



Exploresearch

Impact Factor (Cosmos: 6.262 & I2OR: 3.585)

© Copyright by MGM Publishing House (MGMPH)

www.mgmpublications.com



Recent Trends in Auditing

Dr. Neelu Jain¹ & Dr. Pooja Purohit^{2*}

^{1,2}Assistant Professor, Department of ABST, S.S. Jain Subodh P.G. College, Jaipur.

*Corresponding author: saraswat_pooja@yahoo.co.in

Citation: Jain, N. & Purohit, P. (2026). Recent Trends in Auditing. *Exploresearch*, 03(02), 175-189. <https://doi.org/10.62823/ExRe/2026/03/02.231>

Article History:

Received: 22 May 2026

Revised: 05 June 2026

Accepted: 12 June 2026

Published: 24 June 2026

Keywords:

Data Analytics, Continuous Auditing, ESG Assurance, Cybersecurity Auditing, Remote Auditing.

Abstract: In recent times, there has been tremendous change in the field of auditing. These changes emanate from technological advancement, regulatory reforms, and the changing expectations from the stakeholders of auditing professionals. In this chapter, the developments in the current audit environment are analyzed. The focus will be on the impact of technological advances such as the use of Artificial Intelligence and data analytics as well as the adoption of continuous auditing among other issues. Environmental, social, and governance concerns are becoming an increasingly important aspect of audit activity. There has been growing recognition of corporate responsibility within various organizations and the need for greater emphasis on sustainable development. The changing audit landscape requires greater scope of the audit process and new competencies for the practitioner. These concerns are addressed in this chapter in relation to the evolution of audit practice. As information technology becomes increasingly sophisticated, so too do the cybersecurity risks associated with it. It is incumbent upon the auditing professional to develop knowledge and competencies adequate to evaluate the organization's controls related to information systems as part of an audit. The use of blockchain technology poses its own set of challenges for audits. The use of remote auditing, made imperative by global conditions, has revolutionized approaches to engagement delivery models. Inspection methodologies, document review using electronic technology, and videoconferencing have become part and parcel of the auditor's repertoire. Issues pertaining to audit quality, independence, and professionalism still need to be tackled in this new environment. This chapter serves as an important tool that gives practitioners, students, and other interested parties a grasp of all these issues. It brings together relevant regulations, professional standards, and research findings into one cohesive picture of where the auditing profession is headed.

Introduction

Audit is at the heart of ensuring the credibility of the financial markets through independent confirmation, which assists all parties involved to make sound judgments based on factual information. Auditing as a practice has seen many changes from its early days due to various factors. Nevertheless, change in recent years has been quite fast, forcing all auditing practitioners to re-evaluate their practices, techniques, and skillset.

Some key trends have been driving change in the auditing profession:

- **Technological Disruption:** The development of advanced computing power, machine learning techniques, and complex software platforms has opened up new avenues for audit evidence collection and analysis
- **Regulatory Changes:** Regulatory authorities and standard-setting bodies around the world have revised their standards to keep up with changing risks and increased demands for transparency
- **Expectations of Stakeholders:** Stakeholders now expect audit reports to cover more than just financial statement audits
- **Complexity of Business:** Global activities, complex financial products, and interlinked systems have presented auditors with increased difficulties
- **Changes in the Risk Environment:** Auditors need to pay attention to the rising risks related to cybersecurity, climate change, and geopolitics

This chapter thoroughly discusses eight significant trends influencing modern auditing practice. Each trend is discussed within its theoretical background, application, challenges, and potential implications.

Technology-Driven Auditing

- **The Digital Transformation of Audit**

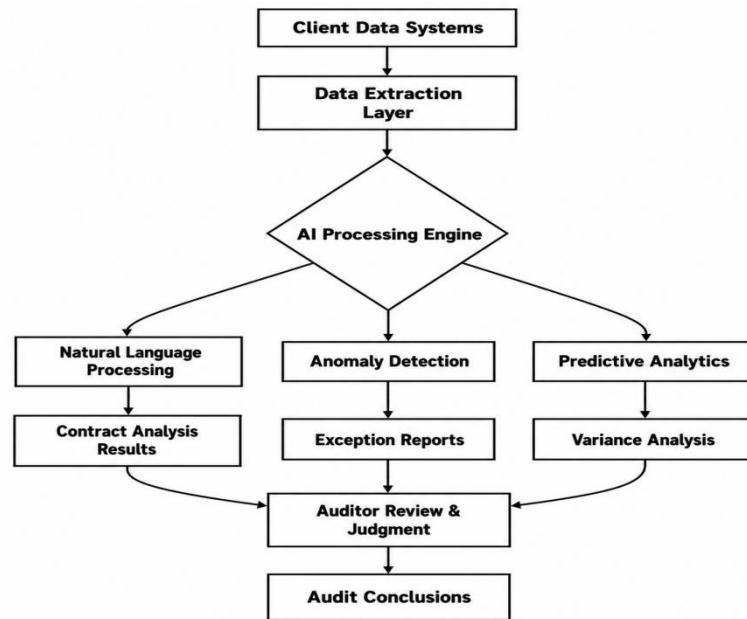
Technology has played a role in auditing all along, with calculators and spreadsheets being examples. Current technology is, however, a step beyond that – it is no longer just an improvement on the earlier technologies. Today's technologies enable auditors to use tools capable of working with an entire population of transactions, finding any irregularities in their patterns, and doing away with routine tasks.

