APPENDIX I: ADDITIONAL IT AUDIT TOPICS OF INTEREST

This appendix provides an overview of some other topics that IT auditors may come across in the course of their audits. The topics discussed in this appendix include

- computer forensics and forensic audits,
- smart devices,
- 5G wireless,
- data mining,
- big data,
- artificial intelligence (AI),
- machine learning and algorithms,
- robotic process automation (RPA), and
- blockchain.

Many emerging areas in IT could become auditable subjects. Thus, auditors should have an awareness of these areas and be able to conduct, if required, audits relating to these subjects.

Even though these areas might have some technical differences or specific aspects, they can be audited using the same approaches and techniques that are being discussed throughout this guidance. They may require some additional audit questions that auditors could develop on their own when dealing with these subjects, depending on the audit objectives.

I. Computer Forensics and Forensic Audits

Computer forensics includes the approach, tools, and techniques to examine digital information for identifying, preserving, recovering, analysing, and presenting facts and opinions about the information stored. It is often considered to be part of an organisation's incident response program where further analyses and investigation are required to identify evidence and data to understand an incident. Computer forensics have also been applied in a number of areas including, but not limited to, fraud, espionage, murder, blackmail, computer misuse, technology abuse, libel, malicious mails, information leakage, theft of intellectual property, pornography, spamming, hacking, and illegal transfer of funds.[1]

Forensic audits are a type of audit that is carried out to examine digital media for evidence regarding an investigation or dispute. These types of audits involve similar techniques and principles as data recovery, but with additional guidelines and practices designed to create a legal audit trail, including

- retaining evidence (e.g., data, access, and log) for analysis;
- capturing and preserving data as close to the breach as possible;
- collecting data following standards for possible law enforcement use;
- using a minimally invasive data capture process without disruption to business operations; and
- identifying attackers, if possible.

[1]ISACA's IT Audit and Assurance Guideline G38 Computer Forensics.

References and Further Reading

Electronic Crime Scene Investigation: A Good Practice Guide for Computer-Based Electronic Evidence.

International Organization for Standardization/International Electrotechnical Commission. *ISO/IEC 27035-2:2016, Information Technology— Security Techniques—Information Security Incident Management.* Geneva, Switzerland: International Organization for Standardization, November 11, 2016.

National Institute of Justice. *Forensic Examination of Digital Evidence: A Guide for Law Enforcement.* http://www.ncjrs.gov/pdffiles1/nij/199408.pdf. April 2004.

Wikipedia. "Computer Forensics." http://en.wikipedia.org/wiki/Computer_forensics.

II. Smart Devices

Smart devices such as smartphones, tablets, and other internet of things (IoT)[2] devices are changing the landscape of how information systems are used. These devices provide portable computing power and the ability to connect to the internet wherever there is Wi-Fi or cellular service. Types of smart devices can vary greatly, but there are some common characteristics associated with smart devices, such as an operating system, voice and data networking, data storage, and global positioning system, among others.[3]

Smart devices can also provide convenient options for working remotely. Traditionally, working remotely consisted of connecting to the organisation's network via a laptop provided by the organisation. However, smart devices have enabled employees to utilise applications and other features to work remotely.

However, smart devices connecting to an organisation's network can introduce new risks. The use of smart devices should be considered when assessing the organisation's security posture. Risks related to smart devices include risks to compliance, privacy, physical security, and information security. Specific risks in these areas include the use of multiple versions of hardware or software, unauthorised access or removal of personally identifiable information, and risks of the device being lost or stolen, among others. In order to reduce the impact of these risks, organisations may implement security and policy controls, such as authentication controls, remote erasing capabilities, hardware encryption, software encryption, data backup, and enterprise device management.

When assessing risks and controls related to smart devices, auditors should, for example:

- understand the organisation's smart device strategy,
- evaluate the effect of smart devices on the organisation's overall technology architecture,
- identify and assess risks introduced by smart devices, and
- determine the adequacy of governance and risk management controls for smart devices.

