AICPA

Use of Technology in an Audit of Financial Statements

Practice Aid

Part
01

The use of automated tools and techniques in the auditor's risk assessment

Contents

Notice to readers

Overview

The AICPA® has developed the *Use of Technology in an Audit of Financial Statements* practice aid (the technology practice aid) to help auditors focus on the use of technology in the audit of financial statements.

About the technology practice aid

Part 1 of the technology practice aid, "The use of automated tools and techniques in the auditor's risk assessment," has been developed to assist practitioners in considering the use of technology when applying Statement on Auditing Standards (SAS) No. 145, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement*. SAS No. 145 addresses the auditor's responsibility to identify and assess the risks of material misstatement in the financial statements. It is effective for audits of financial statements for periods ending on or after December 15, 2023, and is codified in AU-C section 315, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement*.[1]

SAS No. 145 was designed to clarify certain aspects of the identification and assessment of the risks of material misstatement to drive better risk assessments and, therefore, enhance audit quality. It includes additional guidance that addresses significant changes in, and the evolution and increasingly complex nature of, the economic, technological, and regulatory aspects of the markets and environment in which entities and audit firms operate. Accordingly, SAS No. 145 resulted in modernizing AU-C section 315 in relation to IT considerations, including how the auditor addresses risks arising from an entity's use of IT.

Part 1 of this practice aid contains three modules. Additional parts may be added to this document in the future.

Part 1 — The use of automated tools and techniques in the auditor's risk assessment

- Module 1-A, "The benefits of leveraging technology in the auditor's risk assessment and of obtaining an understanding of the entity's use of technology," is designed to help the auditor understand the benefits of using technology when performing risk assessment procedures in an audit of financial statements. It explains why the auditor's risk assessment is important, highlights the importance of obtaining an understanding of the entity's technology maturity, and provides insights into ways the auditor may want to use automated tools and techniques when performing risk assessment procedures in an audit of financial statements.
- Module 1-A does not include all aspects of AU-C section 315. It is therefore recommended that an auditor have sufficient knowledge of AU-C section 315 when applying the technology concepts contained herein as the auditor performs risk assessment procedures.
- Module 1-B, "Commonly used automated tools and techniques in the auditor's risk assessment," helps the auditor understand commonly used forms of automated tools and techniques and how they may be used when performing risk assessment procedures in an audit of financial statements.
- Module 1-C, "Example of the auditor's use of technology when performing risk assessment procedures," is designed to illustrate a traditional risk assessment approach and how that may differ from a technology-enabled risk assessment approach.

[1] All AU-C sections can be found in AICPA *Professional Standards*.

Other related resources

The "Additional resources" appendix provides a list of resources that may provide valuable information relating to the use of technology in the audit. In addition, the following publications may be helpful:

- AICPA Audit Guide *Risk Assessment in a Financial Statement Audit* provides additional information and practical guidance relating to the auditor's risk assessment in accordance with SAS No. 145.
- AICPA *Guide to Audit Data Analytics* was developed to provide an introduction to and overview of data analytics techniques to assist auditors in applying such techniques in performing their audit engagements. In particular, it discusses the use of audit data analytics in performing risk assessment procedures.

Acknowledgments

The AICPA gratefully acknowledges those members of the Auditing Standards Board Technology Task Force who contributed to the development of part 1 of this practice aid: Samantha Bowling (chair), Brad Ames, Daniel Balla, Danielle Supkis Cheek, Margaret Christ, Jeff Cook, Kathleen K. Healy, Chris Rogers and Sara Watson.

AICPA staff

Jennifer Burns
Chief Auditor

Linda Delahanty
Senior Manager — Audit & Attest Standards

Brian Wilson
Director — Audit & Attest Standards

Erin Mackler
Senior Manager — Assurance, Advisory & Innovation

Other auditing publications

This publication is an other auditing publication as defined in AU-C section 200, *Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance With Generally Accepted Auditing Standards.* Other auditing publications have no authoritative status; however, they may help the auditor understand and apply generally accepted auditing standards (GAAS).

In applying the auditing guidance included in an other auditing publication, the auditor should, exercising professional judgment, assess the relevance and appropriateness of such guidance to the circumstances of the audit.[2]

The auditing guidance in this document has been reviewed by the AICPA Audit and Attest Standards staff and published by the AICPA and is presumed to be appropriate. This document has not been approved, disapproved, or otherwise acted on by a senior technical committee of the AICPA.

This technology practice aid does not discuss the application of all AU-C sections that are relevant to the audit of financial statements, nor does it contain all the requirements necessary for risk assessment. This technology practice aid is provided with the understanding that the staff and publisher are not engaged in rendering legal, accounting, or other professional service. All such information is provided without warranty of any kind.

[2] Paragraph .28 of AU-C section 200, *Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance With Generally Accepted Auditing Standards.*

Module 1-A: The benefits of leveraging technology in the auditor's risk assessment and of obtaining an understanding of the entity's use of technology

Introduction

Note: SAS No. 145

This module reflects the issuance of Statement on Auditing Standards (SAS) No. 145, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement*.

1A.01 — Audits of the financial statements of entities of all types and sizes may be performed in an environment in which there is pervasive use of information technology (IT). Continuous and rapid developments in technology and data analytics create opportunities for auditors to evolve their risk assessment procedures by leveraging technology. In this context, increased use of automated tools and techniques, such as audit data analytics (ADAs), is likely to be important in maintaining and enhancing the relevance and value of the financial statement audit.

1A.02 — The purpose of Module 1-A, "The benefits of leveraging technology in the auditor's risk assessment and of obtaining an understanding of the entity's use of technology," is to help you, the auditor, understand the benefits of using technology when performing your risk assessment procedures in an audit of financial statements in accordance with SAS No. 145, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement* (AU-C section 315).[1] (Note: Throughout this module, the auditor is referred to as "you.") It explains why the auditor's risk assessment is important, highlights the importance of obtaining an understanding of the entity's technology maturity, and provides insights into ways you may want to use automated tools and techniques when performing risk assessment procedures in an audit of financial statements.

1A.03 — Often there is a correlation between your use of technology in the audit and the entity's use of technology, including the availability of data. In other words, the effectiveness of your use of technology, such as ADAs, may depend on the level of data available from the entity. Therefore, it is important for you to obtain an understanding of the entity's use of technology and consider how that may affect your risk assessment.[2]

[1] SAS No. 145, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement*, issued in October 2021, is effective for audits of financial statements for periods ending on or after December 15, 2023, and is codified in AU-C section 315, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement*, in AICPA *Professional Standards*.

[2] Paragraphs .27–.29 of AU-C section 315 set out specific requirements for the auditor to identify controls that address risks of material misstatement at the assertion level. Based on these controls, the auditor is required to identify the IT applications and other aspects of the IT environment that are subject to risks arising from the use of IT and identify both the risks arising from the use of IT and the entity's general IT controls that address those risks.

Appendix E of AU-C section 315 provides further considerations for the auditor in understanding the entity's use of IT in its system of internal control. Appendix F of AU-C section 315 provides further explanation of the nature of general IT controls that may be implemented for different aspects of the IT environment.

1A.04 — Auditors can leverage ADAs regardless of the extent of the entity's use of IT. Greater use of IT by the entity generally allows you to perform more sophisticated ADAs because there may be more organized data available to you electronically. However, there are opportunities for you to leverage technology in any environment. Your use of technology is not limited to complex entities, and therefore, it can be useful in audits of less complex entities as well.

Note: Audit data analytics

Paragraph .A4 of AU-C section 500, *Audit Evidence*, describes audit data analytics (ADAs) as "the analysis of patterns, identification of anomalies, or extraction of other useful information in data underlying or related to the subject matter of an audit through analysis, modeling, or visualization." ADAs are techniques that can be used to perform various audit procedures, including elements of risk assessment, tests of controls, substantive procedures (that is, tests of details or substantive analytical procedures), or concluding procedures. See module 1-B for further discussion about ADAs.

Why performing risk assessment procedures is important

1A.05 — Risk assessment requirements are not designed to make the audit more onerous; in fact, if followed and scaled appropriately, the risk assessment requirements allow you to be more effective and efficient in your audit. A thorough risk assessment allows you to appropriately design and perform audit procedures in response to identified and assessed risks. Similarly, using automated tools and techniques when performing your risk assessment is another way to be more effective and efficient in your audit. Using automated tools and techniques may help you with the following:

- Corroborating the work you have done through inquiry and observation
- Identifying areas in which you may gain efficiencies in the audit
- Revealing new insights into the entity and thereby providing a more precise risk assessment

1A.06 — Risk assessment procedures assist in identifying and assessing risks based on a spectrum of inherent risk.[3] Careful attention to both the uniqueness of the entity under audit and changes that may have occurred since the prior year is important in conducting a risk assessment in the current year. Such careful attention helps you tailor standardized audit programs and design and perform further audit procedures that are responsive to the assessed risks.

Note: AICPA risk assessment guide

AICPA Audit Guide *Risk Assessment in a Financial Statement Audit* provides you with guidance on how to perform your risk assessment in accordance with SAS No. 145 (AU-C section 315).

[3] Paragraph .12 of AU-C section 315 defines *inherent risk factors* and explains that depending on the degree to which the inherent risk factors affect the susceptibility of an assertion to misstatement, the level of inherent risk varies on a scale that is referred to as the *spectrum of inherent risk*.

Obtaining an understanding of the entity's use of technology to help you determine your use of technology in the audit

1A.07 — AU-C section 315, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement*, addresses your responsibility to identify and assess the risks of material misstatement in the financial statements. AU-C section 315 requires you to understand and evaluate the entity's control environment, including the IT environment. Paragraph .19 of AU-C section 315 requires you to understand the entity's organizational structure, ownership and governance, and its business model, including the extent to which the business model integrates the use of IT.

1A.08 — Inquiries directed toward IT personnel may provide information about IT processes and system changes, related control failures, or other IT-related risks. Understanding what new technologies, or changes in technologies, management has put in place — and the rationale for doing so — can help you better understand the risks and opportunities that management is trying to address. This can help you tailor your approach to the current audit engagement.