This basic objective of auditing – getting evidence – has not changed. Technology simply changes the way it is achieved.

- **Artificial Intelligence and Machine Learning**

Applications of AI in the field of auditing include:

- **Natural Language Processing:** AI can be used to analyze contracts, agreements, and correspondence, identifying key terms and potential problems within them. Auditors do not need to scan through a thousand pages of paperwork by themselves, but can use computer programs that will flag anything that needs to be looked at more carefully.
- **Anomaly Detection:** By analyzing past patterns in data, machines are able to find unusual transactions or anomalies. They know what is considered normal for that company, and then flag any deviations for review.
- **Predictive Analytics:** AI can provide expectations for how much should be in an account or how many transactions should take place.
- **Process Automation:** Robotic process automation can do things like data gathering, reconciliations, and matching confirmations.



• Data Analytics in Practice

Data analytics has moved from experimental applications to mainstream audit methodology. The following table illustrates common applications across audit areas:

Audit Area	Analytics Application	Benefit
Revenue	Complete transaction population analysis	Identifies gaps in sequence numbering, unusual pricing, timing anomalies
Payroll	Ghost employee detection, duplicate payment identification	Catches fraudulent or erroneous payments
Inventory	Age analysis, turnover pattern assessment	Highlights obsolescence risks, valuation concerns
Accounts Payable	Duplicate invoice detection, vendor analysis	Identifies control weaknesses, potential fraud
Journal Entries	Unusual entry identification, preparer analysis	Focuses testing on high-risk manual adjustments

• Implementation Considerations

Technology-auditing organizations encounter various obstacles in practice:

- **Quality and Availability of Data:** The reliability of analytical techniques relies on quality of the data; format differences and insufficient information can hinder successful adoption
- **Learning Process:** Staff have to be trained in order to utilize new techniques correctly
- **Skepticism:** Results produced by new technologies should be critically analyzed; auditors should avoid excessive trust
- **Documentation Requirements:** Audit documentation should be sufficient for conclusions made using technological methods

Continuous Auditing and Real-Time Assurance

• Moving Beyond Periodic Auditing

The traditional form of auditing works on periodic intervals in which the audit work is done at certain periods—normally one year or a quarter. The nature of this audit leads to time delay in providing assurance as compared to when the transaction occurs. Continuous auditing provides a revolution from the above practice.

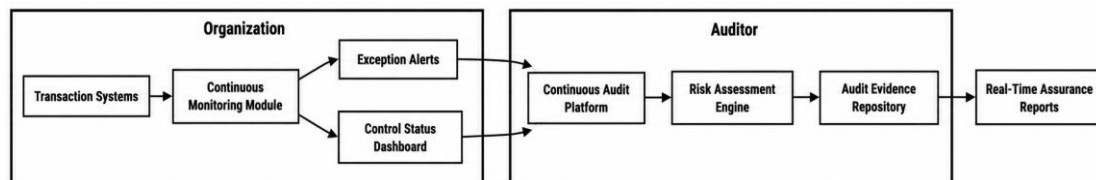
- **Conceptual Framework**

The definition of continuous auditing covers two elements:

- **Continuous Auditing:** The process by which the auditor continuously evaluates transactions and internal controls during the process
- **Continuous Monitoring:** The application by the management of automated methods to measure control and transaction effectiveness

These two elements complement each other since the continuous monitoring of the management forms a base for the auditor's continuous auditing process.

- **Architecture of Continuous Auditing Systems**



The flowchart explains the concept of continuous auditing and real-time assurance within organizations. This starts from the transaction systems that offer information to the continuous monitoring system. From here, the continuous monitoring module analyzes the transactions, and when there is any exception and control issues, they are communicated to the auditor in form of exception messages and control dashboard through the continuous audit platform. The auditor evaluates the information provided by use of risk assessment engine and retains the information in the audit evidence repository. Finally, all the above processes lead to the production of real-time assurance reports.

- **Benefits and Limitations**

Aspect	Benefits	Limitations
Timeliness	Issues identified when they occur, not months later	Requires significant initial investment in systems
Coverage	Can examine 100% of transactions rather than samples	May generate excessive false positives
Efficiency	Reduces year-end workload, spreads effort throughout period	Demands ongoing auditor engagement rather than defined seasons
Relevance	Provides information when it can still influence decisions	Some judgments still require human evaluation at period-end

- **Practical Applications**

The following processes represent some of the most common places to start with continuous auditing initiatives:

- **Accounts Payable:** Continuous comparison of purchase order documentation, receipts, and invoices, with automatic exception reporting
- **Travel and Expenses:** Continuous review of expense submissions in relation to pre-defined policy parameters
- **Access Control:** Continuous monitoring of user access rights, conflicts between segregation of duties, and other privilege-related issues
- **Inventory Movements:** Continuous monitoring of inventory transfer activity and adjustments

Environmental, Social, and Governance Auditing

- **The Rise of ESG Assurance**

There is rising pressure from stakeholders for organizations to be accountable for the impact that they create outside the bottom line of financials. Organizational environmental sustainability, social responsibility, and good governance have all become important factors in investments, regulatory concerns, and the workplace.

