KPMG

AI and automation in financial reporting

Guide

November 2024

Contents

Foreword

Navigating risks, challenges, and adaptation: Governance and internal controls in an AI era

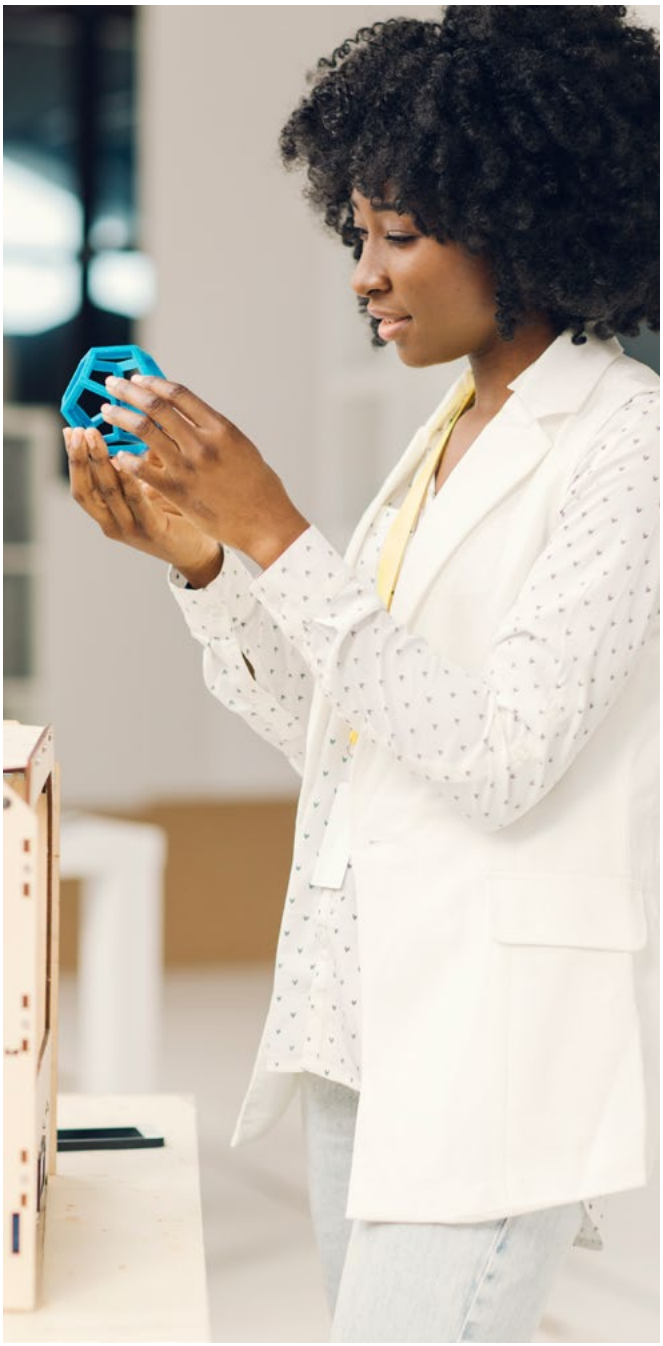
Intelligent Tools—encompassing the spectrum of Automation and Artificial Intelligence (AI) technologies—are being embraced across industries. Many departments within a typical entity have integrated these tools into their operations or are exploring doing so. Financial executives are no exception. These tools not only can meaningfully increase productivity but also can help entities stay ahead in today's rapidly evolving business landscape.

Yet, these tools come with added, but manageable, operational and regulatory risks. New or existing rules and regulations may also require disclosures about how an entity uses this technology, the risks related to its use, and the role the Board of Directors plays in its oversight.[1] Responsible use and strong governance of AI and automation tools promotes confidence of investors and other relevant stakeholders in the capital markets. Those tasked with corporate governance over the financial reporting process need a game plan for identifying the Intelligent Tools already being used in that process, evaluating the ones being considered, identifying the accompanying risks, and responding to those risks by establishing strong governance and control policies and procedures over the tools' development, acquisition, deployment and operation. Management, with board oversight, plays a key role in establishing the right control environment for using these tools.

This publication is designed to assist you in developing and implementing such a game plan for Intelligent Tools used in the financial reporting process. It explains key considerations for identifying and understanding the risks and walks through the process of developing strong governance policies and procedures to respond to those risks.

We hope you find our analysis and insights useful as you start or continue your journey with using Intelligent Tools.

KPMG LLP
Department of Professional Practice



[1] SEC.gov | The State of Disclosure Review

About this publication

This publication is for those tasked with corporate governance over the financial reporting process—whether it be individuals in an oversight role (e.g. board members and C-suite executives), managers with responsibility over financial reporting processes, or professionals who design and operate internal controls within those processes. It is a resource to use when integrating Intelligent Tools into financial reporting—or considering Intelligent Tools for that purpose.

The contents of this publication can be summarized in two broad objectives.

Section	Adapting
Identify the Intelligent Tools you are using or contemplating using in financial reporting	Adapt your internal control over financial reporting (ICFR) to address identified risks
Gain an understanding of how those tools are being used so that you can identify the risks associated with their use (i.e. process risk points (PRPs) and risks arising from IT (RAFITs))	Develop appropriate governance, including entity-level controls, process control activities and general IT controls (GITCs)

The publication explains the key considerations involved in each objective and illustrates how to apply them in practice. Seeing how these considerations are applied in practice brings insight into what the concepts really mean. These insights are highlighted throughout this publication as 'Actions'.

Intelligent Tools and the associated underlying technologies are evolving, and therefore, the considerations, questions and examples in this publication are not static or exhaustive.

Organization of the text

We will walk you through considerations in designing, implementing, and maintaining an effective system of ICFR around the use of Intelligent Tools. We also illustrate differences between governance considerations around AI compared to more traditional automation. While this publication discusses the various aspects of a risk-based approach to ICFR in a sequential manner, designing, implementing and maintaining an effective system of ICFR really is an iterative process.

The key areas discussed are listed in the following table.