Note: Understanding the entity's information system and communication and control activities

Paragraph .25 of AU-C section 315 specifies that you should, through performing risk assessment procedures, obtain an understanding of the entity's information system and communication relevant to the preparation of the financial statements by, among other things,

- understanding the entity's information-processing activities, including its data and information, the resources to be used in such activities, and the policies that define, for significant classes of transactions, account balances, and disclosures,[4] the following:
  - How the information flows through the entity's information system
  - The accounting records, specific accounts in the financial statements, and other supporting records relating to the flows of information in the information system
  - The financial reporting process used to prepare the entity's financial statements, including disclosures, and
  - The entity's resources, including IT environment, relevant to the preceding items
- evaluating, based on the understanding you obtained in paragraphs .25*(a)–(b)* of AU-C section 315, whether the entity's information system and communication appropriately support the preparation of the entity's financial statements in accordance with the applicable financial reporting framework considering the nature and complexity of the entity.

In addition, paragraphs .27–.29 of AU-C section 315 set out specific requirements for you to identify controls that address risks of material misstatement at the assertion level. Based on these controls, you are required to identify the IT applications and other aspects of the IT environment that are subject to risks arising from the use of IT and identify both the risks arising from the use of IT and the entity's general IT controls that address those risks.

Appendix E of AU-C section 315 provides further considerations for you in understanding the entity's use of IT in its system of internal control.

Appendix F of AU-C section 315 provides further explanation of the nature of general IT controls that may be implemented for different aspects of the IT environment.

[4] Paragraph .12 of AU-C section 315, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement*, defines *significant class of transactions, account balance, or disclosure* as a class of transactions, account balance, or disclosure for which there is one or more relevant assertions.

1A.09 — *Use of the internal audit function (if the function exits)*. Paragraph .14 of AU-C section 315 specifies that risk assessment procedures should include inquiries of management and of other appropriate individuals within the entity, including individuals within the internal audit function (if the function exists). Similarly, paragraph .24 of AU-C section 315 requires you to obtain an understanding of the entity's process for monitoring the system of internal control relevant to the preparation of the financial statements by understanding those aspects of the entity's process that address the entity's internal audit function, if any, including its nature, responsibilities, and activities. Internal audit's use of IT may indicate the entity's level of technological sophistication with respect to identifying and managing risks. Based on what you learn through performing risk assessment procedures, you may identify areas in which internal audit uses IT that provide opportunities for you to use the work of internal audit and related uses of IT in your audit. See AU-C section 610, *Using the Work of Internal Auditors*, when you plan to use the work of the internal audit function in obtaining audit evidence or plan to use internal auditors to provide direct assistance under your direction, supervision, and review.

1A.10 — Your understanding of the IT environment and risks arising from the use of IT is important because it may affect your

- assessment of inherent risk,[5]
- approach to testing the operating effectiveness of controls to address risks of material misstatement,
- approach to testing information produced by the entity's IT applications, or
- the design of further audit procedures.

Note: IT-related matters identified in the risk assessment process

When obtaining an understanding and evaluating an entity's IT environment (as part of your risk assessment procedures), you may identify IT-related matters that inform your risk assessment, such as the following:

- Whether management has a good understanding of the IT environment, flows of transactions, and data flows into the financial statements
- Whether management has a good understanding of the flow of transactions between systems and interfaces, and the related relevant controls
- Whether change management controls exist (when, for example, upgrading or replacing systems)

1A.11 — AU-C section 315 requires an understanding of how inherent risk factors affect the susceptibility of assertions to misstatement and the degree to which they do so. Depending on the degree to which the inherent risk factors affect the susceptibility of an assertion to misstatement, the level of inherent risk varies on a scale that is referred to as the *spectrum of inherent risk*. Inherent risk is assessed before the consideration of any related controls. In addition to assessing inherent risk, a key decision that is often made in an audit is the assessment of control risk and determining whether to test the operating effectiveness of controls. If the entity is less mature in its use of IT (that is, if controls are more manual because of a lesser investment in technology, a less effective implementation of technology, or both — see exhibit 1A-1), you might decide, for example, to do the following:

[5] *Inherent risk* is described as the susceptibility of an assertion about a class of transactions, account balance, or disclosure to a misstatement that could be material, either individually or when aggregated with other misstatements, before consideration of any related controls (paragraph .04 of AU-C section 315).

- Assess control risk at less than maximum, because, based on your understanding, you believe certain controls may be operating effectively. That is, you plan to test the operating effectiveness of certain controls in determining the nature, timing, and extent of substantive procedures for a particular area or assertion.
- Assess control risk at the maximum level and take a more substantive approach such that the assessment of the risk of material misstatement is the same as the assessment of inherent risk. However, there can be risks of material misstatement for which substantive procedures alone do not provide sufficient appropriate audit evidence.

1A.12 — When routine business transactions are subject to highly automated processing with little or no manual intervention, it may not be possible to perform only substantive procedures in relation to the risk. This may be the case in circumstances in which a significant amount of an entity's information is initiated, recorded, processed, or reported in the financial statements only in electronic form. For example, it is typically not possible to obtain sufficient appropriate audit evidence relating to revenue for a telecommunications entity based on substantive procedures alone. This is because the evidence of call or data activity does not exist in a form that is observable. Instead, controls testing is typically performed to determine that the origination and completion of calls and data activity is correctly captured (for example, minutes of a call or volume of a download) and recorded correctly in the entity's billing system. In such cases, audit evidence may be available only in electronic form, and its sufficiency and appropriateness usually depend on the effectiveness of controls over its accuracy and completeness. The potential for improper initiation or alteration of information to occur and not be detected may be greater if appropriate controls are not operating effectively.[6]

Note: Substantive procedures alone cannot provide sufficient appropriate audit evidence

Paragraph .A88 of AU-C section 540, *Auditing Accounting Estimates and Related Disclosures*, also discusses circumstances about risks for which substantive procedures alone cannot provide sufficient appropriate audit evidence at the relevant assertion level, such as

- when controls are necessary to mitigate risks relating to the initiation, recording, processing, or reporting of information obtained from outside of the general and subsidiary ledgers
- when information supporting one or more assertions is electronically initiated, recorded, processed, or reported. This is likely to be the case when there is a high volume of transactions or data, or a complex model is used, requiring the extensive use of IT to ensure the accuracy and completeness of the information. A complex expected credit loss provision may be required for a financial institution or utility entity. For example, in the case of a utility entity, the data used in developing the expected credit loss provision may comprise many small balances resulting from a high volume of transactions. In these circumstances, you may conclude that sufficient appropriate audit evidence cannot be obtained without testing controls around the model used to develop the expected credit loss provision.

[6] Paragraphs .37 and .A254 of AU-C section 315.

1A.13 — Understanding the entity's level of IT maturity can help you design and perform risk assessment procedures, including considerations about whether and how to use technology (or automated tools and techniques, such as ADAs) in the audit.

Note: AICPA *Guide to Audit Data Analytics*

AICPA *Guide to Audit Data Analytics* complements the discussion in the technology practice aid. Part 1 of the technology practice aid includes making auditors aware of how various ADAs may be efficiently and effectively used when performing risk assessment procedures in a financial statement audit performed in accordance with generally accepted auditing standards and helping auditors identify and address matters they may encounter in deciding whether to use ADAs when performing risk assessment procedures. Part 1 of the technology practice aid does not cover the types of ADAs that may be used in all aspects of the audit, but rather those specific to the auditor's risk assessment.

1A.14 — As the entity progresses in its IT maturity, it may become a strategic necessity for you to also mature in your use of data and technology in the audit. Management and those charged with governance also may expect you to leverage data and technology to increase the effectiveness and efficiency of the audit. Your use of technology may allow you to engage with management and those charged with governance in focused and productive discussions about audit findings and monitoring of audit progress using data that was obtained for the purposes of the audit. For example, if an entity implemented a new system in its accounts payable process, your work to evaluate the design and implementation of the identified controls[7] and test the operating effectiveness of those controls may identify findings that would be relevant to share with management and those charged with governance, including views about whether the data from the system was reliable. You could facilitate a conversation with those charged with governance regarding why you may not be able to rely on the data produced from the new system and raise awareness about effective implementation of technology.

[7] The controls for which the auditor is required to evaluate design and determine implementation are referred to as *identified controls* in AU-C section 315.

Note: The entity's IT maturity

An entity's use of IT affects the manner in which the information relevant to the preparation of the financial statements in accordance with the applicable financial reporting framework is processed, stored, and communicated and, therefore, affects the manner in which the entity's system of internal control is designed and implemented.[8] Each component of the entity's system of internal control may use some extent of IT.[9] Entities may use various forms of technology, such as software-as-a-service (SaaS),[10] blockchain, robotic process automation, or artificial intelligence, to operate more efficiently and improve business.

An entity's system of internal control typically contains manual elements and automated elements (that is, manual and automated controls and other resources used in the entity's system of internal control). An entity's mix of manual and automated elements varies with the nature and complexity of the entity's use of IT. The characteristics of manual or automated elements are relevant to your identification and assessment of the risks of material misstatement and further audit procedures based thereon. Automated controls may be more reliable than manual controls because they cannot be as easily bypassed, ignored, or overridden, and they are also less prone to simple errors and mistakes.

Automated controls may be more effective than manual controls in the following circumstances:

- High volume of recurring transactions, or in situations in which errors that can be anticipated or predicted can be prevented, or detected and corrected, through automation
- Controls in which the specific ways to perform the control can be adequately designed and automated[11]

See paragraph 18 of appendix E of AU-C section 315 for examples of risks arising from the use of IT, which may include automated controls.

See paragraph 1A.11 of this module for a discussion about the possible effects of the entity's use of technology and the auditor's decision to test the operating effectiveness of controls. The auditor may decide to place less reliance on application controls and general IT controls when the entity has a lower IT maturity. As the entity's IT maturity grows, the auditor may decide to place more reliance on application controls and general IT controls, and to test controls for operating effectiveness.