- **Regulatory Developments**

Many places have made provisions for, or suggested mandatory ESG reporting and verification:

- European Union's Corporate Sustainability Reporting Directive mandates assurance of sustainability information by companies
- Climate disclosures are being proposed by securities regulators in several nations, mandating attestation of the disclosures
- Sustainability reporting is becoming part of the stock exchange listing process

- **Scope of ESG Auditing**

ESG audit is conducted to verify whether an organization performs in accordance with the principles of Environment, Social and Governance performance. ESG practices provide information for determining the extent of organizational responsibility, sustainability, and ethicality. An ESG audit encompasses both financial and non-financial practices within an organization. Also, ESG auditing involves verification of the reliability and accuracy of information provided by organizations.

- **Environmental Component**

The environmental component of ESG auditing assesses the impacts of organization activities on the natural environment. It is essential that businesses today contribute to minimizing pollution of the environment and adopting sustainable practices. Auditors verify the extent to which companies measure and disclose their environmental activities.

- **Measurement and Disclosure of Greenhouse Gas Emissions**

Companies generate greenhouse gas emissions such as carbon dioxide while conducting production processes, delivering products from place to place and using different forms of energy. An auditor evaluates whether organizations measure and report these emissions in accordance with accepted norms.

- **Usage and Efficiency of Energy**

An auditor verifies the efficiency of energy usage by companies. Companies use electricity, fossil fuels, and energy derived from different sources. An audit assesses the extent to which energy resources are used efficiently.

- **Use of Water and Its Discharge**

Many businesses rely on water during production. Auditors assess the amount of water used by the business, the proper conservation of water, and whether there is safe treatment of the water before it is discharged to nature. Proper water management indicates corporate environmental responsibility.

- **Types of Waste Produced and Recycled**

Different businesses produce waste during their operations. The type of waste produced and its recycling by the business indicate corporate environmental responsibility.

- **Assessment of Biodiversity Impact**

The development projects carried out by organizations such as construction projects, mines, and industries may adversely impact the environment by affecting the forests, animal life, and the ecosystem.

- **Social Aspect**

Social aspects of ESG auditing revolve around how companies treat their employees, customers, suppliers, and local communities. This entails checking whether the organization has healthy, safe, and ethical interactions with those people that have connections with their businesses.

- **Metrics for Workforce Diversity and Inclusion**

In today's business world, companies must ensure that they offer equal opportunities irrespective of gender, age, race, or religious affiliations. The audit entails assessing statistics and policies aimed at ensuring fair play and inclusivity.

- **Worker Safety Performance**

Keeping workers safe and healthy should be the priority of any organization. ESG auditors measure performance by looking into safety measures, accidents, health programs, and labor safety laws followed by the organization.

- **Human Rights Risk Assessment**

Organizations need to ensure they adhere to fundamental human rights while conducting their businesses. This involves measuring risks associated with child labor, forced labor, discrimination, and exploitation.

- **Community Involvement and Impact**

Corporations affect the community in which they operate. The ESG auditors will examine whether companies offer positive contributions to the community in terms of job creation, educational programs, environmental actions, or other forms of social responsibility. Good community relations are important for sustained development.

- **Labor Practice in the Supply Chain**

Business operations rely on suppliers and contractors, among others. ESG auditors will examine whether suppliers practice ethical labor practices by paying fair wages and maintaining proper work environments.

- **Governance Component**

Governance is associated with the framework within which corporations are managed. Proper governance promotes accountability, ethics, and transparency.

- **Board Structure and Effectiveness**

Corporate boards are responsible for the management of business. ESG auditors will analyze whether the board is composed of capable and independent board members that can effectively guide the business.

- **Alignment of Executive Compensation**

Organizations must align their executives' compensation with their performance and good ethics. Auditors check the compensation policies of companies to see if they encourage responsible management.

- **Ethics and Anti-Corruption Initiatives**

Firms must avoid corrupt and fraudulent actions. ESG auditors check if there are sufficient ethical policies, trainings for employees, whistleblower systems, and anti-corruption initiatives at the organizations.