Section	Overview
Understand Intelligent Tools	Identify where and how the entity is using Intelligent Tools in financial reporting—e.g.: • used in the financial reporting processes to initiate, process, record and report transactions or information • used to execute controls
Entity-level controls	Considerations around entity-wide risks and applicable entity-level controls
Risk assessment	Considerations around how Intelligent Tools inform risk assessment, including where and how Intelligent Tools are used in an entity's environment and understanding of the entity's overall IT environment

Section	Overview
Process understanding and process control activities	Impact to process understanding and process control activity considerations, including example controls and questions to identify and respond to PRPs
General IT controls	Overview of traditional RAFITs and GITCs, as well as AI-specific risk considerations. This section includes example inquiries and controls to address these risks, as well as considerations when GITCs are executed by AI

Navigation

Guidance: For more information about each general topic, look for references to the Handbook: Internal control over financial reporting

Action: What actions to take

Terminology

Artificial Intelligence (AI) system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment. [Source: OECD]

Controls include entity-level controls and control activities.

Control activities include process control activities and GITCs.

Entity-level controls are policies, procedures and structures that operate at the entity level with an indirect relationship to financial reporting.

Process control activities mitigate a specific risk point within a business process that could lead to a material misstatement of the entity's financial statements.

General IT controls support the continued effective operation of automated process control activities and the integrity of data and information within the entity's IT systems by addressing risks arising from IT.

Abbreviations

We use the following abbreviations in this guide:

COSO	Committee of Sponsoring Organizations of the Treadway Commission
EUC	End-user computing
Gen AI	Generative AI
GITC	General IT control
IA	Internal audit
ICFR	Internal control over financial reporting
ISO	International Organization of Standardization
LLMs	Large language models
NIST	National Institute of Standards and Technology
PRP	Process risk point
RAFIT	Risk arising from IT
SDLC	Software development life cycle
SEC	Securities and Exchange Commission
SOC	System and organization controls

1 What are Intelligent Tools

1.0 What are Intelligent Tools?

Intelligent Tools refers to the spectrum of technology that involves Automation and AI. In many cases, the risks between the various types and uses of Intelligent Tools are different, with the more sophisticated tools posing risks that many entities may not have encountered previously. Therefore, using more sophisticated tools may lead to additional ICFR considerations.

What is automation?

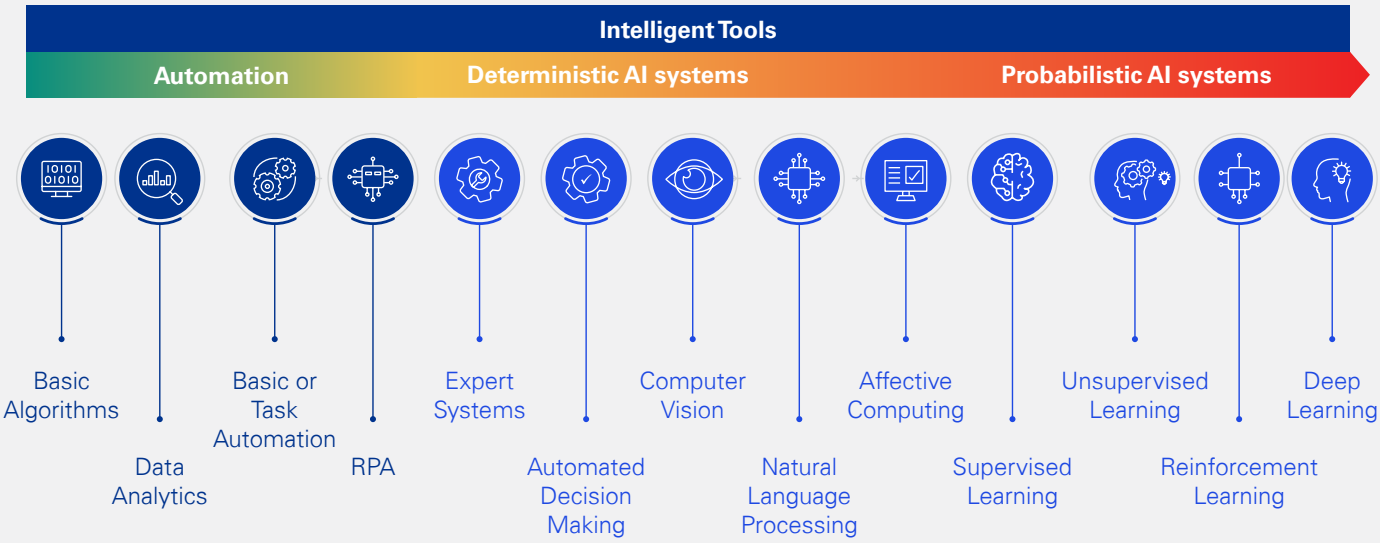
We use the term Automation to mean tools that are used to automate repetitive tasks and processes with the purpose of augmenting a human's activities to improve quality and efficiency. Automation is a spectrum of tools that range from tools that perform data analytics and user-enabled automation to bots that automate repetitive, rule-based tasks or processes (e.g. robotic process automation, or RPA).

What is AI?

We use the term AI to mean tools with advanced algorithms that can perform more complex tasks that expand beyond task automation and can emulate human intelligence to replace humans in performing cognitive tasks. AI is not a single capability, technology or vendor platform. Instead, it represents a progression from systems that rely on explicit rules and knowledge (expert systems), to systems that process unstructured data like images (computer vision) and text (natural language processing, or NLP), to systems that aim to understand and respond to human emotions (affective computing).