References and Further Reading

Global Technology Audit Guide. *Auditing Smart Devices*. https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/GTAG-Auditing-Smart-Devices-An-Internal-Auditors-Guide-to-Understanding-and-Auditing-Smart-Devices.aspx.

---

[2]Technologies and devices that sense information and communicate it to the internet or other networks.

[3]Global Technology Audit Guide, *Auditing Smart Devices*, https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/GTAG-Auditing-Smart-Devices-An-Internal-Auditors-Guide-to-Understanding-and-Auditing-Smart-Devices.aspx.

ISACA. *Mobile Computing Security Audit Program.* https://www.isaca.org/bookstore/audit-control-and-security-essentials/wapmcs. 2010.

Salman, Seyed. "Auditing the Internet of Things." *Internal Auditor Magazine*. October 29, 2015.

U.S. Government Accountability Office. *Internet of Things: Status and Implications of an Increasingly Connected World.* GAO-17-75. https://www.gao.gov/products/gao-17-75. May 15, 2017.

III. 5G Wireless

5G, or fifth-generation, is a suite of wireless technologies that has the capability to deliver more reliable and efficient connections to wireless networks. 5G wireless networks promise to deliver significantly improved network performance and greater capabilities, such as greater speeds and higher capacity to accommodate more devices. According to studies on the socioeconomic benefits of 5G, additional potential benefits include increased access and availability to more advanced health care and education, reduced pollution, increased efficiency in transportation, and enhanced public safety response capabilities. 5G network performance is expected to far exceed that of the previous fourth generation as the technology develops over the next decade. Improved network performance is expected to enhance many existing mobile broadband applications and also enable transformative new applications across industries and society.

Major technology enhancements provided by 5G include:

- **Enhanced broadband applications**. Faster connections and higher throughput could enhance applications like cloud services, video streaming, gaming, and augmented reality.
- **IoT**. 5G could connect massive numbers of devices, such as sensors in systems for intelligent transportation and logistics, smart factories, and smart cities. For example, traffic light and road sensors could help reduce the number of car accidents.
- **Mission critical communications**. Ultra-reliable, low latency communications could enable more reliable operation of self-driving vehicles, industrial equipment, robotics, and drones.

While 5G presents new opportunities across many sectors, there are also concerns about cybersecurity risks and other challenges. For example:

- **Infrastructure deployment**. Applications needing low latency and high bandwidth will need significant infrastructure, including fiber optic cables and small cells. This infrastructure could be expensive to deploy and will require skilled labor as well as time for local permitting, planning, and procurement.
- **Cybersecurity**. The large number of 5G network components increases the risk that some components may not be properly configured and secured.
- **Privacy**. 5G networks could allow for much more precise location data because 5G devices are expected to connect to cells that are located much closer together. This more precise location data could increase the risk of user privacy being compromised.

References and Further Reading

Fraunhofer Institute for Production Technology IPT. *5G-Audit.* https://www.ipt.fraunhofer.de/en/Competencies/Productionqualityandmetrology/Productionmetrology/5g-audit.html.

ISACA. *ISACA Outlines Risks and Benefits of 5G Technology.* https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2021/isaca-outlines-risks-and-benefits-of-5g-technology. February 9, 2021.

U.S. Government Accountability Office. *Science & Tech Spotlight: 5G Wireless.* GAO-20-412SP. https://www.gao.gov/products/gao-20-412sp. March 27, 2020.

U.S. Government Accountability Office. *5G Wireless: Capabilities and Challenges for an Evolving Network.* GAO-21-26SP. https://www.gao.gov/products/gao-21-26sp. November 24, 2020.

IV. Data Mining

Data mining is the process of uncovering patterns and other valuable information from large sets of data. In connection to advancements in related areas, such as data warehousing and big data, data mining techniques have been rapidly improving. Data mining allows organisations to transform raw data into useful knowledge by looking for trends or anomalies. Data mining can improve organisational decision making through insightful data analyses, such as describing the target dataset or predicting outcomes through the use of machine learning algorithms.

Data mining usually consists of four main steps: setting objectives, data gathering and preparation, applying data mining algorithms, and evaluating results.