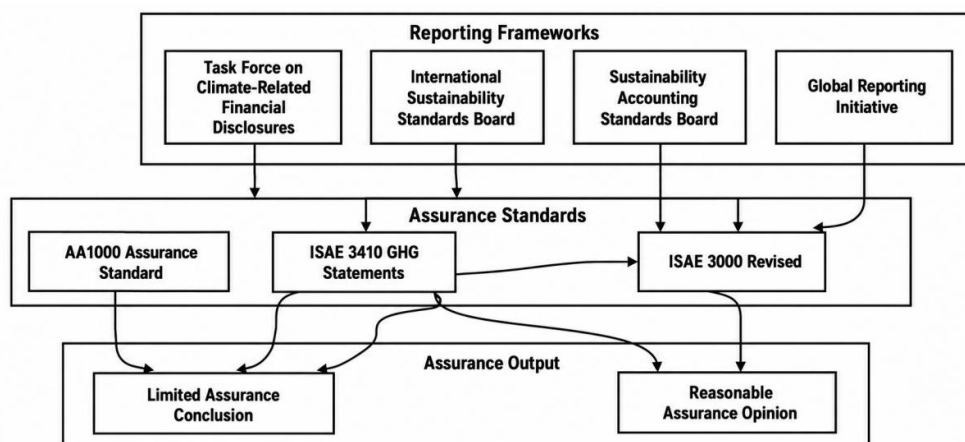
- **Risk Management Systems**

All organizations carry certain risks related to finances, operations, technology, and sustainability. Auditors need to see whether the management has an adequate risk management system in place.

- **Processes for Engaging Stakeholders**

Companies engage with their stakeholders including shareholders, employees, consumers, authorities, and society. Auditors evaluate the effectiveness of communication with stakeholders.

Assurance Standards and Frameworks



The flow chart depicts the connection between reporting frameworks, assurance standards, and assurance outputs in environmental, social, and governance (ESG) audits. The reporting frameworks consist of Task Force on Climate-Related Financial Disclosures (TCFD), International Sustainability Standards Board (ISSB), Sustainability Accounting Standards Board (SASB), and Global Reporting Initiative (GRI). The above frameworks serve as the basis for guiding organizations in preparing their sustainability reports. In addition, assurance standards such as AA1000 Assurance Standard, ISAE 3410 greenhouse gas statement, and ISAE 3000 Revised offer guidance to auditors in verifying the validity of the sustainability report. The outputs resulting from the use of the assurance standards include either a limited assurance conclusion or reasonable assurance conclusion.

Challenges in ESG Assurance

ESG auditing presents unique challenges compared to traditional financial auditing:

Challenge	Description	Auditor Response
Data reliability	ESG metrics often come from systems not designed for external reporting	Enhanced testing of data capture processes, verification to source documents
Measurement uncertainty	Many ESG metrics involve estimation and judgment	Understanding methodologies, assessing reasonableness of assumptions
Evolving standards	Reporting frameworks continue to develop	Staying current with requirements, flexible engagement approaches
Competency requirements	Subject matter expertise beyond traditional accounting	Building multidisciplinary teams, obtaining specialist input
Scope boundaries	Organizational and operational boundaries may differ from financial reporting	Clear boundary definition, consideration of value chain impacts

Practical Procedures

Auditors performing ESG assurance engage in procedures including:

- Evaluating the appropriateness of reporting frameworks selected by management
- Assessing the completeness of material topics included in disclosures
- Testing the accuracy of quantitative metrics through recalculation and verification to source data
- Evaluating the consistency of qualitative statements with supporting evidence
- Considering the balance and neutrality of overall presentation

Cybersecurity Auditing

• The Imperative for Cybersecurity Assurance

Organizations experience constant threats to their information systems. These attacks affect data security, operations, and cause considerable financial and reputational losses to the firm. There is a growing demand from the stakeholders for the assurance that these organizations have proper cybersecurity.

• Cybersecurity Audit Objectives

The various purposes of cybersecurity audit include:

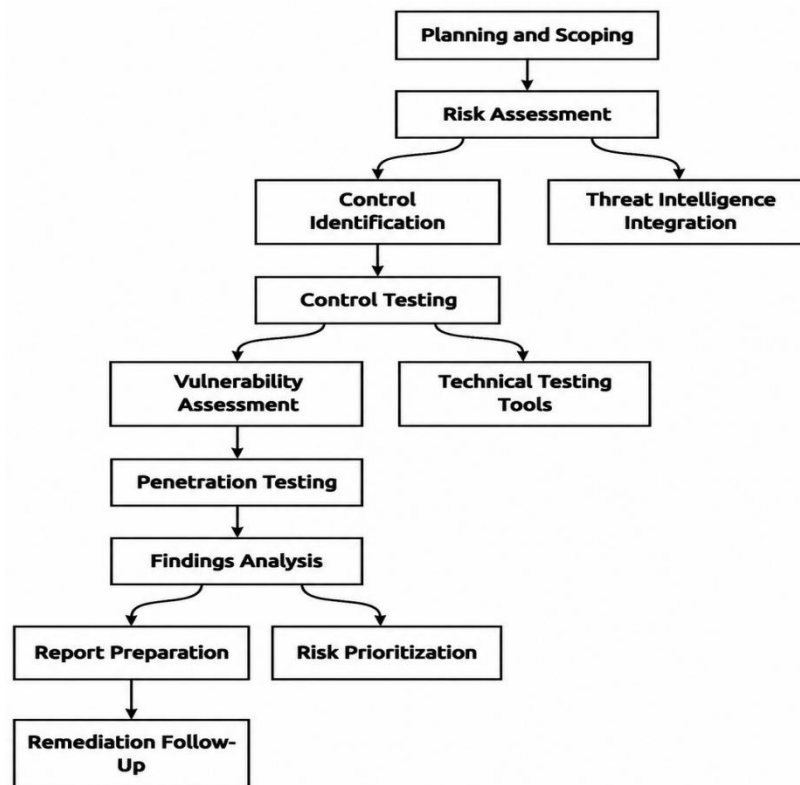
- **Risk Assessment:** To find out the vulnerabilities and threat that may affect the information asset
- **Control Testing:** To check the effectiveness of control measures in addressing the risk assessed
- **Verification of Compliance:** To verify the organization's compliance with applicable laws and regulations
- **Incident Response Readiness:** Assessing the readiness of the organization to handle security incident responses