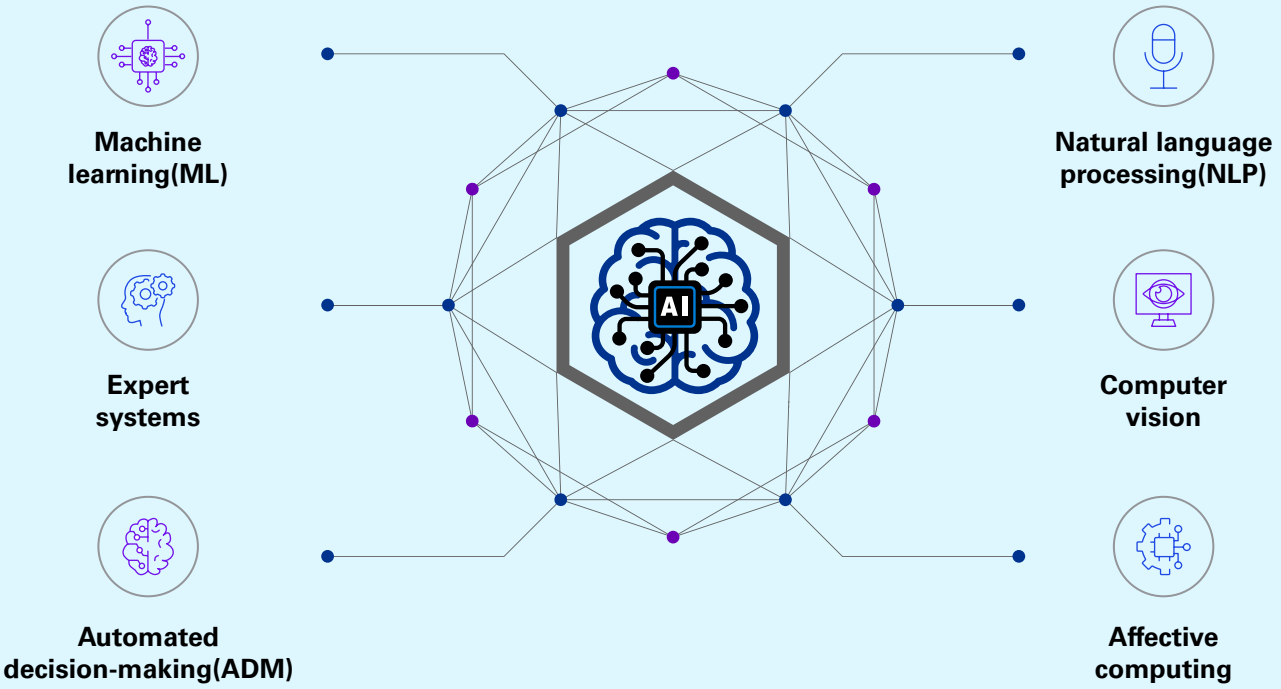
The spectrum of AI extends to machine learning, which enables systems to develop models, predictions, or insights by 'learning' from training data without being explicitly programmed. The machine learning spectrum begins with supervised learning and progresses towards deep learning as training models using labeled data diminish and complexity of models used evolves. These AI systems are further defined in section 1.1.

Understanding where a specific tool falls on the spectrum of Automation and AI helps you identify the related PRPs and RAFITs.



1.1 What are common subsets of AI?

AI is an umbrella term that encompasses a range of interrelated techniques and technologies. Above we demonstrated how the common subsets of AI may fall on a spectrum from simple rule-based logic (deterministic) to more advanced and complex algorithms (probabilistic). Below we provide more information about each of these subsets, including definitions and examples. Click each icon below to learn more.



What is Gen AI and in which subset of AI does it fit?

Gen AI (e.g. OpenAI's ChatGPT, DeepMind's WaveNet, OpenAI's DALL-E) falls in the machine learning subset of AI. It entails deep learning in which algorithms automatically produce content in the form of text, images, audio, and video. Gen AI algorithms, specifically LLMs (e.g. GPT-4, BERT) that include components of natural language generation and understanding, are trained on significant amounts of data. LLMs start from a source input called a prompt and work by predicting the next word or pixel most likely to occur to produce an output. The data used to train Gen AI is created and defined by humans and the algorithms are trained using deep learning with human feedback (i.e. it modifies the response each time to improve the outcome).

What does it mean when we say AI is a 'black box'?

In the context of AI, a 'black box' refers to a model or system whose underlying algorithms are not transparent or explainable. It means that the input-output behavior of the system can be observed, but the internal decision-making mechanisms are not readily accessible or interpretable.

In other words, the 'black box' focuses on the outcome or prediction generated by AI without providing insights into how it arrived at that result.

1.2 What are common subsets of automation?

Basic algorithms

Basic algorithms refer to the fundamental algorithms used in computer science and programming, such as sorting, searching and basic data structures. For example, tools that perform matching rules, which can be programmed with matching rule sets to check for 1-to-1, 1-to-many, many-to-1, and many-to-many matches, such as accounts receivable to cash account matching tools.

Data analytics

Data analytics refer to the process of examining and interpreting data to discover patterns, trends and insights. It often entails using statistical methods and tools to extract valuable information from extensive datasets. Microsoft Power BI® is a common application used to perform computer assisted techniques for data transformation and preprocessing to organize and visualize data.

Another common application used for data analysis is Alteryx®, which is a platform that is used for data preparation, transformation and analysis. Alteryx is commonly used by entities to transform and prepare data for visualization, as well as to automate tasks.

Basic or task automation

Basic or task automation refers to the use of technology to perform tasks or processes with minimal human intervention. It can range from simple tasks like automating repetitive actions in software applications to more complex processes involving multiple systems. For example, an entity could use automation to trigger a computer task after an action is performed, such as sending a customer a contract after the customer selects that they agree to the entity's terms.

Robotic process automation

Robotic process automation, also referred to as 'robotics' or 'bots', is a type of application used to automate manual tasks within a workflow. These tasks are generally repetitive, low judgment and high-volume in nature and are often associated with processes that follow explicit or predictable rules and prescriptive steps. Bots may rely on end-users to trigger the activity (i.e. attended bots) or run independently, enabling work to be scheduled or completed continuously (i.e. unattended bots).

Using the automation example above, after the customer sends the signed contract back to the entity, the bot could extract the information from the contract and put it into a customer record.

1.3 Automation versus AI

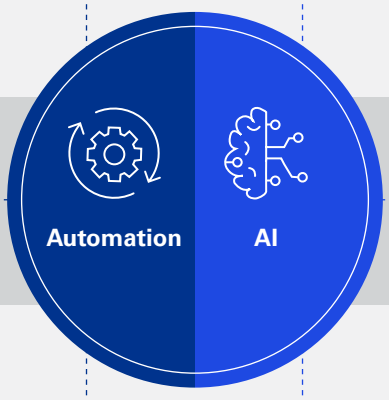
What are the differences between automation and AI and why are they important to understand?

Automation is the use of computer programs to allow a process to operate automatically with minimal human involvement. AI, on the other hand, covers a broad range of computer programs that are intended to mimic human behavior through capabilities such as language and speech recognition, visual perception (i.e. recognizing pictures), learning from experiences, and decision making. Many AI applications implement automation, but not all automation includes AI. Understanding the nature of the technology is important because the type or category of a technology may involve different complexities, subjectivity, and uncertainty. These factors are important in identifying risks (i.e. PRPs and RAFITs).

What are examples of differences between automation and AI?

The following table includes examples to demonstrate where similar scenarios may differ between automation and AI.

