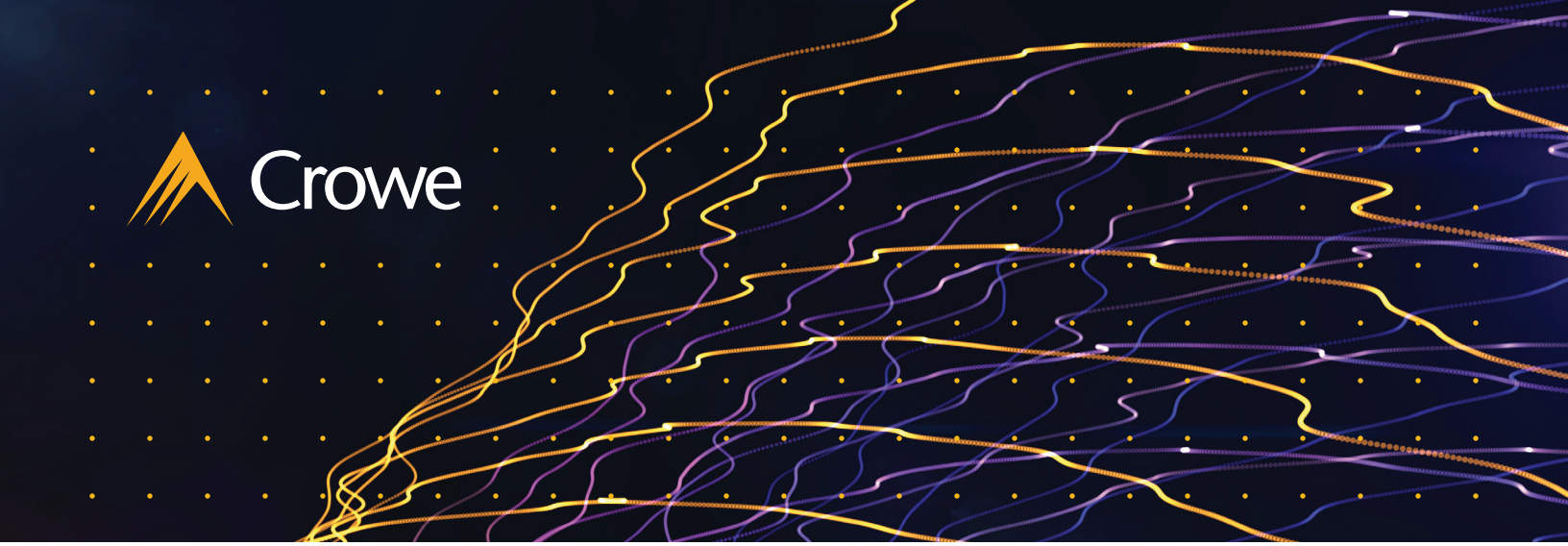

Preparing Internal Audit for Blockchain

A checklist by Michael W. High; Richard C. Kloch, Jr., CPA; and Simon J. Little, CPA

As blockchain networks become more widespread in business organizations, the responsibilities of internal audit departments are likely to expand. Even if their organizations do not embrace blockchain directly, their suppliers, customers, or other third parties are likely to adopt blockchain applications that will affect their transactions.

At a minimum, internal auditors will need to develop a working knowledge of blockchain functions and risks so that proper controls and risk mitigation efforts can be developed, implemented, and evaluated. The following checklist, drawn from a recent joint research report by the Internal Audit Foundation and Crowe, can help internal audit departments prepare for growing exposure to this transformative technology.

To prepare for blockchain adoption, internal audit should:

✓ Recognize and evaluate potential blockchain applications.

- Blockchain-driven "smart contracts," which require that a specific contract milestone must be met before the next transaction can take place, can be applied across a broad range of business functions and processes.
- An important early step is to verify that blockchain is indeed the most appropriate solution for the business functions being addressed.
- Smart contracts can be used to verify compliance with contract terms, automate routine work processes, track the origins and history of goods and materials, and safeguard the privacy and accuracy of medical and financial records, among many other applications.
- Blockchains can support and enhance other digital technologies such as artificial intelligence, machine learning, robotic process automation, advanced data analytics, 3D printing, and the internet of things (IoT).

✓ Analyze blockchain's impact on internal audit.

- Internal audit will need to adjust its capabilities to validate that individual blockchain components such as access permission, encryption, and cryptographic and transaction codes are functioning correctly.
- Relevant governance, risk management, and control procedures also will require internal audit review.
- Recent research suggests many internal audit professionals do not think they are prepared to address blockchain adoption in their organizations.

✓ Develop necessary resources and human capital.

- Internal auditors – both new hires and existing staff – are likely to need specialized training to evaluate risks associated with blockchain.
- Internal audit departments should expand their recruitment efforts to include candidates with technical skills such as coding or cybersecurity.
- In the absence of adequate in-house capabilities, outside firms with specialized skills can provide needed depth and expertise.

Learn more

Mike High
+1 954 489 7423
mike.high@crowe.com

Rich Kloch
Partner
+1 818 325 8424
rich.kloch@crowe.com

Simon Little
+1 214 777 5235
simon.little@crowe.com

For additional information, download the entire report at:

lp.crowe.com/bcia

✓ Identify major categories of risk associated with blockchain adoption.

- Internal audit must determine that existing confidentiality protections are adapted as necessary to accommodate the use of blockchain.
- The inherent risk associated with a blockchain network will vary, depending on the number of nodes on the network, and the presence or absence of backup nodes.
- As more entities are added to a blockchain, and as smart contracts increase in complexity, the risks of error, security beaches, or other vulnerabilities also increase.

✓ Evaluate and validate relevant controls.

- Internal audit must evaluate the types and volume of data on the network to determine that codes, control procedures, and data storage controls are appropriate and functioning as designed.
- The effectiveness of access controls, which grant different users varying levels of access, must be evaluated and verified by internal audit.
- The handoffs or transition points where the blockchain interacts with other business systems require adequate controls.

✓ Implement effective risk mitigation, management, and governance.

- Long-term internal audit strategies must be updated to incorporate activities that demonstrate blockchain systems are functioning as intended.
- Cybersecurity enhancements include the validation of permitted nodes, the development of smart contracts, and the management of external interactions.
- Internal audit must address relevant governance issues such as security guidelines, procedures for adding and removing nodes, and various digital signature components and verification algorithms.