Framework-Based Approach

Cybersecurity auditing typically references established frameworks that define control expectations:

Framework	Focus	Common Application
NIST Cybersecurity Framework	Risk management approach across five functions	US organizations, critical infrastructure
ISO 27001/27002	Information security management system requirements	International organizations seeking certification
CIS Controls	Prioritized security actions	Organizations seeking practical implementation guidance
COBIT	IT governance and management	Organizations integrating cybersecurity with broader IT governance
SOC 2	Trust service criteria for service organizations	Technology and service companies providing assurance to customers

Cybersecurity Audit Process



This illustration depicts the process involved in a cybersecurity audit and risk assessment model adopted by companies to detect and manage security threats. This process starts with planning and scoping, which involves defining the scope and objectives for conducting the audit. Following planning and scoping is the risk assessment stage, which aids in identifying potential security threats. The next step in this process involves control identification and threat intelligence integration, through which one understands existing security risks as well as protective controls that can be put in place. Control testing is the next process and this involves carrying out technical testing and vulnerability assessments. Penetration tests are conducted to simulate real attacks in order to detect any weakness in the security process. Findings from the audit process are subsequently evaluated in terms of risk levels and the need to take specific actions. The process concludes with reporting, risk prioritization, and remediation processes.

Key Audit Areas

Comprehensive cybersecurity audits examine multiple domains:

- **Governance and Strategy**
 - Board and management oversight of cybersecurity
 - Cybersecurity strategy alignment with business objectives
 - Resource allocation for security initiatives
- **Technical Controls**
 - Network security architecture and segmentation
 - Endpoint protection mechanisms
 - Encryption practices for data at rest and in transit
 - Access control and identity management
 - Patch management processes
- **Operational Security**
 - Security monitoring and logging
 - Incident detection and response capabilities
 - Backup and recovery procedures
 - Third-party and supply chain risk management
- **Human Factors**
 - Security awareness training programs
 - Phishing susceptibility and social engineering resilience
 - Personnel security practices

Auditor Competencies

Cybersecurity auditing requires expertise that extends beyond traditional audit practices:

- Understanding of networking architecture and technologies
- Understanding of typical attack vectors used by cyber attackers
- Ability to analyze the findings of vulnerability scans and penetration tests
- Knowledge of pertinent regulation standards

A lot of audit firms hire cybersecurity specialists in order to complement their traditional audit staff.

Remote and Digital Auditing

Transformation of Audit Delivery

However, current global trends in the recent past have hastened the uptake of remote auditing techniques that were slowly coming up before. The need has since developed into becoming part of contemporary audit practice. There are some places where remote auditing is efficient, although there are other places where being physically present still makes sense.

Remote Auditing Techniques

Techniques used for remote auditing include:

- **Video Conferencing:** Auditors and clients can communicate in real-time in a virtual environment
- **Screen Sharing:** Clients are able to share demonstrations on screen as auditors view the same remotely
- **Electronic Document Exchange:** Platforms where documentation can be exchanged and viewed by auditors
- **Digital Confirmation:** Third party confirmations that can be done electronically

- **Virtual Inventory Observation:** The use of video technology to observe inventory counts

- **Comparison of Traditional and Remote Approaches**

Element	Traditional Approach	Remote Approach
Document review	Physical examination at client premises	Electronic documents reviewed on secure platforms
Interviews	In-person meetings	Video conferences with recording capabilities
Inventory observation	Physical attendance at count locations	Live video feeds with virtual walk-throughs
Asset inspection	Direct physical examination	Photographs, videos, and technology-enabled verification
System walkthroughs	On-site observation and testing	Screen sharing and remote access to test environments