- **Setting objectives**. Stakeholders need to work together to define the business problem, which helps inform the data questions that need to be answered.
- **Data preparation**. Once the scope is defined, relevant data can be collected and cleaned to maximise performance.
- **Mining algorithms**. Data are analysed to identify relationships, patterns, and correlations. In addition, algorithms may be applied to classify data depending on if the data has been previously labeled.
- **Evaluation**. Once the data have been analysed, results can be evaluated and interpreted. As a result, organisations can use the knowledge gained to achieve intended goals.

Recent developments in machine learning have allowed the field of data mining to expand to textual analysis. This is important because nearly 90 percent of all information is unstructured in formats such as documents, e-mails, social media, and other files. Conducting analyses on these data using data mining techniques is not feasible, as data mining only works for structured data. Text mining involves statistical, linguistic, and machine learning techniques which allow for the analysis of unstructured information. Similar to data mining techniques, new textual mining methods are being developed to help auditors process natural languages. These tools will be critical in assisting auditors in assessing the ever-growing amounts of electronic information.

References and Further Reading

IBM. *Data Mining*, https://www.ibm.com/cloud/learn/data-mining. January 15, 2021.

Scholtes, Jan. *Text Mining and eDiscovery for Big Data Audits*. https://medium.com/ecajournal/text-mining-and-ediscovery-for-big-data-audits-82a1592cac91. March 6, 2020.

V. Big Data

Big data is a term for large complex data sets that are processed in large volumes and are often managed in an unstructured or semi-structured data type. Big data can be used to solve business problems that were previously undiscovered. Some of the main activities big data can help optimise include

- **Product development**. Predictive models can help organisations anticipate customer demand and suggest future products.
- **Predictive maintenance**. Big data can help predict mechanical failures through log entries and sensor data, which can help organisations maximise maintenance.
- **Fraud and compliance**. Big data can help organisations identify patterns in data that would indicate fraud or other malicious activity.

- **Customer experience**. Big data allows organisations to gather data from social media, web visits, call logs, and other sources to personalise the customer experience.
- **Machine learning**. Big data has enabled the ability to train machines and teach machines rather than program them.

The large volume of big data requires a storage solution that can provide accessibility and security. Big data requires the ability to process unstructured data, such as social media data feeds, equipment sensor data, or optimisation data for mechanical equipment. Many organisations will often use outsourced service providers to supply the computing power and storage requirements needed for analyzing big data.

Risks associated with big data include poor data quality, inadequate technology, insufficient security, and immature data governance practices. The auditor should engage the organisation's chief information officer and other leaders to better understand risks of big data in terms of data collection, storage, analysis, security, and privacy.

When assessing big data tools and techniques, the auditor should consider the following:

- **Storage**. How does the organisation store an ever-growing amount of data and how does existing storage integrate with new sources of data?
- **Onsite vs. cloud**. Does the organisation maintain big data environments onsite or outsource to cloud vendors?
- **Data discovery tools**. What level of maturity has the organisation reached in terms of understanding data, acquiring data, and learning from the data?
- **Monitoring tools**. What key performance indicators has the organisation defined for monitoring effectiveness and performance of big data systems?
- **Software acquisition**. Understanding the differences between big data systems and traditional systems will be imperative for selecting the appropriate software.

References and Further Reading

Colombo, Pierro, and Elena Ferrari. "Access Control Technologies for Big Data Management Systems: Literature Review and Future Trends." *Cybersecurity*, Vol. 2, no. 3 https://doi.org/10.1186/s42400-018-0020-9. 2019.

Global Technology Audit Guide. *Understanding and Auditing Big Data.* https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/GTAG-Understanding-and-Auditing-Big-Data.aspx.

Murphy, Maria L. and Journal of Accountancy, "How to Prepare for Auditing in a Digital World of Big Data." *Journal of Accountancy*. https://www.journalofaccountancy.com/news/2014/oct/201411104.html. October. 16, 2014.

Oracle. *What is Big Data?* https://www.oracle.com/big-data/what-is-big-data/.