Entities with a higher IT maturity typically have a greater investment in and more effective implementation of technology, which results in greater volume and reliability of data. Entities with a greater IT maturity will often have a highly automated control infrastructure, process/control validation, continuous, real-time monitoring, and ongoing innovation and investment. For those entities at the lower level of technology maturity, the auditor will often see more manual processes, less technology-driven applications, and less investment in technology with less effective implementation of such technology.

The following exhibit 1A-1, "The entity's technology maturity," illustrates the interplay between an entity's investment in technology and the effectiveness of implementing such technology (see page 11).

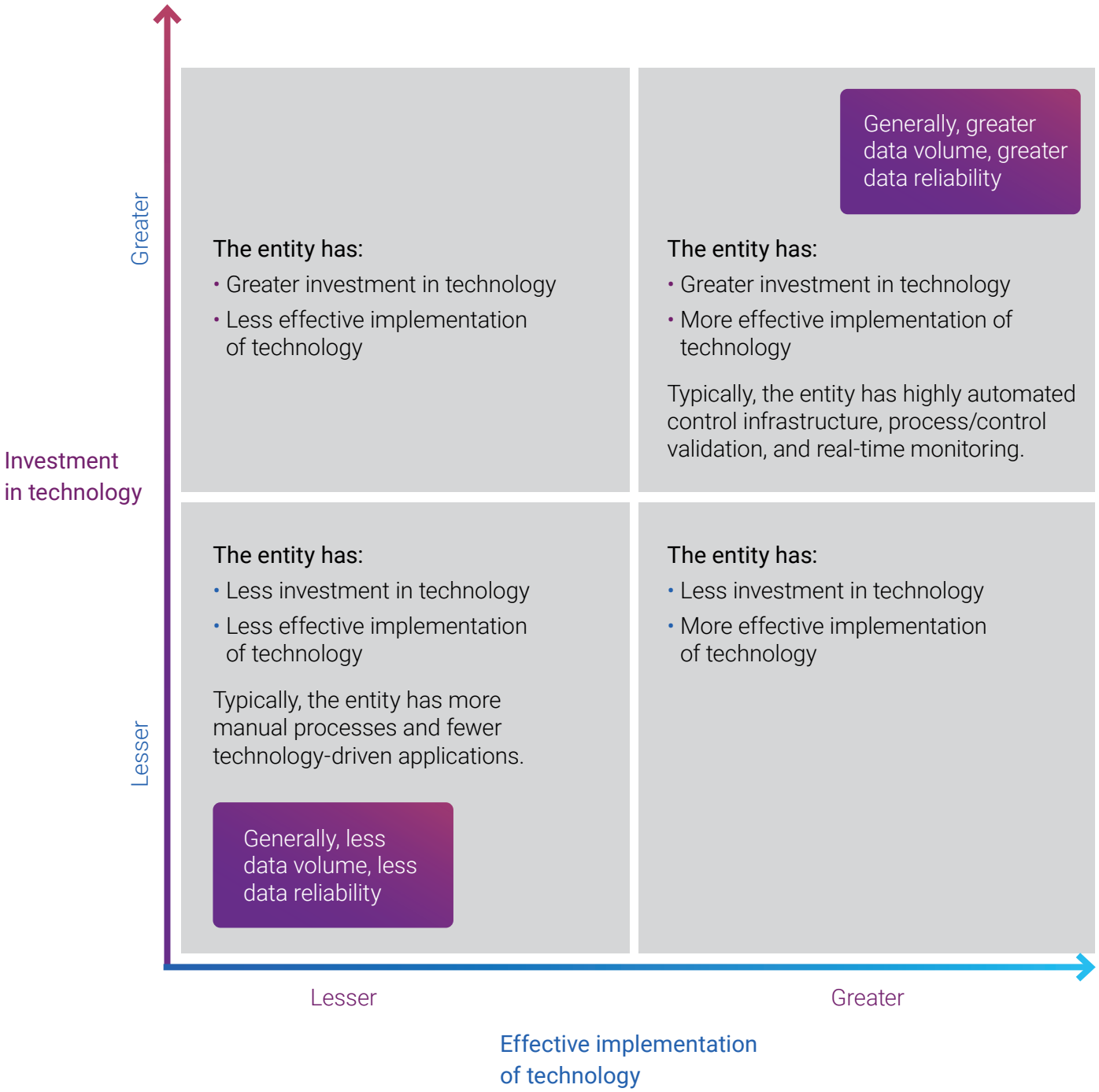
[8] AU-C section 315 defines the terms *risks arising from the use of IT* and *general IT controls* and requires the auditor to identify general IT controls that address the risks arising from the use of IT and to evaluate their design and determine their implementation. General IT controls need not be identified for every IT process. General IT controls are identified based on the risks arising from the use of IT. To identify the risks arising from the use of IT, the auditor identifies the IT applications and other aspects of the entity's IT environment that are subject to such risks. See paragraphs .25 and .29 of AU-C section 315.

[9] Paragraph 1 of appendix E, "Considerations for Understanding IT," of AU-C section 315.

[10] Software-as-a-service (SaaS) refers to an internet protocol (IP) that is run on the entity's systems (commonly referred to as the "cloud") and accessed remotely by the customer's users.

[11] Paragraph 2 of appendix E of AU-C section 315.

Exhibit 1A-1: The entity's technology maturity



Using automated tools and techniques for your risk assessment

1A.15 — As more entities are investing in and effectively implementing technology, you also can consider how using technology in the audit may allow for a more efficient and effective risk assessment and audit approach. Your understanding of the entity and its environment, the applicable financial reporting framework, and the entity's system of internal control provides the foundation for your judgments in the identification and assessment of risks of material misstatement.

1A.16 — Consider the following statements and whether they are true or false.

Statement 1: The use of technology by auditors requires a significant investment of money and resources.

True | False

False

Some might think that the use of technology by auditors will require a significant investment, but this is not always true.

There are ways to leverage existing technologies such as Microsoft Excel or to use open-source resources already available for auditors. For example, the AICPA Assurance Services Executive Committee (ASEC) provided an example about how Python can be leveraged to apply the AICPA's audit data standard guidelines on formatting to a data set and to develop and run routines to further analyze the standardized data set. Additionally, there are ADAs available for purchase that can benefit firms that may not have the resources to make a significant investment in building proprietary technology.

Although these resources are available to leverage and may decrease the overall investment needed to use technology, you still need to have the proper expertise to appropriately supervise and review work when technology is used and to determine the ADA is functioning appropriately, in line with your system of quality management.

Statement 2: If the entity does not use technology in its processes, then the auditor cannot use technology to perform the audit.

True | False

False

Some might think that, if the entity does not use technology in its processes, then an auditor cannot use technology to perform the audit, but this is also not always true. There are opportunities to use ADAs even when a limited amount of data, such as general ledger data, is available. For example, you can use ADAs to calculate and visualize financial ratios and some high-level quantitative measures using only general ledger data.

1A.17 — SAS No. 145 includes additional guidance that addresses significant changes in, and the evolution and increasingly complex nature of, the economic, technological, and regulatory aspects of the markets and environment in which entities and audit firms operate. It also recognizes the ability to use automated tools and techniques (including ADAs) when performing risk assessment procedures.

1A.18 — Exhibit 1A-2 provides examples of ways you may want to consider using automated tools and techniques, such as ADAs, as you perform your risk assessment.

Exhibit 1A-2: The use of automated tools and techniques in your risk assessment

Risk assessment topic	Examples of automated tools and techniques
Risk assessment procedures and related activities Par. .A27 of AU-C section 315	Using automated tools and techniques, you may perform risk assessment procedures on large volumes of data (from the general ledger, subledgers, or other operational data), including for analysis, recalculations, reperformance, or reconciliations.
Understanding the entity and its environment Par. .A65 of AU-C section 315	You may use automated tools and techniques to understand flows of transactions and processing as part of the auditor's procedures to understand the information system. An outcome of these procedures may be that the auditor obtains information about the entity's organizational structure or those with whom the entity conducts business (for example, vendors, customers, or related parties).
The information system and communication component Par. .A156 of AU-C section 315	You may use automated tools and techniques to obtain direct access to, or a digital download from, the databases in the entity's information system that store accounting records of transactions. By applying automated tools and techniques to this information, you may confirm the understanding obtained about how transactions flow through the information system by tracing journal entries, or other digital records related to a particular transaction, or an entire population of transactions from initiation in the accounting records through to recording in the general ledger. Analysis of complete or large sets of transactions may also result in the identification of variations from the normal, or expected, processing procedures for these transactions, which may result in the identification of risks of material misstatement.
Identifying risks of material misstatement Par. .A233 of AU-C section 315	You may use automated tools and techniques to assist in the identification of significant classes of transactions, account balances, and disclosures. For example, an entire population of transactions may be analyzed using automated tools and techniques to understand their nature, source, size, and volume. By applying automated tools and techniques, the auditor may, for example, identify that an account with a zero balance at period end comprised numerous offsetting transactions and journal entries occurring during the period, indicating that the account balance or class of transactions may be significant (for example, a payroll clearing account). This same payroll clearing account may also identify expense reimbursements to management (and other employees), which could be a significant disclosure due to these payments being made to related parties. As another example, by analyzing the flows of an entire population of revenue transactions, the auditor may more easily identify a significant class of transactions that had not previously been identified.