Automation	AI
Performs a process by means of programmed commands that are typically rule-based.	*Learns from patterns* in data to provide insights, *without prescriptive code* or rules on how to achieve the outcome.
Generally used for repetitive and routine tasks, such as data entry, processing, and analysis.	
Cannot learn from experience and data.	Can *learn from experience* and data and improve over time.
May be used to improve efficiency, reduce human errors, and increase productivity.	
Cannot make predictions based on data.	Involves development of *algorithms that make predictions* based on data and experiences it is trained on.
Involves the use of technology to perform repetitive tasks that may then be interpreted by humans or other AI to make decisions.	



1.4 What are examples of common use cases?

Action: In your risk assessment, think about these examples when you obtain an understanding of the financial reporting processes to help identify Intelligent Tools and the associated risks (including PRPs and RAFITs).

Intelligent Tools used within the IT system to perform process activities

Below are examples of when an Intelligent Tool is used in a business process or preparation of the financial statements (i.e. the tool is used to initiate, process, record, and/or report transactions).

Automation

- Open or read emails and attachments and extract certain data from specified fields
- Log into web applications
- Extract structured data from documents
- Copy/paste values, fill in forms, move files and folders
- Collect statistics
- Post recurring journal entries

AI

Detecting fact patterns and establishing models, including predictive models and forecasting:

- Simulate market conditions, cash flow predictions and other macroeconomic factors that feed into estimates or cash flow for budgeting
- Analyze supply chain/inventory models that could impact inventory valuation adjustments or related reserves, revenue price adjustments or related reserves, and loan-loss allowances
- Perform analysis on performance targets that impact bonus or commission calculations

Document analysis/scanning large datasets:

- Perform customer evaluations (e.g. credit risk evaluations, loan decision-making)
- Identify relevant data elements in documents, such as within invoices, purchase orders, cash receipts or other third-party documents (e.g. using NLP and computer vision to pull information from unstructured data sources, such as pdfs, scanned documents, or third-party records and then matching them between documents and/or systems)
- Perform supplier evaluations (e.g. scanning for terms that do not comply with vendor policies)

Citations/references:

- Perform research (e.g. accounting research group or legal department using Gen AI models for authoritative literature or regulatory compliance research)
- Identify relevant financial ratios, exchange rates or stock analysis information using Gen AI tools and input the information into schedules or models used in financial reporting processes (e.g. stock compensation calculations, foreign exchange calculations)

Intelligent Tools used to automate process control activities

Below are examples illustrating how Intelligent Tools can be applied in control activities either by integrating the tools into existing controls, or autonomously performing control activities from start to finish. The table presents example scenarios for automation and demonstrates how AI enhances the same use case. When Intelligent Tools are used to automate controls and these controls are relied upon in financial reporting processes, identification of relevant RAFITs is important to enable the related GITCs to be effectively designed and implemented.

See section 5.3 for information on using Intelligent Tools to execute GITCs.

	Automation	AI
Data validation	Validate data by comparing it against predefined rules or criteria to identify exceptions/conflicts for review	Use machine learning to analyze data beyond predefined rules or criteria to identify exceptions/conflicts for review
Access	Compare new user access requests against an approved roles matrix before provisioning access to the IT system	Remove or block access to an IT system based on historical behavior, patterns or unusual activity
Exception handling	Handle exceptions within control activities by following predefined rules or escalation procedures. Automatically route exceptions to the appropriate individuals or departments for resolution	Expand beyond the identification of exceptions/conflicts to often resolve those exceptions/conflicts without human involvement
Example	Using automation to perform user access reviews. Based on pre-defined roles and job functions, the tool automatically generates a report that highlights potential exceptions.	Expanding on the example to the left, AI could perform additional steps to elevate the evaluation: Detect unusual access requests or deviations from typical behavior, access patterns and historical data that goes beyond pre-defined roles and job functions assign risk scores based on type of exceptions to prioritize exceptions remove access based on pre-defined roles and job functions without obtaining human approval first

2 Entity-level controls related to Intelligent Tools

As Intelligent Tools become increasingly integrated into various business processes, establishing strong governance policies and procedures over their development/acquisition, deployment and operation is essential. These policies and procedures can often be entity-level controls, supporting proactive identification and mitigation of potential risks associated with the responsible deployment of Intelligent Tools.

Using the Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework can provide a structured approach to identifying relevant risks, determining appropriate control activities, and managing effective oversight of the use of Intelligent Tools. This section uses the components of the COSO framework and the underlying principles of each component to illustrate entity-level control considerations that directly and indirectly impact financial reporting.

Involving the board of directors

Think about whether the topics discussed below are for full board discussion or whether existing committees or newly established committees will oversee the use of Intelligent Tools. If addressed at the committee level, consider when to inform the full board. Further, we recommend determining whether existing board members possess the requisite competencies to evaluate the relevant considerations. To do so, it may be necessary to pair business strategies with existing member experience to determine if specialized experience and/or education over these topics are necessary.

2.1 Control environment

The control environment COSO component emphasizes the importance of establishing a strong ethical culture, identifying and maintaining the appropriate employee skillset, and setting the appropriate tone at the top. Management, with board and audit committee oversight, play a key role in establishing the right control environment when defining the overall Intelligent Tools vision and strategy in the financial reporting processes and related controls.

Action: Assess whether considerations below apply to you, evaluate the adequacy of your existing policies and procedures, and develop a plan to address these considerations, if required.

COSO principle	Intelligent Tools considerations (AI additional considerations noted in bold)
Principle 1: The entity demonstrates a commitment to integrity and ethical values	Are there policies and procedures in place to enforce that Intelligent Tools are used in accordance with the entity's integrity and ethical values? **Does the entity handle personally identifiable information (particularly in industries such as financial services and healthcare)? If so, how will the use of that information comply with applicable privacy and data protection laws and regulations if employees are allowed to use AI in their processes?**
Principle 2: The board of directors/ those charged with governance demonstrates independence from management and exercises oversight of the development and performance of internal control.	Are there procedures in place to inform those charged with governance of plans to use Intelligent Tools, including in financial reporting, so they can exercise oversight for the development and performance of ICFR? **Who is responsible for overseeing the AI initiatives and evaluating compliance with relevant regulations and ethical considerations?** **Are there specialized skills needed by those charged with governance to assist in risk assessment and understanding of AI being implemented?**
Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Has an overall Intelligent Tools vision and strategy been defined? Are policies, procedures, and guidelines in place to identify and acquire or design, deploy, and monitor Intelligent Tools? Are there specific governance or policies around the use of Intelligent Tools (i.e. what is the established process for the use of Intelligent Tools to assist or replace existing processes)? What use cases are planned and what is management's strategic roadmap to implementation? How is ownership and accountability of Intelligent Tools assigned? Are the individuals that oversee overall governance integrated into the delivery model, including providing risk oversight and direction on risk identification, evaluation, mitigation? Is Internal Audit (IA) involved in the integration of governance, risk, and control considerations throughout the Intelligent Tool's lifecycle? **Does the entity have the requisite expertise to identify and acquire or design, deploy and monitor AI?** **Will you need to engage third parties to identify and acquire or design, deploy and monitor AI?** **Do individuals responsible for overseeing outsourced service providers understand their responsibilities for AI oversight?**