Salijeni, George, Anna Samsonova-Taddie, and Stuart Turley. "Understanding How Big Data Technologies Reconfigure the Nature and Organization of Financial Statement Audits: A Sociomaterial Analysis." *European Accounting Review, vol. 30, no. 3.* https://www.tandfonline.com/doi/full/10.1080/09638180.2021.1882320. 2021.

VI. Artificial Intelligence

Artificial Intelligence (AI) is a transformative technology with applications in medicine, agriculture, manufacturing, transportation, defense, and other areas. The field of AI was founded on the idea that

machines could be used to simulate human intelligence. AI has been conceptualised as having three distinct waves of development. The first wave of early AI technologies includes expert or rules-based systems, whereby a computer is programmed based on expert knowledge or criteria. The second wave of AI systems includes statistical or machine learning with data and infers rules or decision procedures that accurately predict specified outcomes. The third wave of AI development includes aspects of the first two waves while also being capable of contextual sophistication, abstraction, and explanation.

AI holds substantial promise for improving human life and economic competitiveness in a variety of ways. A few examples of high-consequence areas with potential applications for AI include:

- **Cybersecurity**—Automated systems and advanced algorithms can help reduce the time and effort it takes to identify vulnerabilities, patch vulnerabilities, detect attacks, and defend against active attacks.
- **Automated vehicles**—Automotive and technology firms use AI tools to assess a situation, make a plan, and execute vehicle controls decisions.
- **Criminal justice**—Algorithms are automating portions of analytical work to help provide input to human decision makers.
- **Financial services**—AI tools can help augment customer service operations, client wealth management, consumer risk profiling, and internal controls.

While AI has the ability to deliver numerous benefits across many industries, it also poses new risks and could displace workers and widen socioeconomic inequality. Challenges associated with adopting AI include:

- Collecting and sharing reliable and high-quality data that are needed to train AI;
- Accessing adequate computing resources and having adequate workforce with the knowledge, skills, and training to use them;
- Ensuring laws and regulations governing systems enabled by AI are adequate and that the application of AI does not infringe on civil liberties; and
- Developing an ethical framework to govern the use of AI and ensuring the actions and decisions of AI systems can be adequately explained and accepted by those who interact with such systems.

When assessing the use of AI by government organisations and other entities, auditors should consider evaluating key practices in areas such as governance, data, performance, and monitoring. Examples of auditable procedures of these areas at the organisational level include:

- **Governance**—Organisations should define clear goals, roles, and responsibilities, demonstrate values and principles to foster trust, develop a component workforce, engage stakeholders with diverse perspectives to mitigate risks, and implement an AI-specific risk management plan.
- **Data**—Organisations should document sources and origins of data, to ensure the reliability of data, and assess data attributes, variables, and augmentation/ enhancement for appropriateness.
- **Performance**—Organisations should catalog model and non-model components that make up the AI system, define metrics, and assess performance and outputs of each component.
- **Monitoring**—Organisations should develop plans for continuous routine monitoring of the AI system and document results and corrective actions taken to ensure the system produces desired results.

References and Further Reading

Raji, Inioluwa Deborah, and Andrew Smart, Rebecca N. White, Margaret Mitchell, Timnit Gebru, Ben Hutchinson, Jamila Smith-Loud, Daniel Theron, and Parker Barnes. “Closing the AI Accountability Gap: Defining an End-to-End Framework for Internal Algorithmic Auditing.” Presented at the 2020 *Conference on Fairness, Accountability, and Transparency* in Barcelona, Spain. https://arxiv.org/abs/2001.00973. January 28, 2020.

UK Information Commissioner's Office. *Big data, Artificial Intelligence, Machine Learning and Data Protection*. Version: 2.2. https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf. September 4, 2017.

U.S. Government Accountability Office. *Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities*. GAO-21-519SP. https://www.gao.gov/products/gao-21-519sp. June 2021.

U.S. Government Accountability Office. *Artificial Intelligence: Emerging Opportunities, Challenges, and Implications*. GAO-18-142SP. https://www.gao.gov/products/gao-18-142sp. March 28, 2018.