1A.19 — You can help prepare yourself to use ADAs and obtain data from the entity by considering the following (see also the "Data reliability" section of this module):

Note: Planning your ADAs

As discussed in AICPA *Guide to Audit Data Analytics*, when planning your ADA[12]

- determine the financial statement items or accounts, or disclosures, and related assertions and the nature, timing, and extent of the population to which the ADA will be applied.
- determine the overall purpose of the ADA (for example, whether it is used in performing a risk assessment procedure, a test of controls, a substantive analytical procedure, a test of details, or in procedures to help form an overall conclusion from the audit).
- determine the specific objectives of the ADA (within the context of its overall purpose, which for purposes of this module would be to be used in performing a risk assessment procedure).
- determine the data population to be analyzed or tested using the ADA, including, for planning purposes, preliminary consideration of matters likely to affect the relevance, availability, and reliability of that data.
- select the ADA that is likely best suited for the intended purpose and objectives.
- select the techniques, tools, graphics, and tables to be used.

a. As you obtain your understanding of the entity, consider what requests to make to obtain the data needed to perform procedures (including the correct report parameters, if applicable), and understand what data is necessary based on what ADAs and tools are available to you.

b. Communicate and manage expectations with the entity's management for data requests (including the minimum required data elements), and review and update requests as necessary.

c. Plan for data ingestion by working with the entity's IT department to understand capabilities and communicate your needs.

d. Understand and establish policies for data retention, including considerations for archiving; risk management; confidential or sensitive information; and litigation requirements.

Data reliability

1A.20 — AICPA *Guide to Audit Data Analytics* sets out five basic steps and related procedures that may be used in planning, performing, and evaluating the results of an ADA used in identifying and assessing risks of material misstatement and to assist when forming an overall conclusion.[13] The second step is for you to "access and prepare the data for purposes of the ADA."

1A.21 — It is important to remember that, even if you are able to access more data from the entity,

- the data may require preparation (or cleansing and scrubbing)[14] before you can undertake a meaningful analysis of the data.

[12] See chapter 2, "Using ADAs in Performing Risk Assessment Procedures and in Procedures to Assist When Forming an Overall Conclusion," in AICPA *Guide to Audit Data Analytics*.

[13] See chapter 2 in AICPA *Guide to Audit Data Analytics*.

[14] Data preparation is a process of identifying data errors, of which there are many types. For example, some fields that should always contain data may have none; fields that should contain dates may have letters or other types of numbers; or there may be fields that contain data outside preset acceptable minimum or maximum values. See paragraphs 1.36–1.37 of AICPA *Guide to Audit Data Analytics* for further guidance on prepraring data for use.

- AU-C section 500[15] requires you to evaluate the information to be used as audit evidence, including its relevance and reliability and whether it is sufficiently precise and detailed for the auditor's purposes (that is, the underlying data used in an ADA).
  - Paragraphs 1.38–1.45 of AICPA *Guide to Audit Data Analytics* include additional discussion about the relevance and reliability of data when using ADAs, including data characteristics that may affect the relevance and reliability of data such as nature, source, format, timing, extent, and level of aggregation.
  - Appendix D, "Matters to Consider Regarding the Reliability of Data," of AICPA *Guide to Audit Data Analytics* also provides examples of approaches an auditor might use in determining whether data is sufficiently reliable.

Module 1-A key takeaways

1A.22 — You have seen through module 1-A some of the benefits of leveraging technology when performing risk assessment procedures. We have also seen the benefits of obtaining an understanding of the entity's technology maturity as you determine your audit strategy. Here are a few key takeaways to remember:

a. It is important to obtain an understanding of the entity's IT maturity to not only perform a robust risk assessment but also to optimize your use of technology in the audit.

b. The entity does not need advanced technology for you to use technology in the audit.

c. Even the simplest technology can add value to the audit.

d. Data reliability, along with the appropriateness and reliability of the technology itself, is important when using technology in the audit.

e. Many off-the-shelf tools that are already being used by you and the entity may contain ADA capabilities and include artificial intelligence. As these tools continue to evolve, it will become easier for you to incorporate use of technology in the audit.

f. Don't forget the documentation requirements relating to performing your risk assessment. See paragraph .42 of AU-C section 315 for documentation requirements. Also, paragraphs 1.48–1.56 of AICPA *Guide to Audit Data Analytics* discuss matters related to documenting ADAs.

1A.23 — Module 1-B, "Commonly used automated tools and techniques of the auditor's risk assessment," will assist you in identifying the types of automated tools and techniques that are commonly used when applying SAS No. 145.

1A.24 — The example in Module 1-C, "Example of the auditor's use of technology when performing risk assessment procedures," is designed to illustrate a traditional risk assessment approach and how that may differ from a technology-enabled risk assessment approach.

[15] See paragraphs .7–.8 of AU-C section 500, *Audit Evidence*. The auditor's evaluation of information to be used as audit evidence should include obtaining audit evidence about the accuracy and completeness of information, as necessary. In some cases, the auditor may consider it necessary to obtain audit evidence about the accuracy and completeness of the data by testing controls over its preparation and maintenance (for example, in light of the nature, frequency, and volume of transactions).

Module 1-B: Commonly used automated tools and techniques in the auditor's risk assessment

Introduction

Note: SAS No. 145

This module reflects the issuance of Statement on Auditing Standards (SAS) No. 145, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement.*

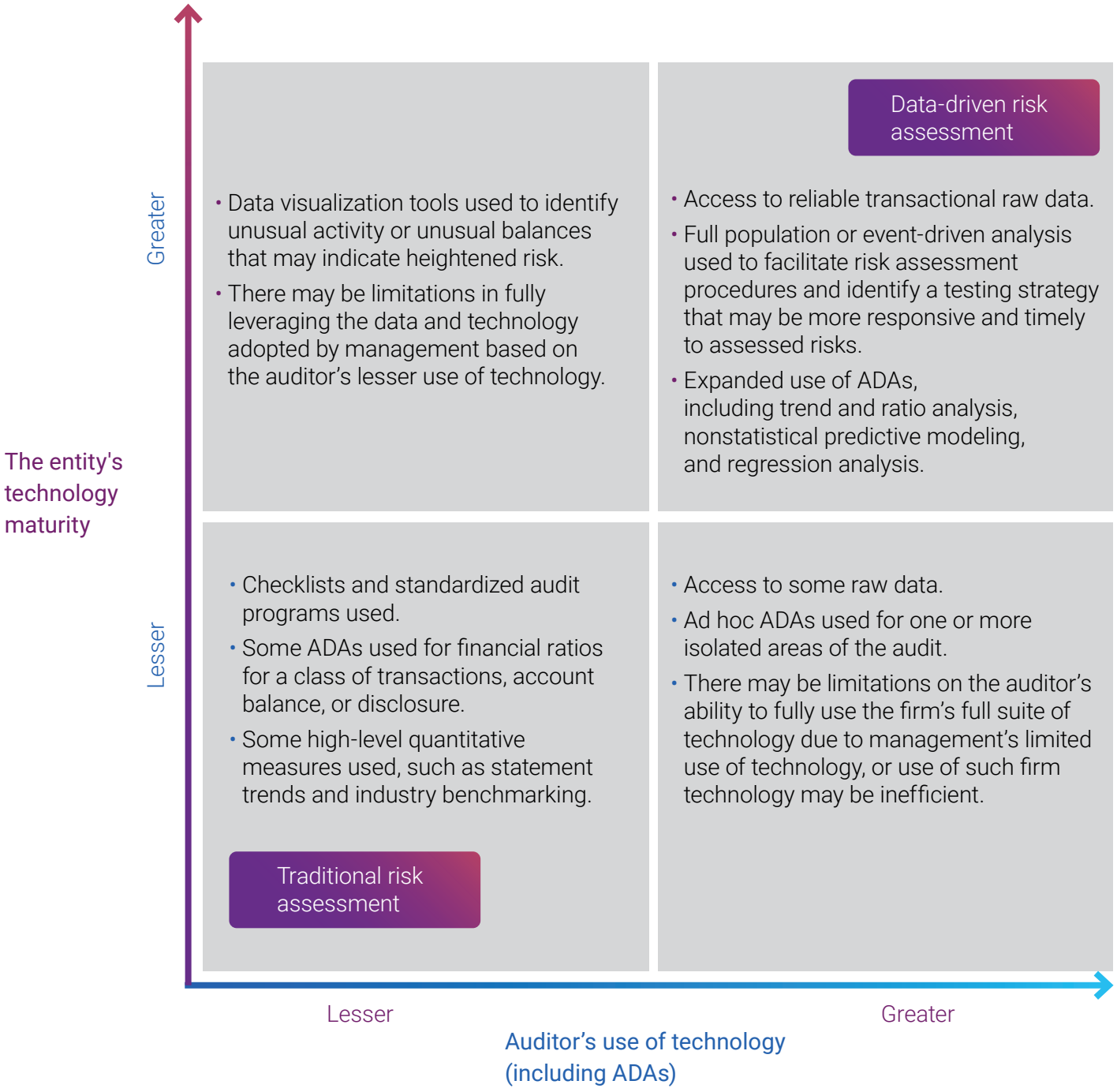
1B.01 — The purpose of Module 1-B, "Commonly used automated tools and techniques in the auditor's risk assessment," is to help you, the auditor, understand the commonly used forms of automated tools and techniques and how they may be used when performing your risk assessment procedures. (Throughout this module, the auditor is referred to as "you.")

1B.02 — Module 1-A, "The benefits of leveraging technology in the auditor's risk assessment and of obtaining an understanding of the entity's use of technology," established the importance of obtaining an understanding of the entity's IT maturity to optimize your use of technology in the audit. It also demonstrated the benefits of using technology when performing your risk assessment procedures in an audit of financial statements. This module will build on the foundation laid in the first module by taking you deeper into commonly used types of automated tools and techniques and how they may be used when performing risk assessment procedures.

1B.03 — As discussed previously in module 1-A, entities with a higher IT maturity typically have a greater investment in technology, along with effective implementation of such technology, resulting in a greater volume and reliability of data. Often entities with a higher IT maturity will have a highly automated control infrastructure; process or control validation; continuous, real-time monitoring; and ongoing innovation and investment. For entities at a lower level of technology maturity, the auditor will often see more manual processes, fewer technology-driven applications, and less investment in and less effective implementation of technology.

1B.04 — Exhibit 1B-1, "The auditor's use of technology considering the entity's technology maturity," illustrates how an auditor may approach using automated tools and techniques, such as audit data analytics (ADAs) in risk assessment, when the entity has a lesser or greater adoption of IT, while also considering the auditor's use of technology. Using ADAs can assist auditors in analyzing large volumes of data, which in turn may enable them to develop a more granular risk assessment and therefore a more targeted response to assessed risks of material misstatement, benefiting audit quality. For certain automated processes, technology-based tools may assist auditors in determining whether identified controls have been implemented. (See paragraph 1B.08 for a description of ADAs.)