COSO principle	Intelligent Tools considerations (AI additional considerations noted in bold)
Principle 4: The entity demonstrates a commitment to attract, develop and retain competent individuals in alignment with objectives.	Does the entity's Intelligent Tool deployment framework contemplate whether employees possess necessary competency and capabilities? If not, how does the entity plan on acquiring the necessary skillsets? What training offerings are available to upskill employees? **Is there an individual or team organized to focus on the emergence of AI, including evaluating the potential impacts?** **How are IT team members and other subject matter experts involved in decision-making and implementation of AI?**
Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Are there mechanisms in place to address non-compliance with roles and responsibilities concerning the implementation of Intelligent Tools, as well as the ongoing oversight of these tools? **Have you assessed if there are new performance metrics necessary for evaluating employees in relation to AI?** **Are the performance measurements and reward plans tied to the implementation of AI aligned with the entity's ethical values and ICFR objectives?**

2.2 Risk assessment

The risk assessment COSO component involves the entity's process for identifying and assessing the potential risks to financial reporting that may arise from using Intelligent Tools. Conducting a thorough risk assessment when Intelligent Tools are introduced into processes, including financial reporting processes is crucial for managing risks and achieving objectives.

Do these considerations differ when thinking about AI?

Risk assessment can be especially challenging when AI is introduced into processes, including financial reporting processes and may require considering new and emerging risks. For example, risks related to data privacy breaches, algorithmic bias, or the reliability of the solution can arise when AI is involved in decision-making.

Action: Assess whether considerations below apply to you, evaluate the adequacy of your existing policies and procedures, and develop a plan to address these considerations, if required.

COSO principle	Intelligent Tools considerations (AI additional considerations noted in bold)
Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Is the deployment of the Intelligent Tools consistent with the entity's objectives of producing reliable financial statements in accordance with the applicable financial reporting framework? Are the Intelligent Tools designed to support accounting and financial reporting in accordance with the applicable financial reporting framework? **Have you determined the criteria for acceptable use of AI across the entity?**
Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Have you developed a risk and control framework that aligns with the Intelligent Tool operating model? Have you updated process narratives, flowcharts, etc. for the use of Intelligent Tools, if applicable? Have you identified PRPs and RAFITs related to the use of Intelligent Tools? **Is the entity's risk assessment at the appropriate level of specificity to address AI that may be designed to change or adapt over time?** **Is there a policy in place over when human involvement is required in the process or ICFR (e.g. a manager is not permitted to use AI to review the output provided from AI)?**
Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	How have you considered whether Intelligent Tools provide greater opportunities for employees or third parties to commit fraud? Have you identified new fraud risks because of Intelligent Tool deployment? **Have you considered the use of AI in your fraud risk assessment?** **Are you aware of the specific fraud risk factors associated with AI (e.g. malicious manipulation of prompts)?**

COSO principle	Intelligent Tools considerations (AI additional considerations noted in bold)
Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	How do you identify the use of Intelligent Tools that impact ICFR, including the identification and assessment of new risks or changes to risks? Do you have a process or policy in place to determine who at the entity is involved in the evaluation of the risks to ICFR? How do you identify the impact of changes in its operations, flow of data or nature of transactions, on the effectiveness of its Intelligent Tools operating in a particular financial reporting process? **How do you evaluate whether model training data continues to be fit for purpose?** **How do you monitor changes in training data on the effectiveness of the tool for its financial reporting objectives?**

2.3 Information and communication

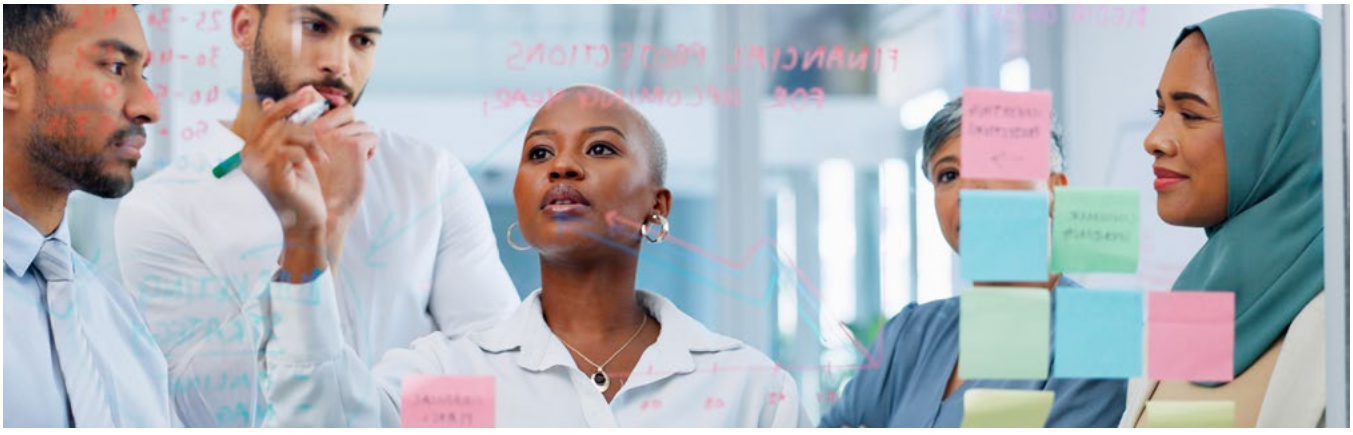
The information and communication COSO component emphasizes the importance of timely and accurate information flow throughout the entity relevant to financial reporting, including information used by the entity's Intelligent Tools. This component of ICFR also provides that relevant information regarding Intelligent Tool systems, their performance, and potential risks or issues are communicated accurately to the relevant stakeholders.

Do these considerations differ when thinking about AI?