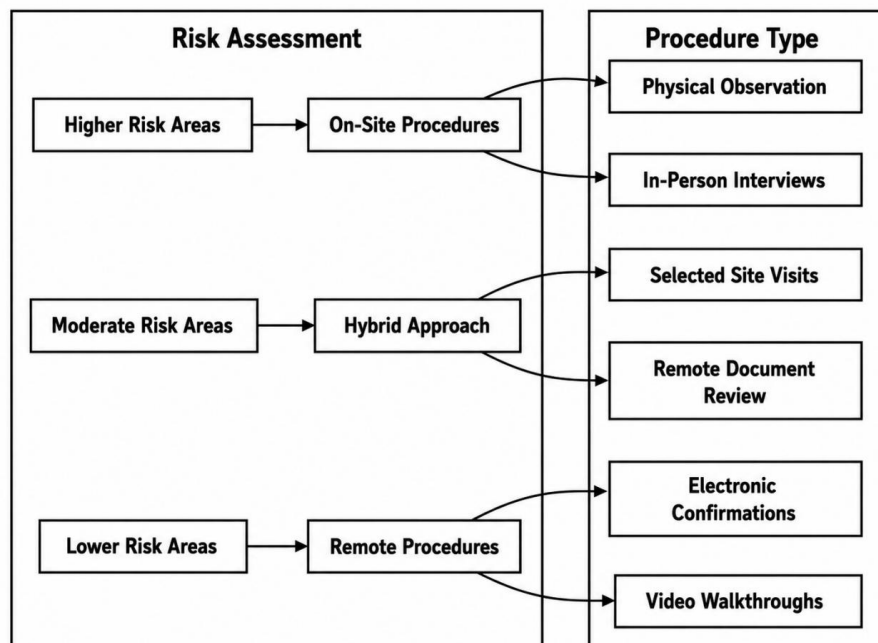
- **Quality Considerations**

Issues relating to remote auditing arise in terms of quality control considerations:

- **Authenticity of Evidence:** Measures to ensure that evidence collected in digital form is authentic and unchanged
- **Restrictions on Observations:** Understanding that video observations may not reveal everything observable in person
- **Difficulty with Communication:** Appreciating body language and interpersonal relationships within virtual audits
- **Security of Data:** Protecting data that is electronically transferred and stored from misuse or breach
- **Proper Documentation:** Properly documenting evidence in audit files for drawing conclusions from digital evidence

- **Hybrid Models**

Most organizations have adopted hybrid approaches that combine remote and on-site elements based on risk assessment and practical considerations:



In this diagram, the process through which audit procedures are determined in relation to the degree of risk identified in the risk assessment is depicted. Areas that have been identified as having high risks have on-the-ground audit procedures because of their uncertainties and need for confirmation. The procedures used in high-risk areas include observation procedures and physical meetings where audit evidence is obtained. Areas with moderate risks adopt the mixed procedure, which entails physical and off-the-ground procedures, such as selected site meetings and remote document reviews. Lastly, low-risk areas have predominantly off-the-ground audit procedures like electronic confirmation and video review, saving both time and money.

Blockchain and Distributed Ledger Technology

• Understanding Blockchain Relevance to Auditing

Blockchain technology enables the recording of immutable, distributed ledgers that multiple parties can review without the need for a third-party authority. This has potential effects not only on the environment being audited but also on the auditing techniques that can be used.

• Blockchain Features of Potential Interest to Auditors

A number of blockchain features have relevance to audit activities:

- **Immutability:** The inability to alter transaction records once made can lead to more reliable transaction records.
- **Transparency:** Access to transaction history is available to all participants, leading to better insight into transaction flows.
- **Decentralization:** There is no single authority that maintains the ledger; this presents certain fraud risks.
- **Smart Contracts:** Automated contract execution based upon certain conditions.

• Audit Implications

Blockchain Aspect	Audit Opportunity	Audit Challenge
Immutable transaction records	Reliable audit trail, reduced alteration risk	Understanding technical architecture, verifying initial data accuracy
Real-time transaction visibility	Continuous monitoring capability	Managing large data volumes, interpreting complex transactions
Smart contract automation	Control testing through code review	Assessing code logic, understanding technical dependencies
Decentralized consensus	Reduced reliance on single-party confirmations	Evaluating consensus mechanism reliability

• Practical Audit Considerations

In the auditing of organizations making use of blockchain, auditors should focus on the following matters:

- **Assessment of Governance:** In what ways does the firm get involved in blockchain governance? What control mechanisms govern node activity?
- **Cryptographic Key Management:** How are the cryptographic keys for conducting transactions managed?
- **Audit of Smart Contracts:** Has an audit been done of the code? How do the change management processes work?
- **Value of Crypto Assets:** What methods of valuation of digital assets are applied? Can fair value calculations be justified?
- **Regulation of Digital Assets:** How does the firm handle regulations relating to digital assets and blockchain?

• Future Possibilities

Blockchain technology could someday allow for:

- Access to transaction logs straight from distributed ledger systems, not from the client system

- Assurance on transactions that happen in real time
- The automation of assurance process through distributed ledgers
- The improved verification of supply chains using distributed ledger technology

The above scenarios remain speculative, as the application is still limited to select areas.

Regulatory and Standards Evolution

• Responding to a Changing Environment

As technology evolves and issues of auditing quality persist, auditing standards and regulations continue to change in order to meet these challenges.