Exhibit 1B–1: The auditor's use of technology considering the entity's technology maturity



How automated tools and techniques may be used in the audit

1B.05 — AU-C section 500, *Audit Evidence*, highlights the fact that you may use automated tools and techniques for the purpose of planning or performing the audit, such as ADAs.[1] *Automated tools* include, when applicable, the hardware and software (or particular aspects of software) that are used. Automated tools can include remote observation tools as well as data analytics software packages available for purchase.

1B.06 — *Remote observation tools* relate to ways in which you can perform observations remotely. For example, a camera mounted on a drone or a video transmission may aid the auditor in performing an inspection or an observation procedure, such as management's physical inventory count.[2] Remote observation tools are being used more and more as audits are performed in hybrid environments (that is, parts of the audit are on-site and others off-site).

1B.07 — *Automated techniques* are variations in the way an ADA might be applied. These may include, for example, the way in which data is accessed, organized, analyzed, and how the results are communicated. In additon to ADAs, automated techniques can include

- artificial intelligence (AI) and machine learning and
- robotic process automation.

Audit data analytics

1B.08 — Paragraph .A4 of AU-C section 500 describes ADAs as "the analysis of patterns, identification of anomalies, or extraction of other useful information in data underlying or related to the subject matter of an audit through analysis, modeling, or visualization." ADAs are techniques that can be used to perform various audit procedures, including elements of risk assessment, tests of controls, substantive procedures (that is, tests of details or substantive analytical procedures), or concluding procedures. Some benefits of making more use of ADAs include

- improved understanding of an entity's operations and business risks, including the risk of fraud.
- increased potential for detecting material misstatements.
- improved communications with those charged with governance.

1B.09 — The use of ADAs in performing risk assessment procedures may relate to the identification of risks of material misstatement, the assessment of such risks, or both. As the entity's IT environment matures and management increases its use of IT, using ADAs may make the audit more efficient and effective.

[1] Paragraph .A4 of AU-C section 500, *Audit Evidence*.

[2] See paragraph .A53 of AU-C section 500.

1B.10 — There are various techniques that can be used to help achieve the objective of an ADA. For example, you will want to determine the nature and extent of the use of *visualization techniques*. The term *visualization* may refer to the use of various types of graphics (for example, charts, scatter diagrams, trend lines), tables, or combinations thereof in formats such as dashboards.[3] Graphics may be used as part of an ADA to quickly identify matters that may be significant to performing and reaching conclusions from the ADA (for example, a bar chart or scatter plot showing trends in sales may make it easier to view and identify possible issues than would be possible by reviewing a traditional report of sales numbers).[4] In addition to *visualization techniques*, other techniques include the following:

a. **Process mining.** Process mining allows you to analyze transaction cycles. It can be used in risk assessment to help understand business processes in more detail.[5]

b. **Ratio analysis.** Calculating ratios can also be considered a technique (for example, liquidity ratios, leverage ratios, and margin ratios, to name a few). Calculations can be compared to those for previous years and charted in a graphic.[6]

Note: AICPA *Guide to Audit Data Analytics*

AICPA *Guide to Audit Data Analytics* complements the discussion in this module. This module is designed to make auditors aware of how various ADAs may be efficiently and effectively used when performing risk assessment procedures in a financial statement audit performed in accordance with generally accepted auditing standards, and it helps auditors identify and address matters that they may encounter in deciding whether to use ADAs when performing risk assessment procedures. This module does not cover the types of ADAs that may be used in all aspects of the audit, only those specific to the auditor's risk assessment.

(Note: AICPA *Guide to Audit Data Analytics* has not yet been updated to reflect the issuance of SAS No. 145; however, the concepts contained in that guide related to ADAs remain relevant.)

[3] A dashboard is a series of related graphics or visualizations that the auditor may use to analyze the underlying data, similar in concept to speedometers, odometers, and gas gauges used on dashboards of automobiles.

[4] See paragraphs 1.20–1.26 in AICPA *Guide to Audit Data Analytics* for further discussion about visualizations.

[5] AICPA *Guide to Audit Data Analytics* includes an example of how process mining can be used in risk assessment in example 2.5 (par. 2.59). This example also provides a visualization of a business process. (Note: AICPA *Guide to Audit Data Analytics* has not yet been updated to reflect the issuance of SAS No. 145, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement*; however, the concepts contained in that guide related to ADAs remain relevant.)

[6] See example 2-2 (par. A.12) in AICPA *Guide to Audit Data Analytics*.

Artificial intelligence

1B.11 — AI is the science of teaching computer programs and machines to complete tasks that normally require human intelligence. AI is a key technological driver that enables continuous audit and data analysis — it is changing the future of auditing. Advances in AI technology are automating tasks that previously only humans could perform, including accounting, tax, and audit data gathering. AI could identify unusual transactions while also providing insights on relevant considerations you might take into account, including the applicable standards (accounting, disclosure, auditing, or regulatory standards), similar historical situations, or outcomes from publicly available sources (including similar situations from industry peer groups). The AI could also analyze board meeting minutes or key communications to assist the auditor in identifying additional risks and requesting relevant supporting information, as well as scheduling meetings with the appropriate individuals to discuss audit matters. This is all in addition to being able to process large amounts of data (such as reading bank statements and legal contracts) and reconcile accounts many times faster than a human auditor can and with fewer errors.[7]

Machine learning

1B.12 — Machine learning is an advanced form of AI that uses algorithms to guide its predictions. Its name is derived from the ability of algorithms to "learn" from experience (for instance, by using data sets) rather than relying on a rules-based system. The algorithms create computational models that process large data sets to predict outputs and make inferences. More data leads to more examples; this helps the algorithm finely tune its output over time. In this way, the algorithm adjusts — or "learns" — by trial and error.[8]

Robotic process automation[9]

1B.13 — Robotic process automation (RPA) is a set of software capabilities that can automate high-volume, repeatable tasks such as answering questions, making calculations, maintaining records, and recording transactions. RPA and analytics can be used to extract data from prior periods or interim financial statements to determine proposed materiality based on a range of benchmarks. The same techniques can be used to determine materiality in a continuous or real-time audit. RPA and analytics can be applied to identify anomalous transactions or areas that have not followed the understood course of business to determine scope and focus of testing on accounts or transactions that appear to present a greater risk of misstatement.

[7] *The Data-Driven Audit: How Automation and AI Are Changing the Audit and Role of the Auditor*, © 2020, by Chartered Professional Accountants of Canada. All rights reserved by owner. Used with permission. *The Data-Driven Audit* is a joint publication of the AICPA and the Chartered Professional Accountants of Canada and is part of a series of resources on AI.

[8] *A CPA's Introduction to AI: From Algorithms to Deep Learning, What You Need to Know*, © 2019, by Chartered Professional Accountants of Canada. All rights reserved by owner. Used with permission. *A CPA's Introduction to AI* is a joint publication of the AICPA and the Chartered Professional Accountants of Canada and is part of a series of resources on AI.

[9] This section on robotic process automation is based on content from appendix A, "Auditing with Automation, Analytics, and AI," of *The Data-Driven Audit: How Automation and AI Are Changing the Audit and Role of the Auditor*, © 2020, by Chartered Professional Accountants of Canada. All rights reserved by owner. Used with permission.

1B.14 — Automating business processes using RPA expands auditors' capacity, but it also introduces new risks to the system of internal control. Therefore, designing new testing approaches is the new challenge for auditors. As is the case with AI, RPA presents opportunities for significant advances in the way that audits are performed; however, auditors will want to be aware that new skills and expertise may be required.

1B.15 — "Audit bots" can perform repetitive tasks through RPA. For instance, these "audit bots" can do the following:

- Copy data across different audit files without risk of human fatigue or input errors.
- Run calculations (typically those that require business rules to be considered, such as simple tax calculations) to assist in determining financial statement mathematical accuracy, internal consistency, and tie-outs of prior-year amounts.
- Rebuild financial statements from underlying data to form independent expectations of the financial statements for tie-out purposes.

1B.16 — *Risk assessment RPAs.* Risk assessment RPAs can be used to source information from subscription databases and publicly available information sources as part of the typical planning cycle. The following are examples of RPAs:

- Extraction of information from prior-period financial statements; key financial metrics used in risk assessment; and extraction of bodies of text for natural language processing (NLP).[10]
- Effective categorization and recording of geographic and industrial data for comparisons (for example, generating ratio analysis appropriate for the given industry or geography as applicable).
- Completion of nonjudgmental independence checks; review of entity structures and associated and related entities with internal audit department records and investments held, which assists in making relevant independence considerations; and background checks of entity directors or owners. This information will inform the auditor's assessment of independence (in fact and appearance).
- Acquisition of entity listing status across the globe. Geographical registrations of entity names and numbers are automatically obtained and populated in the risk profile of an entity.
- Acquisition of market data on clients. For example, the auditor can gather information on the percentage of an entity's stock that is held in a short position, which can be a leading indicator of potential going concern issues.

[10] Natural language processing, or NLP, is everywhere. We interact with NLP in the form of autocorrect on our phones, spell check tools, grammatical error detection software, and when we Google something. In essence, it is the ability of a computer system or device to understand spoken or written natural language in order to provide a range of insights or answers.

1B.17 — *Optical character recognition (OCR)*. OCR can be used to extract terms from standard contracts to perform comparisons and ensure no changes have been made (or to evaluate the changes). Due to evolving accounting standards, leases are a good example of an area that can benefit from large-volume data analysis and extraction of key contract term information. Contract information can be used to substantively test the population as a whole or simply identify riskier areas for targeted review and testing.

1B.18 — AI tools exist that read text and provide summaries of the key messages. These tools could identify standard and nonstandard terms in a contract and summarize these terms for review. This would allow the auditor to focus on the reasonability of the key terms and understand how the contract fits within the larger business picture.