Obtaining relevant information and having appropriate communication protocols for any Intelligent Tool is important; however, the type of information collected and communicated may differ for AI versus automation . For example, when automation is used, the information communicated to those charged with governance may include performance measures on the number of successfully completed tasks and error rates. The performance measures for AI may become more subjective or difficult to measure, such as how the model manages bias, how errors are identified, and how the entity is managing responsible use of the technology.

In addition, the nature of information used by AI may differ from the information used by less sophisticated Intelligent Tools. Such information may be more complex and unstructured and present different risks in terms of its relevance and reliability.

Action: Assess whether considerations below apply to you, evaluate the adequacy of your existing policies and procedures, and develop a plan to address these considerations, if required.



COSO principle	Intelligent Tools considerations (AI additional considerations noted in bold)
Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Are there controls over the relevance and reliability of information used by an Intelligent Tool? **Is there an inventory of information used to train AI?** **Are there controls over the information used to train AI used in financial reporting?** **How is an understanding obtained over information used by AI at third-party vendors that is part of the entity's financial reporting process?**
Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Have the responsibilities for controls over Intelligent Tools to address the effectiveness of achieving financial reporting objectives been effectively communicated to responsible parties? **Are there established policies and procedures for making information about the model and decision-making of AI understandable and available to relevant stakeholders?** **Are there communication protocols in place for individuals in financial reporting roles and in IT to communicate to the appropriate individuals at the entity whether there is any use of AI in financial reporting processes or anything that impacts those processes?**
Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	Is Intelligent Tool performance reporting provided to stakeholders and to the public? For example, disclosures in annual filings that outline how these tools impact financial reporting. For an SEC registrant, do disclosures clearly explain how the tools impact the entity's results and operations and describe the risks introduced by using these tools?[2] For an SEC registrant, does the implementation of Intelligent Tools represent a change that is material to the entity's ICFR that should be reported under S-K Item 308(c)? **Have you considered whether there are existing rules or regulations that require disclosure about how the entity uses AI and the risks related to its use?**

[2] SEC.gov | The State of Disclosure Review

2.4 Monitoring activities

The monitoring activities COSO component emphasizes the need to monitor and evaluate Intelligent Tools on an ongoing basis. This requires regularly assessing the effectiveness of controls, conducting ongoing evaluations, and implementing mechanisms for reporting and addressing any identified deficiencies or weaknesses.

Do these considerations differ when thinking about AI?

To mitigate potential risks associated with the use of AI, you may have to conduct monitoring activities more frequently compared to other technologies and at various points within the AI software development lifecycle (SDLC). Data quality and integrity risks, model accuracy and reliability risks, and biases can be effectively identified and proactively addressed when an entity has an appropriate level of monitoring in place.

For AI, monitoring activities that involve continuous human interaction are typically more successful at timely identifying deficiencies than those with less human involvement. For instance, having employees conduct post-deployment reviews at regular intervals to evaluate the performance and fairness of the model aids in identifying potential biases timely. Implementing monitoring controls where employees periodically review the model and the information used for training the underlying algorithms helps identify the need for updates to the models timely. Additionally, monitoring mechanisms that continuously test the model's underlying information and functionality, with human interaction and monitoring of the results, can detect performance issues.

Action: Assess whether considerations below apply to you, evaluate the adequacy of your existing policies and procedures, and develop a plan to address these considerations, if required.

COSO principle	Intelligent Tools considerations (AI additional considerations noted in bold)
Principle 16: The entity selects, develops and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Do monitoring procedures contemplate if Intelligent Tools are used in financial reporting processes or ICFR to identify tools not previously reported? Is there a monitoring program in place for Internal Audit or Compliance reviews over Intelligent Tool deployment? Are you using appropriate combinations of ongoing and separate evaluations to ascertain whether the components of internal control are present and functioning? How do you determine that the Intelligent Tools are operating as intended? Have key performance indicators (KPIs) or key risk indicators (KRIs) been defined to assess ongoing operation of the Intelligent Tools program? How are KPIs and KRIs being monitored, such as tool effectiveness or return on investment? **Are there policies and procedures covering:** • **Model training and testing, including independent bias reviews** • **Identification of and monitoring compliance with applicable laws and regulations** • **Post-deployment monitoring?** **How does the entity address model governance and monitoring to maintain compliance with ICFR requirements?** **How is the model monitored for performance, accuracy and reliability?** **Are there mechanisms to detect and address model drift or degradation over time?** **How are models validated and updated to reflect changes in the underlying data or business environment?** **Are there mechanisms to identify and mitigate potential biases or unintended consequences of algorithms?**
Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	How are Intelligent Tool related KPIs and KRIs reported to key stakeholders? If Intelligent Tool related control deficiencies are identified, are they evaluated and communicated in a timely manner to those charged with governance? **Do you have a process to evaluate the pervasiveness and aggregation of deficiencies identified related to the use of AI?**

3 Risk assessment

Guidance: ICFR Handbook, Section 3. Risk Assessment

Risk assessment is a process conducted to identify potential misstatements in the financial statements. We recommend a top-down approach to performing risk assessment at various levels within the entity - starting at the entity level. To effectively consider the sources and likelihood of potential misstatements in the financial statements, ensure that those responsible for performing risk assessment have sufficient knowledge and understanding of the entity's business, its organization, operations and processes.

What risk assessment considerations are important with respect to the use of AI?

AI can introduce risks that directly or indirectly impact financial reporting.[3] When performing risk assessment consider how the responsible and ethical use of AI is managed. The following questions may assist in assessing the impact to risks.

1. Are there established policies and procedures covering responsible and ethical use, including explainability, accountability, fairness in data and outcomes, security, privacy, safety and data integrity?
2. How does the deployment of Intelligent Tools affect statutory, regulatory or contractual compliance?
3. Has the entity identified a framework to follow for compliance (NIST, ISO, etc.) that is consistent with SEC or other applicable regulations?

KPMG has developed a trusted AI approach, which centers around 10 ethical pillars across the AI lifecycle. You can use a similar approach to establishing a framework for designing, building, deploying and using AI and to understand where risks are present.

[3] "SEC.gov | The Importance of a Comprehensive Risk Assessment by Auditors and Management

3.1 Understand the impact to the entity's environment when using Intelligent Tools

Guidance: ICFR Handbook, Question 2.5.10 | What is the risk assessment component of ICFR? and Question 2.5.100 | What is the importance of identifying risks to the achievement of objectives across the entity and performing an analysis on how to manage them (Principle 7)?