VII. Machine Learning and Algorithms

Machine learning is a field of computer science dealing with methods to develop models from input data to make predictions about data. Machine learning uses programmed algorithms to predict output values within an acceptable range and as new data is fed to these algorithms they learn and optimise performance. An algorithm is a set of rules and instructions that a computer follows automatically when performing calculations to solve a problem or answer a question. Algorithms can come in many forms such as computational models, decision trees, and other complex data models and self-learning applications.

In general, there is a sense that algorithms are becoming increasingly intelligent. This is due to the fact that, as the volume of data increases and better hardware becomes available, algorithms are able to process more data at greater speed. This leads to algorithms becoming more innovative and wide-ranging. Algorithms can support and improve operational management and service delivery for organisations. In addition, algorithms are intended to boost the efficiency of processes that use complex data. Algorithms make a prediction or perform an analysis, which experts then use to aid in their work.

However, the use of algorithms can pose a number of risks to organisations, including the following:

- The algorithm's impact may not be sufficiently clear to the public.
- The algorithm or data set used by the algorithm may contain certain biases.
- The programmer or data scientist may lack specific knowledge or context to enable the algorithm to reach informed decisions.
- The algorithm may engage in unintended learning.
- The underlying details of the algorithm may only be known by the supplier.

An audit of machine learning can include auditing components of IT infrastructure that use machine learning algorithms. The audit should always include a risk assessment of related IT systems as algorithms are not typically used as stand-alone software. When assessing or analysing algorithms, the auditor should consider the following areas:

- **Governance and accountability.** This includes roles, responsibilities, expertise, management of the algorithm's life cycle, risk factors in using the algorithm, and agreements with external stakeholders. Assessment of governance and accountability can be modeled after IT governance standards as outlined in COBIT.[4]
- **Model and data.** This includes data quality and the development, use, and maintenance of the underlying model for the algorithm. This could also include questions about the data and possible biases within the data, data minimalisation, and how the model is tested.
- **Privacy.** Algorithms may use personal data. In these scenarios, the algorithms must comply with statutory regulation on the processing of personal data.

[4]COBIT is an IT governance control standard designed to meet the need for assessing information-related and IT-related risks.

- **IT general controls.** These include conventional IT controls, such as access rights, continuity management, and change management.

References and Further Reading

ISACA. *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*. 2012.

Netherlands Court of Audit. *Understanding Algorithms*. https://english.rekenkamer.nl/publications/reports/2021/01/26/understanding-algorithms. 2021.

Supreme Audit Institutions of Finland, Germany, the Netherlands, Norway, and the United Kingdom. *Auditing Machine Learning Algorithms*. https://www.auditingalgorithms.net/. November 24, 2020.

VIII. Robotic Process Automation

Robotics process automation (RPA) is an automation of routine business tasks governed by business logic and structured inputs. The tasks for RPA include processing transactions, triggering responses, and communicating with other digital systems. This often includes functions such as copy-pasting, scraping web data, making calculations, opening and moving files, parsing emails, and extracting data.

If implemented effectively, RPA can provide organisations with the ability to reduce staffing costs and human error. Further, RPA can improve business outcomes, such as customer satisfaction, and free up staff to solve problems, conduct analysis, and other value-added work. RPA is typically low cost to implement and does not often require custom software to integrate. At times, organisations may utilise machine learning or other artificial intelligence technologies to enhance their RPA.

RPA, as with any automation technology, has the potential to eliminate jobs, which can present challenges with managing the organisation's talent. In addition, RPA can increase risk exposure compared to typical IT applications. For example, changes to job roles, access security, application change management, and governance of the RPA environment are aspects that need to be considered when implementing RPA. Automation of a business process can result in changes to process control requirements. This makes auditing the automated environments critical for auditors to have assurance the desired output is being produced.

