Deloitte.

This article originally appeared in Deloitte's 2020 Directors' Alert

Can IoT enable continuous auditing?

Auditors now see continuous auditing—external audits conducted in near real time and completed shortly after a company's accounting period—as inevitable. The question is, are organizations and auditors ready for it, and how we get there.

The required technologies already exist within certain parts of organizations. For example, data generated by sensors embedded in objects connected to the Internet—the Internet of Things (IoT)—may accelerate the move toward continuous auditing. There were an estimated 15 billion IoT connected devices in 2015; in 2019, that number grew to 27 billion. By 2025, IoT connected devices is projected to exceed 75 billion, and it won't stop there.[1] IoT is evolving at a rapid pace, exponentially increasing the volume of data available to organizations and auditors.

Auditors can use data generated by IoT sensors as evidence to support their findings rather than relying on samples of traditional data and documentation. Powered by IoT and other automated sources of data, continuous auditing will require organizations to revamp their reporting processes and how auditors design audit procedures. It will have an impact on organizations' closing processes, reporting schedules, technology investments, and data security and privacy. For auditors, it will represent a quantum leap beyond manual processes for gathering supporting evidence, which at times rely heavily on hard-copy internal documents and data sourced from outside the organization.

Yet, continuous auditing presents challenges, as well as opportunities, to organizations and auditors. Not the least among these challenges are the need to manage the volume of data collected and optimize its use. ❯

Chad Shaver
National Audit Transformation and Innovation Leader
Deloitte Canada

Nicole Deschamps
Audit Analytics and Innovation Team Leader
Deloitte Canada

---

1 Statista, Internet of Things (IoT) Connected Devices Installed Base Worldwide from 2015 to 2025, November 2019

To manage the data, organizations need well-designed processes, appropriate investments in technology and training, and a strong commitment from management. Data privacy and systems interoperability also need to be addressed to accommodate IoT. Robust security is required given that IoT devices expand the cyber threat landscape and create new exposures. In general, management and audit committees will need to understand how the finance function uses IoT data to support reporting, especially as the data relates to underlying estimates and judgments, or is used in the company's internal controls over the financial reporting processes.

Auditors will require new processes to incorporate and rely on IoT data, which will often constitute new evidence. Operational and financial reporting processes that use IoT data will have new internal controls for auditors to test. The quality of audit evidence will be directly influenced by the design and reliability of the sensors and the accuracy and specificity of the data they provide. Interoperability of systems within the organization or with customers or suppliers, and the ability to reconcile data from disparate systems, could be deciding factors in whether the information can be used for audit purposes. Auditors may also need to test internal controls in areas of the organization where they have not previously ventured.

The ability to leverage IoT data as audit evidence presents vast opportunities. Data can be captured in real time to provide the auditor with a live picture that enhances transparency into operations. Results can be interpreted and insights delivered in mere minutes or hours, rather than weeks. IoT data can augment the risk assessment process and provide new ways to test management's assertions. Manual inventory counts could be transformed by IoT, including GPS technology, to track inventory throughout the product life cycle. For example, an auditor can validate sales to customers through inventory transferred from shipper to customer or the assumptions underlying management's estimates for depreciation using IoT diagnostic data from machinery. Access to this type of data can enhance the timeliness and quality of the analysis supporting an auditor's conclusions.

Both external and internal auditors will need additional skills and expertise. The audit committee should keep abreast of these needs, and how they are being met, as part of their oversight duties.

IoT will be one of the critical elements to enabling continuous auditing. Organizations will continue to improve their ability to analyze and use the data they collect through IoT and other sensing technologies. While companies and their external and internal auditors are preparing for this eventuality, boards and their audit committees should be considering how the organization is aligning uses of the technology with its reporting systems and decision-making processes, as well as the associated risks and opportunities.
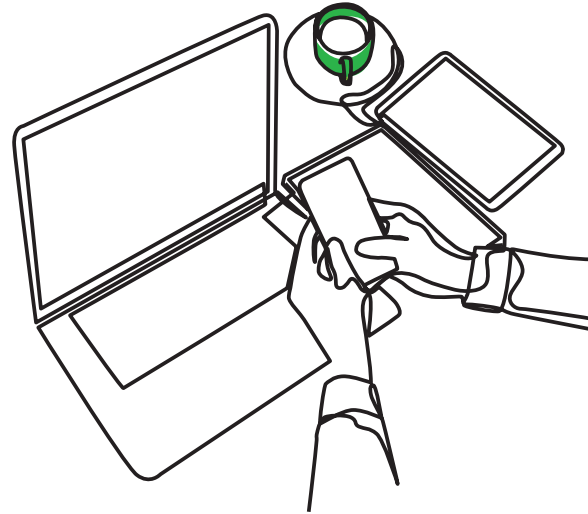
Contact us

Chad Shaver
416-775-7029
cshaver@deloitte.ca

Nicole Deschamps
519-967-7753
nideschamps@deloitte.ca

www.deloitte.ca