Risk assessment includes evaluating the entity's processes to identify business risks relevant to financial reporting objectives. Performing an entity-level risk assessment may help to identify if and where Intelligent Tools are currently being used throughout the entity. For the Intelligent Tools identified, this assessment includes the impact to the entity's financial reporting objectives. For tools that impact financial reporting, this assessment extends to include identifying new PRPs and RAFITs, where applicable. The table below describes how Intelligent Tools may impact the entity's business and the broader environment in which the entity operates.

Elements of the entity's environment	How Intelligent Tools may impact these areas
Relevant industry, regulatory, and other external factors	The type of Intelligent Tools being used may impact the regulations applicable to the entity. Current regulations pertaining to technology are relevant to Intelligent Tools, and the regulatory landscape around AI is evolving. See further information under non-compliance with privacy laws and regulations below. Certain regulations may be more relevant for specific industries. For example, data privacy and data security regulations may be more relevant for healthcare or financial services entities when they use personally identifiable information in their Intelligent Tools.
The nature of the entity	The entity's organization may impact how Intelligent Tools are deployed and monitored and whether the entity has the necessary resources. For example, there may be additional considerations for entities that use AI to directly interact with customers. Assess the entity's ability to provide appropriate oversight of its technology strategy, and how it adapts its system of internal control to address the development, deployment, and maintenance of Intelligent Tools.
The entity's objectives and strategies and those related business risks that might reasonably be expected to result in risks of material misstatement	Assess how the use of Intelligent Tools fits within an entity's overall business strategies.

How does AI impact business risks?

Business risks may be impacted when the entity uses AI, or may impact the entity's use of AI.

Business risks/economic conditions	Potential business impact
Risks of inappropriate integration/ implementation of new information technology	Financial losses can result if an Intelligent Tool is not implemented properly or if there are inconsistencies between the entity's Intelligent Tool strategy and its business strategies.
Exposure to new legal risks	AI Tools, particularly Gen AI tools, that are built on large amounts of text data from the internet, may pose risks to proprietary data and subject the entity to third-party legal risks. AI Tools may also have biases built into the underlying algorithms that lead to discriminatory practices, which could result in legal liabilities, fines, or reputational damage for an entity.
Non-compliance with regulatory requirements	Evolving regulations in the areas of governance and use of AI could result in non-compliance with regulatory requirements. For example, the SEC requires disclosure in the Form 10-K over the entity's processes to identify and manage material risks from cybersecurity threats, including considerations of board of director's oversight.[4]
Cybersecurity breaches	AI may increase cybersecurity risks for the entity, which could lead to financial losses. See Cybersecurity risks.
Non-compliance with privacy laws and regulations	AI creates increased exposure to corporate compliance risks over privacy and data protection. The use of AI increases the chances of breaches that may compromise sensitive customer or employee data. Additionally, the entity's confidential data could be mismanaged if it is entered into AI that logs and stores all inputs (for future development of the technology) or if it is hosted on an open-sourced platform where individuals outside the entity could gain access to sensitive information. When using AI developed by a third party, think about how to obtain sufficient information from the third-party provider regarding the technology's compliance with applicable laws and regulations.
Changes in industry developments/ competition	An entity may be in an environment where its competitors are using AI and investments in AI will be required to stay competitive. The entity may not have the personnel, expertise, or the financial resources to make such an investment.

[4] Defining Issues: SEC staff issues new C&DIs on cybersecurity rules.

3.2 Understand the overall IT environment

Guidance: ICFR Handbook, Question 3.2.70 | Are IT systems included in management's risk assessment? and Question 4.6.20 | Why is understanding the overall IT environment important?

Understanding the overall IT environment is a key part of your risk assessment, because IT systems are pervasive to overall ICFR and changes to IT systems are examples of entity-wide events that could have related financial reporting risk. For example, in the context of Intelligent Tools, think about:

- the level of business and IT involvement throughout the implementation of Intelligent Tool(s);
- the key performance indicators or key risk indicators used to monitor and assess ongoing operation of the use of Intelligent Tools;
- the appropriateness of the risk assessment activities designed to identify PRPs or RAFITs introduced or altered by the implementation of Intelligent Tools;
- the operational plan and implementation protocols to understand how related PRPs and RAFITs are identified and mitigated; and
- whether the entity's governance and oversight of the process for implementing and monitoring Intelligent Tools is commensurate with the complexity or maturity of the Intelligent Tools and the extent to which the entity relies on them to support its financial reporting.

How can you obtain an understanding of how and where Intelligent Tools are used?

- Conduct a meeting with individuals or departments that impact the financial reporting processes or other key stakeholders to:
  - Identify the use of Intelligent Tools while understanding the related business processes and the impact on ICFR.
  - Understand the overall vision, strategy, and guidelines in place to identify, prioritize and deploy Intelligent Tools.
- Understand strategic initiatives related to deployment of Intelligent Tools, such as those discussed in Board of Director meetings.
- Understand whether the entity's strategy includes plans for governance, compliance and monitoring of Intelligent Tools, including assessing the appropriateness and reliability of outputs, as well as assessing the involvement of experts.
- Discuss with HR whether there are any departments requesting new positions related to Intelligent Tools (e.g. data engineer, data scientist, prompt engineer, machine learning architect).
- Inspect IT system overview diagrams maintained by various groups within the entity that describe IT infrastructure and applications.
- Understand how other recent Intelligent Tool implementations, including steps to identify new PRPs, RAFITs, and related controls have been handled.
- Maintain awareness of evidence within program changes that suggest Intelligent Tools are being used.
- Ask those familiar with costs allocated to internally developed internal-use software, acquired internal-use software licenses, and cloud computing arrangements, whether there have been investments in AI.

What are examples of questions to ask during risk assessment, including with whom and when?

Consider having individuals or departments that impact the financial reporting processes respond to specific questions, such as those below. The purpose of these questions is to identify whether and where Intelligent Tools are used in financial reporting processes and understand what policies, processes and controls are in place or may need to be established.