1B.19 — *Cognitive automation.* Cognitive automation, which refers to AI techniques applied to automate specific processes, creates more capabilities. For instance, companies are using cognitive automation to perform signature verification (through digital image processing) for contract assurance.

Examples of audit data analytics in risk assessment

1B.20 — Often as management's use of IT expands, there is an opportunity for you to access more data from the entity, enabling you to use more ADAs. Exhibit 1B-2 shows some examples of how ADAs may be used to help enhance the auditor's risk assessment, based on the level of data available to the auditor (see page 23.)

Exhibit 1B-2: Examples of ADAs in risk assessment

	Less access to data →		More access to data
Examples of ADAs in risk assessment	With access to an entity's current and prior-year data, you may use an ADA to identify general ledger accounts that may have unusual changes from previous years, including unexpected trends in liquidity, leverage, and margin ratios that may result in changes to the planned nature, timing, and extent of other risk assessment procedures or further audit procedures to be performed in response to the assessed risk. General ledger ADAs may include the following: • Journal entry queries — Keyword search — "related party" — Unusual posters — Unusual dates • Posting pattern analysis — Debit/credit combinations — Account posting timing (See example 2-2, "Preliminary General Ledger Account Balance Analysis," of appendix A, "Examples of ADAs Used in Performing Risk Assessment Procedures," in AICPA *Guide to Audit Data Analytics*.)	With access to an entity's subledger transactional data, you may use an ADA to produce a visualization of transaction detail to assist you in identifying areas that might represent specific risks relevant to the audit, including the existence of unusual transactions and events, and amounts, ratios, and trends that warrant investigation. Subledger ADAs may include the following: • Many business rule–based tests • Outlier detection • Benford's law • Regression • Cluster analyses (See par. .A60 of AU-C section 500)	With access to an entity's enterprise resource planning (ERP) system[11] event logs, you may use a process-mining ADA to help obtain an understanding of the business process, the related transaction flows through the system, and the entity's application controls. This may aid you in your analysis, for example, of where and how employees might circumvent controls, or take advantage of gaps in controls that had not previously been identified, to perform unauthorized actions. Such actions could increase the assessed risk of material misstatement due to error or fraud and result in further audit procedures to be performed in response to the assessed risk. (Note: When you have this level of data [and potentially gain comfort over a complete population] your audit strategy may shift toward a controls-based approach to support the reliance on the inputs used for analytics.) (See example 2-5 of appendix A in AICPA *Guide to Audit Data Analytics*).

[11] An ERP system is a software system that entities use to manage day-to-day business activities such as accounting, procurement, human resources, manufacturing, and more.

1B.21 — Although more access to data might enable you to use more ADAs, more data does not always lend itself to providing persuasive audit evidence. In accordance with AU-C section 500, in evaluating information to be used as audit evidence, the auditor should consider whether the results of audit procedures provide a basis for concluding on the sufficiency and appropriateness of audit evidence obtained.[12]

Module 1-B key takeaways

1B.22 — Module 1-B has explained various types of automated tools and techniques that may be used when performing your risk assessment and has provided you with some examples. Here are a few key takeaways to remember:

a. Technology is continuing to advance and is becoming increasingly accessible for both the entity and for auditors.

b. The entity's IT maturity may affect how well you optimize your use of technology in the audit (see module 1-A for further discussion about the benefits of obtaining an understanding of the entity's IT maturity).

c. Using technology in your audit may help you perform a robust risk assessment.

d. The entity does not need advanced technology for you to use technology in the audit.

e. Even the simplest technology can add value to the audit.

f. Many off-the-shelf tools that are already being used by you and the entity may contain ADA capabilities and artificial intelligence. As these tools continue to evolve, it will become easier to incorporate use of technology in the audit.

g. Don't forget the documentation requirements relating to performing your risk assessment. See paragraph .42 of AU-C section 315, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement*, for documentation requirements. Also, paragraphs 1.48–1.56 of AICPA *Guide to Audit Data Analytics* discuss matters related to documenting ADAs.

1B.23 — The example in module 1-C, "Example of the auditor's use of technology when performing risk assessment procedures," is designed to illustrate a traditional risk assessment approach and how that may differ from a technology-enabled risk assessment approach.

[12] Paragraph .09 of AU-C section 500.

Module 1-C: Example of the auditor's use of technology when performing risk assessment procedures

1C.01 — The purpose of module 1-C, "Example of the auditor's use of technology when performing risk assessment procedures," is to illustrate how auditors can use technology when performing risk assessment procedures.

1C.02 — Recall that module 1-A, "The benefits of leveraging technology in the auditor's risk assessment and of obtaining an understanding of the entity's use of technology," established the importance of obtaining an understanding of the entity's IT maturity to optimize your use of technology in the audit. Module 1-B, "Commonly used automated tools and techniques in the auditor's risk assessment," then helped you, the auditor, better understand the commonly used forms of automated tools and techniques and how they may be used when performing risk assessment procedures. (Throughout this module, the auditor is referred to as "you.")

1C.03 — This module will illustrate a traditional[1] risk assessment approach and how that may differ from a technology-enabled risk assessment approach for a fictitious retail company, "Bling, Inc." Although traditional risk assessment approaches may use some form of technology, this illustration will contrast a more traditional risk assessment approach with one that uses more advanced technology so you can see the benefits of using technology in the audit.

Example: Bling, Inc.

1C.04 — The following example about "Bling, Inc." will help illustrate how you may use technology when performing risk assessment procedures.

Background

1C.05 — For purposes of this example, the following circumstances apply:

- Bling, Inc. is a high-growth multi-state retailer.
- This is the second year in which Member CPA Firm is auditing this entity.
- Bling, Inc. uses a cloud-based off-the-shelf software technology to maintain its books and records.
- Revenue was determined to be material during the initial planning and scoping with the occurrence (cut-off) and accuracy assertions being more susceptible to misstatement.
- Bling, Inc.'s business is seasonal and, as a result, revenues are usually higher prior to holidays such as Black Friday and Christmas.
- The customer base does not fluctuate significantly from period to period.
- In Member CPA Firm's technology-enabled risk assessment approach,
  - the audit data analytic (ADA) was performed after initial planning and scoping as part of the ongoing and iterative risk assessment process.
  - Member CPA Firm used an artificial intelligence (AI) supported data analytics program that can analyze an export file or can directly import data from the management tools to the auditor tool.
  - all the transactions within the account were subject to the same processes and controls.

[1] For purposes of this document, a "traditional risk assessment approach" refers to performing risk assessment procedures with minimal use of technology.

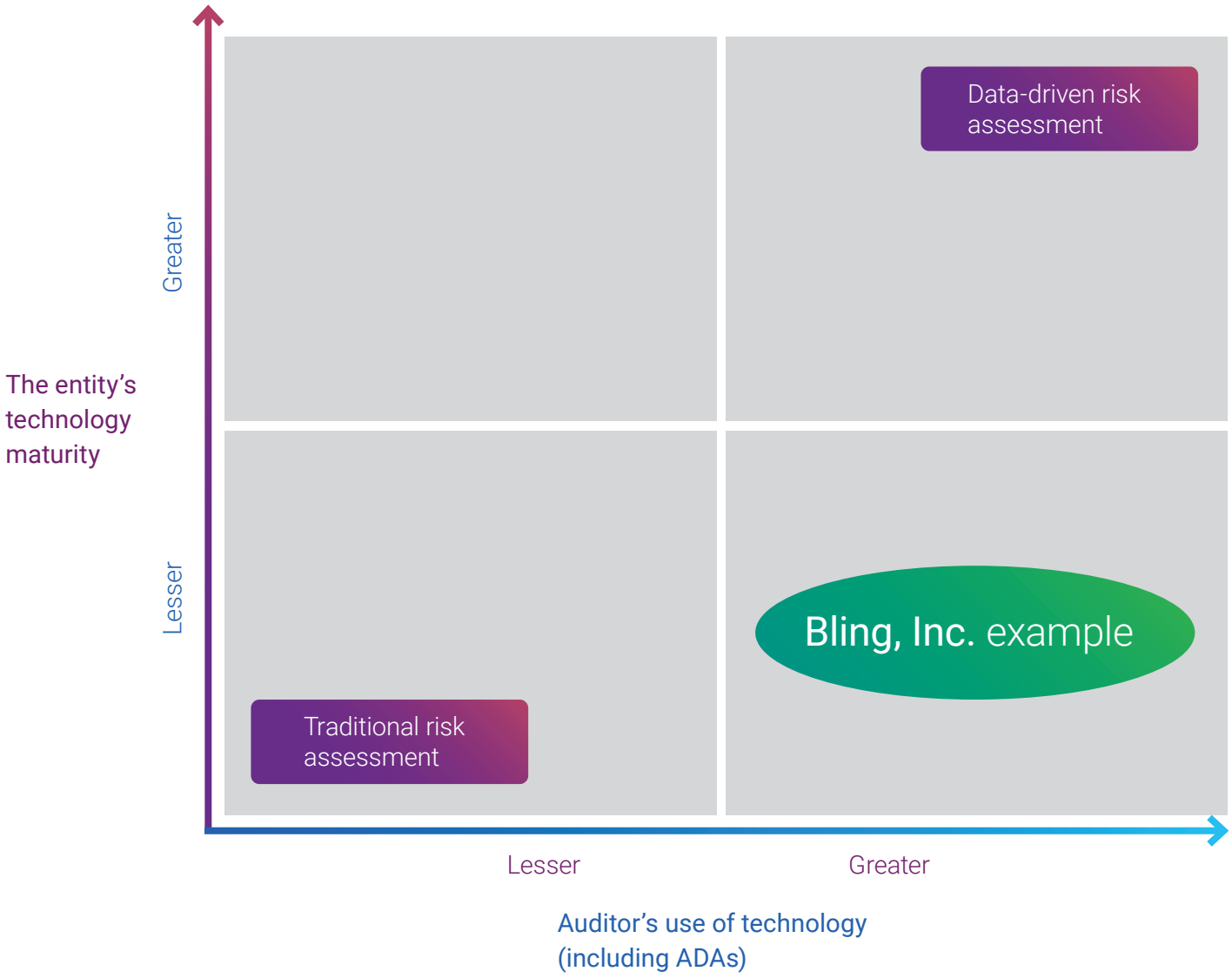
— the purpose of the ADA was to help the auditor determine whether there were any unusual changes or trends in revenue that might affect the auditor's assessment of risk of material misstatement.