When auditing a RPA environment, several different stages of the environment need to be assessed and specific steps need to be considered in these stages:

- **Planning**—In the planning phase, to have a clear understanding of the areas where RPA is implemented, the auditor needs to define the level of automation, analyse workflows, and determine what other integrated systems should be included.
- **Walkthrough**—Once the auditor identifies automations are in an environment, it is important to test the risks associated with each automation in the process. A code walkthrough is critical to understanding risks, controls, and systems involved in automation.
- **Design**—Automations need to be considered elements of IT, and the auditor should include the most relevant automations in the scope of the design. This should include any automations that generate reports or other outputs used by management. In addition, the auditor should assess the adequacy of applied controls for mitigating and eliminating risks associated with each automation in the process.
- **Reporting**—If automation is used for creating reports, the auditor needs to assess the completeness and accuracy of the reports by evaluating the code, logic, and parameters used in creating the reports.

References and Further Readings

Automation Anywhere. *What is Robotic Process Automation (RPA)?* https://www.automationanywhere.com/rpa/robotic-process-automation.

Boulton, Clint. *What is RPA? A Revolution in Business Process Automation.* https://www.cio.com/article/3236451/what-is-rpa-robotic-process-automation-explained.html.

Deloitte. *Auditing the RPA environment, https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-auditing-the-rpa-environment-noexp.pdf*. March 2018.

IX. Blockchain

A blockchain is a distributed ledger that allows for real-time transactions of digital assets. Specifically, blockchain is a ledger of digital events organised in chronological blocks that are encrypted and distributed among many different entities. Blocks can only be updated when a majority of the entities agree on the transaction. Blockchain uses a peer-to-peer framework where every node on the blockchain has an identical copy of the data and a consensus protocol synchronises the data across nodes. This results in a real-time update of data without the need of a central authority or third party to validate transactions. Transactions can only be written to the blockchain once, and there is no reversing of transactions. Foundational attributes of blockchain technologies include being

- **Decentralised**—Blockchain can operate independently of any intermediary or authority allowing it to operate on a peer-to-peer basis.
- **Distributed**—The blockchain ledger is distributed and replicated across all nodes on the network.
- **Traceable—** Every entry on the blockchain is linked to the previous transaction so that there is a complete and traceable audit trail of the underlying transactions.
- **Validated**—Transactions are validated by participating nodes against the consensus mechanism before being appended to the blockchain.
- **Immutable**—Transactions on the blockchain are immutable, meaning they cannot be replaced, reversed, or altered, once they have been validated.
- **Verifiable**—Transactions on the blockchain are transmitted to all nodes on the network where each node can verify the history of transactions.

While blockchain provides capabilities such as the ones mentioned above, several issues could result as part of implementing blockchain technologies, including:

- **Blockchain hard forks**—These are events where two divergent copies of the blockchain have been created. This typically occurs when there is a disagreement among nodes on the rules governing the blockchain.
- **Double spending**—This issue is associated primarily with cryptocurrencies where an asset can be transferred to multiple entities.
- **51 percent dominance**—This is an issue that could arise when one entity controls the majority of the network which gives that entity the ability to act maliciously.
- **Poor performance**—Consensus mechanisms often create a tradeoff between performance speed and trust of transaction reliability.

One important consideration when auditing blockchain technologies is the reliability of data. Specifically, auditors need to be aware of the ability of the blockchain to be manipulated or altered. The consensus algorithm used by specific blockchains might be manipulated so that transactions are appended to the blockchain without proper authorisation. Other considerations when auditing blockchain include privacy

concerns, such as digital ID data storage on a blockchain, which could disclose personal information if the encryption is broke at a future time.

References and Further Readings

Deloitte. *An Internal Auditor's Guide to Blockchain: Blurring the Line between Physical and Digital*. https://www2.deloitte.com/us/en/pages/risk/articles/internal-auditing-guide-to-blockchain.html. 2019.

KPMG. *Auditing Blockchain Solutions.* https://assets.kpmg/content/dam/kpmg/in/pdf/2018/10/Auditing_Blockchain_Solutions.pdf. October 2018.

RSM US. *How Blockchain Technology Will Affect the Audit.* https://rsmus.com/what-we-do/services/assurance/how-blockchain-technology-will-affect-the-audit.html. November 13, 2019.

U.S. Government Accountability Office. *Blockchain: Emerging Technology Offers Benefits for Some Applications but Faces Challenges.* GAO-22-104625. *https://www.gao.gov/products/gao-22-104625.* March 23, 2022.