions update the records of the dummy entity. The operator enters the test transactions simultaneously with the live transactions that are entered for processing. An IT auditor then compares the output with the data that have been independently calculated to verify the correctness of the computer-processed data.

- Complexity: high
- Useful when: it is not beneficial to use test data

Continuous and intermittent simulation (CIS)
During a process run of a transaction, the computer system simulates the instruction execution of the application. As each transaction is entered, the simulator decides whether the transaction meets certain predetermined criteria and, if so, audits the transaction. If not, the simulator waits until it encounters the next transaction that meets the criteria.

- Complexity: medium
- Useful when: transactions meeting certain criteria need to be examined.

Other continuous audit techniques

Techniques that are used to operate in a continuous auditing environment must work at all data levels—single input, transaction, and databases—and include:

- Transaction logging
- Query tools
- Statistics and data analysis
- Database management system (DBMS)
- Data warehouses, data marts, data mining
- Intelligent agents
- Embedded audit module (EAM)
- Neural network technology
- And standards such as Extensible Business Reporting Language (XBRL)