— data used in the ADA is relevant and reliable and has been tested for accuracy and completeness.

Note

Think back to exhibit 1B-1, "The auditor's use of technology considering the entity's technology maturity," in module 1-B. This example relates to an entity (Bling, Inc.) with lesser technology maturity and an auditor (Member CPA Firm) with greater technology maturity. See exhibit 1C-1, "Illustration of Bling, Inc.'s technology maturity and Member CPA Firm's use of technology."

Exhibit 1C-1: Illustration of Bling, Inc.'s technology maturity and Member CPA Firm's use of technology



1C.06 — The following paragraphs contrast a traditional risk assessment approach with that of a more technology-enabled risk assessment approach.

Traditional risk assessment approach

1C.07 — Under AU-C section 315, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement*, the auditor's risk assessment procedures and related activities include performing a variety of procedures to obtain audit evidence that provides an appropriate basis for the identification and assessment of risks of material misstatement, whether due to fraud or error, at the financial statement and assertion levels.

1C.08 — Risk assessment procedures are aimed at understanding an entity and its environment, the applicable financial reporting framework, and the entity's system of internal control. Risk assessment procedures include[2]

- inquiries of management and other appropriate individuals within the entity, including individuals within the internal audit function (if the function exists);
- analytical procedures; and
- observation and inspection.

1C.09 — In this example, through performing risk assessment procedures, Member CPA Firm discovered some large special orders that Bling, Inc. was able to acquire that contributed to its growth. Member CPA Firm assessed the identified relevant assertions[3] relating to revenue close to the upper end of the spectrum of inherent risk.

Technology-enabled risk assessment approach

1C.10 — Leveraging additional technology, Member CPA Firm was able to perform further data analysis that enabled it to refine the nature, timing, and extent of audit procedures to more appropriately tailor them to the assessed risks of material misstatement.

1C.11 — In this example, because of the use of additional technology, Member CPA Firm was able to note that although revenue has been determined to have a risk of material misstatement at the relevant assertion level, it would be beneficial to perform a more granular risk assessment to focus Member CPA Firm's work effort on those transactions that represent higher risk. This enables Member CPA Firm to refine the nature, timing, and extent of audit procedures to more appropriately tailor them to the assessed risks of material misstatement. It would be difficult to gain this level of refinement in the auditor's risk assessment using the traditional audit approach.

1C.12 — Therefore, Member CPA Firm wanted to use an approach that allows the full population to be analyzed at the risk assessment phase of the audit to refine its risk assessment of revenue. To use this revised approach, Member CPA Firm requested an interim general ledger to input into the data analytics program, which then ran a series of tests of the full population of data to determine how different each transaction was from every other transaction.

[2] See paragraph .14 of of AU-C section 315, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatemen*t.

[3] An assertion about a class of transactions, account balance, or disclosure is relevant when it has an identified risk of material misstatement. A risk of material misstatement exists when (a) there is a reasonable possibility of a misstatement occurring (that is, its likelihood), and (b) if it were to occur, there is a reasonable possibility of the misstatement being material (that is, its magnitude).

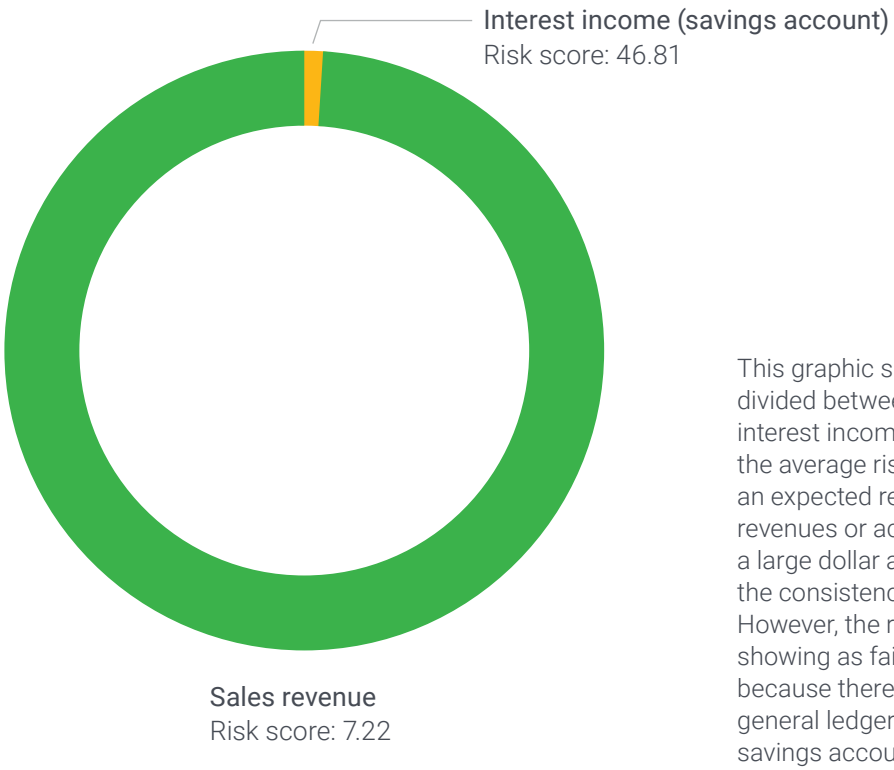
Note: Reliability of audit tool and data reliability

It is important for Member CPA Firm to determine its ability to rely on the audit tool used to perform the risk assessment analysis and the data being used. Recall that module 1-A discussed data reliability. Before Member CPA Firm can use the interim general ledger as input into the computer system, Member CPA Firm will need to evaluate whether the information is sufficiently reliable.

1C.13 — Once each transaction was provided a score to denote how different (that is, anomalous) it was from other transactions, then the scores could be aggregated through methods such as averaging by significant class of transaction or account balance, or by adding dimensions of granularity such as region, department, or service line, depending on the level of detail in the general ledger.

1C.14 — After analyzing all transactions by using its technology (the data analytics program discussed in paragraph IC.05 under "Background"), Member CPA Firm used the following graphics that were created by the technology (see pages 29–30).

Figure 1C-1: Allocation of amounts compared to average risk by type of revenue[4]

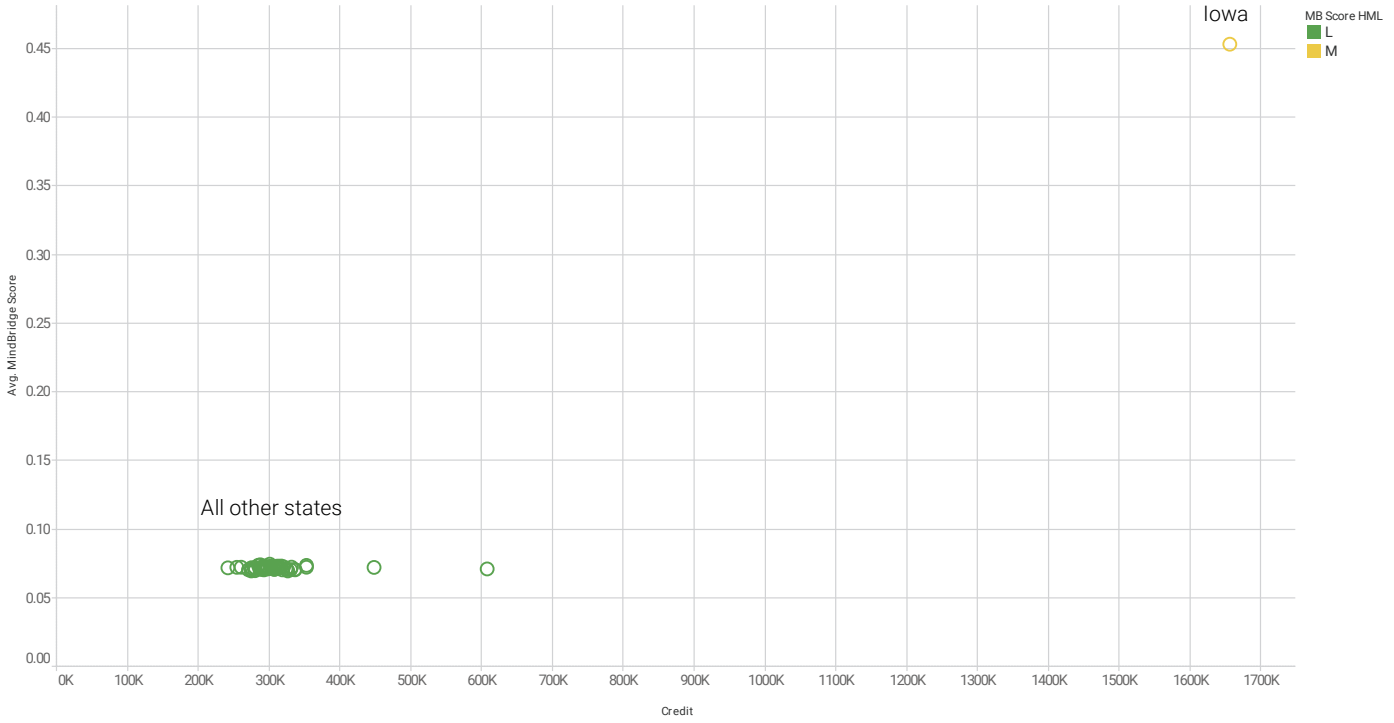


This graphic shows the relative amount of revenue divided between operating sales revenue (green) and interest income from a savings account (yellow), with the average risk score annotated on the graphic. It is an expected result that large amounts of operational revenues or activities should be fairly similar and have a large dollar amount total but a low risk score due to the consistency and general similarity of transactions. However, the relatively small other revenue amount is showing as fairly high risk, likely due to its infrequency because there are not many transactions in the entire general ledger that are similar to it. This is because savings account interest transactions may only happen 12 times a year. The yellow component is likely immaterial and insignificant to the audit due the small dollar amount and the low-risk nature of savings account interest and may not warrant further audit considerations.