• Major Issues in Standards Development

- **Quality Management:** The IAASB issued quality management standards that required organizations to put in place systems to manage risks related to quality.
- **Going Concern:** Standards have been amended to make the assessment of going concern risk and reporting requirements more stringent.
- **Audit Evidence:** Various projects have been initiated to update evidence standards with respect to changes in the environment and types of audit evidence.
- **Fraud:** New focus on auditor responsibilities with respect to fraud risk assessment and response.
- **Group Audits:** Standards relating to the audits of group financial statements including communication between component auditors.

• Regulatory Developments

Regulators worldwide have intensified focus on audit quality:

Jurisdiction	Regulatory Development	Impact
United States	PCAOB inspection and enforcement activities	Enhanced scrutiny of large audit firms, focus on quality control
European Union	Audit reform implementation	Mandatory rotation, prohibited non-audit services, public interest entity requirements
United Kingdom	Audit market study recommendations	Proposals for operational separation, enhanced accountability
International	IOSCO statements on audit quality	Coordination of regulatory expectations across jurisdictions

• Technology-Specific Guidance

Technology-based standards and regulations are being developed to cover technology-related matters, including:

- Usage of technology and artificial intelligence in audits
- Provisions for audits of estimates with complex models
- Factors to consider in the audit of blockchain ledger entries
- Cybersecurity disclosure and related audit procedures

Emerging Trends and Future Directions

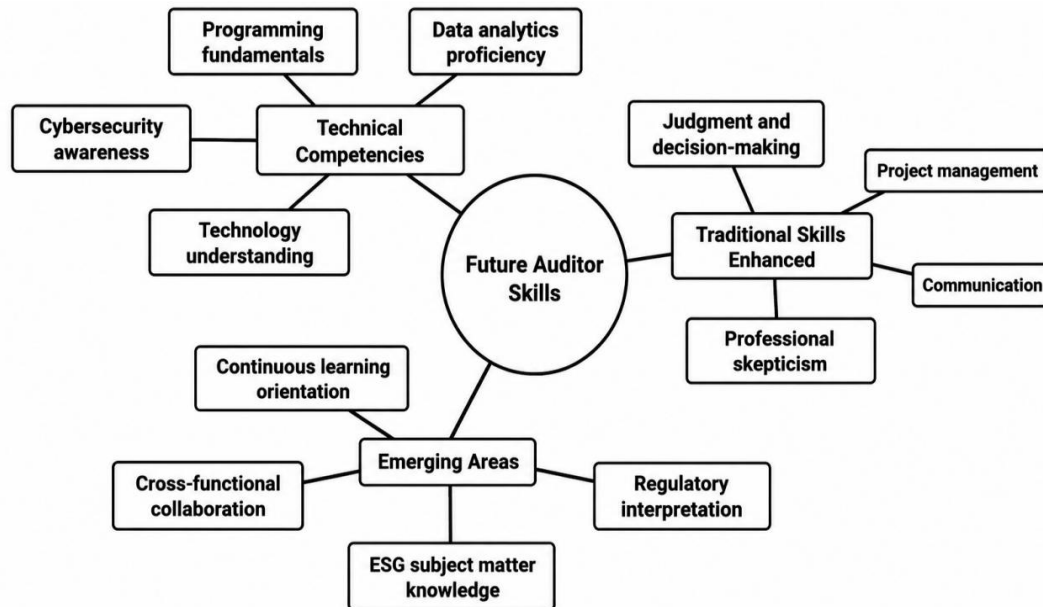
• Looking Ahead

The following trends are expected to influence auditing in the years ahead:

- **Integrated Assurance:** Trend towards integrated assurance that takes into consideration financial, sustainability, and operational performance
- **Predictive Auditing:** Use of predictive techniques to identify any potential problems or risks prior to their occurrence
- **Increased Scope:** Role of auditors beyond traditional financial statements to include other areas like forward-looking information
- **Real-Time Reporting:** Synchronization of audit process with real-time reporting by the companies

- **Skills Required for Future Auditors**

The new environment requires enhanced skills from the auditor:



This diagram illustrates the key skills that future auditors should have considering the fast-evolving environment in terms of both business and technologies. At the core of this concept there are "Future Auditor Skills" that are supplemented by three key areas: technical competencies, enhancement of traditional skills, and new knowledge areas. Technical competencies are comprised of basics of programming, data analysis skills, cybersecurity, and knowledge of technologies. The significance of these skills is growing due to the fact that contemporary audit is highly dependent on technologies, automation, artificial intelligence, and vast amounts of data. Auditors should be able to analyze digital data and comprehend related technological risks.

The next area relates to the traditional skill set, which will always be relevant for the role of an auditor. It includes judgment and decision-making skills, communication skills, professional skepticism, and project management skills. Despite having advanced technology at their disposal, auditors still require critical thinking and professional judgment in order to assess evidence and make decisions. Communication skills would also assist auditors in dealing with all interested parties, including their clients, management, government agencies, and others.

Finally, the last part of the diagram discusses the emerging areas that are vital for the future of the auditing profession. These emerging areas relate to the auditor's expertise in ESG subject matters, understanding of regulations and how to interpret them, cross-functional collaboration, and willingness to engage in continuous learning activities. Today, organizations have many challenges to deal with in terms of sustainability, governance, and compliance, and the role of an auditor needs to be expanded accordingly. Since technology, regulations, and business environment keep changing, auditors will have to be ready to acquire new knowledge and skills on an ongoing basis.

- **Balancing Innovation and Fundamentals**

In adopting modern technology and wider reach, the profession should not lose sight of essential values:

- Independence and objectivity remain non-negotiable irrespective of how work is done
- Professional doubt applies just as much to technology-based work as to all others
- Work should not be sacrificed for speed
- Ethical considerations still apply

Conclusion

The auditing profession is currently at an important crossroad in its development. There is no doubt that technology presents great opportunities for improving the quality, effectiveness, and relevance of audits. Expectations on audits have shifted from merely providing financial assurance to include sustainability, cybersecurity, and overall organizational performance.

However, moving through the transition phase will require auditors to embrace change while upholding core values. Technology complements but does not replace professional skepticism. The new fields of audit assurance need expertise in subject matter but must still have the ability to evaluate evidence objectively and critically.

It is important for organizations that involve auditors to have professionals who are well-versed in new tools and approaches, yet remain firmly rooted in long-lasting principles. The audit of tomorrow will not be like the audit of yesterday; however, the objective behind the auditing process is the same.

These trends described in this chapter are not the final destination of the road, but only milestones along the way. Audit will keep changing with time due to advancements in technology, change in stakeholder requirements, and changes in the business environment. Those professionals willing to adapt to the changing world will succeed.

References

1. American Institute of Certified Public Accountants. (2023). *SOC for cybersecurity guide: Reporting on an entity's cybersecurity risk management program and controls*. AICPA.
2. Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise risk management: Integrating with strategy and performance*. COSO.
3. European Commission. (2022). *Corporate Sustainability Reporting Directive (CSRD)*. European Union Publications Office.
4. Global Reporting Initiative. (2021). *GRI sustainability reporting standards*. GRI.
5. Institute of Internal Auditors. (2020). *Global technology audit guide: Understanding and auditing big data*. IIA.
6. Institute of Internal Auditors. (2022). *International professional practices framework (IPPF)*. IIA.
7. International Auditing and Assurance Standards Board. (2021). *International Standard on Auditing (ISA) 315 (Revised 2019): Identifying and assessing the risks of material misstatement*. IFAC.
8. International Auditing and Assurance Standards Board. (2020). *International Standard on Assurance Engagements (ISAE) 3000 (Revised): Assurance engagements other than audits or reviews of historical financial information*. IFAC.
9. International Auditing and Assurance Standards Board. (2021). *International Standard on Quality Management (ISQM) 1*. IFAC.
10. International Organization for Standardization. (2022). *ISO/IEC 27001: Information security, cybersecurity and privacy protection — Information security management systems*. ISO.
11. International Sustainability Standards Board. (2023). *IFRS S1 General requirements for disclosure of sustainability-related financial information*. IFRS Foundation.
12. International Sustainability Standards Board. (2023). *IFRS S2 Climate-related disclosures*. IFRS Foundation.
13. National Institute of Standards and Technology. (2024). *Cybersecurity framework (CSF) 2.0*. U.S. Department of Commerce.
14. Public Company Accounting Oversight Board. (2023). *Spotlight: Staff priorities for inspections and interactions with audit committees*. PCAOB.
15. Sustainability Accounting Standards Board. (2021). *SASB conceptual framework*. SASB.
16. Appelbaum, D., Kogan, A., & Vasarhelyi, M. A. (2017). Big data and analytics in the modern audit engagement: Research needs. *Auditing: A Journal of Practice & Theory*, 36(4), 1–27.
16. Alles, M. G. (2015). Drivers of the use and facilitators and obstacles of the evolution of big data by the audit profession. *Accounting Horizons*, 29(2), 439–449.

17. Brown-Liburd, H., Issa, H., & Lombardi, D. (2015). Behavioral implications of big data's impact on audit judgment and decision making. *Accounting Horizons*, 29(2), 451–468.
18. Dai, J., & Vasarhelyi, M. A. (2017). Toward blockchain-based accounting and assurance. *Journal of Information Systems*, 31(3), 5–21.
19. Porter, B., Simon, J., & Hatherly, D. (2014). *Principles of external auditing* (4th ed.). Wiley.
20. Arens, A. A., Elder, R. J., & Beasley, M. S. (2022). *Auditing and assurance services: An integrated approach* (18th ed.). Pearson.
21. Messier, W. F., Glover, S. M., & Prawitt, D. F. (2022). *Auditing and assurance services: A systematic approach* (12th ed.). McGraw-Hill Education.
22. Knechel, W. R., & Salterio, S. E. (2016). *Auditing: Assurance and risk* (4th ed.). Routledge.
23. Vasarhelyi, M. A., Kogan, A., & Tuttle, B. M. (2015). Big data in accounting: An overview. *Accounting Horizons*, 29(2), 381–396.
24. Yoon, K., Hoogduin, L., & Zhang, L. (2015). Big data as complementary audit evidence. *Accounting Horizons*, 29(2), 431–438.