Note: The identification of interest income in the same account as sales revenue may indicate IT design or control issues; this anomaly may be further considered by Member CPA Firm in performing the audit and may be shared with management for their further consideration.

[4] The risk score was calculated using Ensemble AI by MindBridge with a combination of business rules, statistical methods, and machine learning algorithms. This score shows the aggregation, using a weighted average, of how different (that is, anomalous) each transaction is from every other transaction in the ledger for each of the financial statement line items presented. This anomaly detection approach is a type of ADA scoring method outlined in paragraph .A69 in AU-C section 500, *Audit Evidence*. Note: Although Ensemble AI by MindBridge was used for this example, other technology tools might be available that would perform similar risk score calculations

Figure 1C-2: Scatter plot of average revenue risk by amount per region[5]



The data analytic is looking at the characteristics of transactions so that homogenous transactions are grouped together, which results in a lower risk score. The technology then isolates transactions with different characteristics that may result in a higher risk score. Simply put, this helps the auditor isolate different transactions.

This graphic shows the total amount of revenue compared to the averaged risk score for each state of operations. The top right yellow circle represents the state with the greatest revenue as well as the highest average risk. This is an unusual finding because, typically, the largest center of operations that has the most transactions will also have the lowest risk scores. This is because by definition there are high volumes of similar transactions, which helps reduce the aggregate risk score. To be this different from the cluster of green circles representing other states implies that this state has very different operations than the others.

[5] See previous footnote.

Comparison of traditional and technology-enabled risk assessment approach

1C.15 — Using the outcomes in figures 1C-1 and 1C-2, Member CPA Firm decided to bifurcate its assessment of the risk of material misstatement relating to revenue to the high-risk population versus the more routine operations. In the traditional approach, Member CPA Firm was aware that some of the growth was driven by the special requests, but at that early stage in the audit, they were not aware that these were centralized to one location and all other regions remained very consistent with each other in operations. Also, in the technology-enabled approach, Member CPA Firm didn't have to rely on interviewing techniques to develop the appropriate questions to identify and narrow potential risks.

1C.16 — Based on the results of the traditional approach, Member CPA Firm determined that revenue has a higher risk of material misstatement. However, Member CPA Firm was not able to isolate transactions that were more likely to represent a risk of material misstatement, and therefore the testing approach may have been less effective because Member CPA Firm's determination was made on a larger class of transactions (all revenue) versus the more specifically affected classes of transactions.

1C.17 — Using the technology-enabled approach, the identified relevant assertions related to revenue would be assessed lower on the spectrum of inherent risk for all states except Iowa. The identified relevant assertions for Iowa would be assessed as higher on the spectrum of inherent risk (if not already close to the upper end of the spectrum). In the auditor's professional judgment[6], the nature, timing, and extent of procedures on the revenue for all states except Iowa would be reflective of this lower risk assessment. Keep in mind that the auditor may perform substantive procedures or tests of controls, concurrently with risk assessment procedures, such as when it is efficient to do so.[7] Accordingly, Member CPA Firm can use the same system that generated the risk assessment ADA to perform substantive procedures.

[6] For illustrative purposes, this example only considered the inherent risk assessment, and the auditor would combine the above assessment with the assessment of control risk.

[7] Paragraph .A25 of AU-C section 315.

Note: Performing substantive procedures concurrently with risk assessment procedures

AU-C section 315[8] recognizes the ability to use automated tools and techniques (including ADAs) when performing risk assessment procedures. Further, paragraph .A25 of AU-C section 315 explicitly permits performance of substantive procedures concurrently with risk assessment procedures when it is efficient to do so. Exhibit A, "Using ADAs to Simultaneously Accomplish Multiple Audit Procedures," of AU-C section 500, *Audit Evidence*,[9] outlines an ADA scoring model that can "simultaneously accomplish the objectives of both risk assessment and substantive audit procedures."

1C.18 — In this example, using a technology-enabled risk assessment allowed Member CPA Firm to do the following:

a. Obtain some corroborating evidence of its inquiry of management very early in the audit scoping.
b. Do a more granular risk assessment to determine the significant classes of transactions, account balances, or disclosures (such as those that represent a reasonable possibility of a risk of material misstatement), by evaluating the revenue transactions and essentially disaggregating them.

Other considerations

1C.19 — In anticipation of year-end field work, Member CPA Firm obtained a year-end general ledger, compared it to the interim general ledger, and had the system reperform the same analysis. This reperformance of the analysis enabled Member CPA Firm to easily evaluate the appropriateness of its risk assessment determination made in the planning phase, commonly referred to as the "stand back."[10]

1C.20 — In addition to fulfilling the documentation requirements in paragraph .42 of AU-C section 315, Member CPA Firm documented its ability to rely upon the audit tool used to perform this analysis as well as information related to the completeness of the general ledger it was provided.

[8] Paragraphs .A11, .A33–.A37, and .A233 of AU-C section 315.

[9] Paragraph .A68 of AU-C section 500.

[10] Paragraph .40 of AU-C section 315 states that for material classes of transactions, account balances, or disclosures that have not been determined to be significant classes of transactions, account balances, or disclosures, the auditor should evaluate whether the auditor's determination remains appropriate.

Module 1-C key takeaways

1C.21 — Module 1-C has illustrated a traditional risk assessment approach and how that may differ from a technology-enabled risk assessment approach for a retail company. Here are a few key takeaways to remember:

a. Technology is continuing to advance and is becoming increasingly accessible for both the entity and auditors.

b. By performing a technology-enabled risk assessment, Member CPA Firm was able to obtain some corroborating evidence of its inquiry of management very early in the audit scoping.

c. Technology can enable the auditor to perform a more granular risk assessment.

d. Don't forget the documentation requirements relating to performing risk assessment procedures. See paragraph .42 of AU-C section 315 for documentation requirements. Also, paragraphs 1.48–1.56 of AICPA *Guide to Audit Data Analytics* discuss matters related to documenting ADAs.

Appendix

Additional resources

A.01 — Statement on Auditing Standards (SAS) No. 145, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement*, resulted in modernizing AU-C section 315 in relation to IT considerations, including how the auditor addresses risks arising from an entity's use of IT. Appendix E, "Considerations for Understanding IT," of AU-C section 315 provides further considerations for you in understanding the entity's use of IT in its system of internal control. Appendix F, "Considerations for Understanding General IT Controls," of AU-C section 315 provides further explanation of the nature of general IT controls that may be implemented for different aspects of the IT environment.

A.02 — The following list contains additional resources that may provide valuable information relating to the use of technology in the audit.

List of additional resources

Resource	Description
Audit data analytics resources on aicpa-cima.com	This webpage contains available AICPA audit data analytics resources.
A CPA's Introduction to AI: From Algorithms to Deep Learning, What You Need to Know	The AICPA and the Chartered Professional Accountants of Canada have issued two joint publications as part of a series of resources on AI. This is the first in the series and is a foundational resource; it explains the buzzwords and terms you have likely been hearing; discusses the evolution of data, AI, and computing power; and helps you begin learning about AI and how it might affect your work.
The Data-Driven Audit: How Automation and AI Are Changing the Audit and the Role of the Auditor	The AICPA and the Chartered Professional Accountants of Canada have issued two joint publications as part of a series of resources on AI. This is the second in the series and covers the benefits of an AI-enabled audit and how AI will evolve the audit and the role of the auditor. It explores the opportunities for enhanced quality and efficiencies as well as challenges or considerations of implementing automation, analytics, and AI across each phase of the audit. It provides examples of possibilities for using automation, analytics, or AI that could help you identify opportunities in the audit.
"5 Ways Firms Can Use Technology to Transform Audits"	For additional information on how technology has been transforming audits, see the *Journal of Accountancy* article "5 Ways Firms Can Use Technology to Transform Audits" (Dec. 20, 2022).

Resource	Description
Rutgers AICPA Data Analytics Research Initiative (RADAR)	The Rutgers AICPA Data Analytics Research Initiative (RADAR) will facilitate the integration of data analytics into the audit process and demonstrate through research how this can lead to advancements in the public accounting profession. The scope of the research will encompass the testing of theory and methodology to inform the development of professional guidance on the application of audit data analytics. One of the projects under the RADAR initiative, "Multidimensional Audit Data Selection," dealt with developing an approach for filtering through large populations of data and identifying items that may require more testing or review.
Audit data standards	The AICPA Assurance Services Executive Committee's Audit Data Standards Working Group has developed voluntary, uniform audit data standards that identify the key information needed for audits and provide a common framework covering • data file definitions and technical specifications, • data field definitions and technical specifications, and • supplemental questions and data validation routines to help auditors better understand the data and assess its completeness and integrity. Please note that these are voluntary, recommended data standards for the extraction of information. These data extract standards are not required, nor do they represent authoritative audit or accounting standards.
AICPA audit data API	When auditors request client data to analyze as part of their audits, this data (audit data) is typically transferred to the auditor as discrete data files in a custom format. The AICPA has developed an audit data transfer standard in an open API format. This standard builds on the already-developed audit data standards as well as International Organization for Standardization (ISO) standards.
AICPA Audit Risk Assessment Resource	The AICPA has developed this Audit Risk Assessment Resource to provide documentation guidance with respect to the requirements of AU-C section 315 and it is recommended for use on audit engagements that are generally smaller in size and have less complex auditing and accounting issues. The resource is designed to be used as a supplement to a firm's existing planning module whether in a firm-based or commercially provided methodology.

Founded by AICPA and CIMA, the Association of International Certified Professional Accountants powers leaders in accounting and finance around the globe.

aicpa-cima.com

2303-138781