General understanding	**Chief Technology Officer and/or Chief Information Officer**
• Can you provide an overview of how Intelligent Tools are used in our operations? • How would you know if Intelligent Tools were being used?	
Identification of Intelligent Tools	**Business process owners, heads of financial reporting department and IT department**
• What Intelligent Tools are used, and what type of Intelligent Tools are they (e.g. RPA, NLP, etc.)? • Which specific business processes or functions leverage Intelligent Tools? • Are you automating manual processes or using any new tools in any of your processes? If so, is the automation learning from experience and data or making predictions without process owner involvement? These may be indicators of use of AI. • Are you using or have you seen the use of any AI tools in financial reporting processes (e.g. open-source tools or libraries, AI development platforms, AI/cognitive enterprise software, AI embedded via third party services, automated machine learning tools)? • Are you currently aware of the use of AI in operational areas of the business? Even if not directly used within the financial reporting process, notifying appropriate individuals at the entity of all uses cases assists with maintaining an inventory of AI used and can help to identify areas where AI may indirectly impact financial reporting processes. • How are Intelligent Tools integrated into existing systems and workflows?	
Monitoring and controls	**Heads of internal audit department and IT department**
• How would you know if Intelligent Tools were being used? • What monitoring mechanisms are in place to track the performance of Intelligent Tools over time? • Are there automated or manual controls to identify and address anomalies or issues in Intelligent Tool driven processes?	
Impact on internal controls	**Heads of financial reporting department and internal audit department**
• How has the implementation of Intelligent Tools impacted internal controls related to financial reporting? • What are the impacts to the control environment, including the identification and assessment of new risks or changes to risks? • Who was involved to evaluate the new risks or changes to risk introduced by the implementation of Intelligent Tools? • How is the sufficiency of the design of controls considered, including general IT controls, when addressing any newly identified risks or changes to risks?	

Employee training and competence	**Heads of HR department and training and development department**
• How are employees trained to interact with Intelligent Tools and what measures are in place regarding their competence? • Is there ongoing training to keep personnel updated on changes in Intelligent Tool technologies and their implications?	
Vendor relationship	**Heads of IT department and legal department**
• If third-party Intelligent Tool solutions are used, how are these vendors assessed for reliability and security? • What contractual agreements are in place with the vendor to support the entity's control and governance over Intelligent Tools? For example, do contracts govern the established scope, data protection and other responsibilities between the vendor and the entity? • Does the vendor provide a SOC 1 or SOC 2 report?	

Cybersecurity risks

Guidance: ICFR Handbook, Question 7.6.30 | What are management's responsibilities related to cybersecurity risks?

Action: Management's cybersecurity risk assessment requires evaluating cybersecurity risks related to Intelligent Tools. This includes understanding the following:

- the actions the entity has put in place to mitigate potential cybersecurity risks specifically as a result of the use of Intelligent Tools;
- how potential cybersecurity risks resulting from use of Intelligent Tools are monitored;
- the process for reporting breaches to those charged with governance;
- whether any breaches directly related to the use of Intelligent Tools have occurred and what the entity did to respond; and
- for SEC registrants, the process for disclosing material cybersecurity incidents.[5]

Management is responsible for evaluating the risk of cybersecurity incidents and cyber-related frauds across all aspects of the entity's business operations and establishing processes, structures, and safeguards to mitigate those risks. Fulfilling this responsibility means obtaining an understanding of how using Intelligent Tools has changed the entity's cybersecurity risks. It also requires understanding how the entity responds to cybersecurity risks and considers the occurrence of cybersecurity incident(s), taking into consideration the nature of the entity's business, customer and vendor base, reliance on automated business processes and other relevant factors.

Cybersecurity risks and Intelligent Tools are intrinsically linked. Cybersecurity risks encompass multiple aspects of an entity's operations, including the potential for fraud, changes impacting ICFR, and the overall integrity of data used in Intelligent Tools.

Gain an understanding of how Intelligent Tools are interacting with systems outside the entity's environment to identify potential cybersecurity risks. If the Intelligent Tools have access to the internet, security risks could arise from bad actors, misinformation, or adverse events. For example, bad actors could obtain inappropriate access to change the underlying algorithms or could alter either training data or data that the tool uses to continue its learning (also referred to as 'data poisoning'). These actions can trick an AI model into producing unreliable information.

If AI is relying on prompts, such as those used for Gen AI models, there could be malicious actions by individuals outside of the entity to obtain access and direct the prompts to produce unreliable information. Examples include direct malicious prompts generated to spread misinformation, indirect malicious prompts crafted to exploit vulnerabilities or bias in the model, and malicious override of prompts using vulnerabilities in the system to alter the system's behavior.

Moreover, the use of AI could increase the likelihood of breaches that may compromise sensitive customer, employee, or entity data. Data breaches can also expose cybersecurity risks to other systems and data and result in financial loss, reputational damage, or disruption of services.

The cybersecurity risk assessment process includes understanding how the entity has taken steps to safeguard the data it uses. In response to these cybersecurity risks, consider the need for a multi-layered approach to cybersecurity, incorporating not only firewalls but antivirus software, intrusion detection/prevention systems, regular software updates, user education, and other security best practices.

[5] Defining Issues: SEC staff issues new C&DIs on cybersecurity rules.

3.3 Fraud risk factors

Guidance: ICFR Handbook, Question 2.5.140 | What are fraud risk factors? and Question 3.6.20 | How is the fraud risk assessment performed?

The COSO Framework requires consideration of the potential for fraud in assessing risks to the achievement of the entity's objectives.

Are fraud risk factors impacted when an entity uses AI?

Action: Think about the opportunities that may be created using Intelligent Tools when identifying fraud risks.

AI may result in opportunities to commit fraud more easily and without it being detected. For example, Intelligent Tools can impact the potential for employees to engage in fraudulent activities or hide fraudulent activities, or for external parties to deceive the entity. Identifying these opportunities to commit fraud is an important element of identifying fraud risk factors. In addition to some of the cybersecurity risks discussed above, some examples of how AI has been used to perpetrate fraud include the following:

- Using deepfake video or voice technology to impersonate management in or to deceive entity personnel and obtain transferred funds through fraudulent means.
- Exploiting vulnerabilities in AI algorithms to trick it into making incorrect decisions or manipulating its behaviour (e.g. incorporation of deliberate bias into the model). For example, by injecting deceptive transactions or altering transaction attributes, such as amounts or descriptions, users can mislead the model into misclassifying legitimate transactions as fraudulent or vice versa.
- Falsifying documents, transactions, or accounting records.

4 Process understanding and process control activities

4.1 Process understanding

Guidance: ICFR Handbook, 4. Process Understanding and Question 4.3.10 | Is management required to gain an understanding of business processes?

An aspect of Principle 7 of the COSO Framework requires understanding the business process activities and the flow of data from initiation to reporting. Obtaining an understanding of business and financial reporting processes provides the basis for identifying and assessing PRPs.

How does the entity use Intelligent Tools as part of its financial reporting?

While some entities may choose to automate parts of certain processes using Intelligent Tools, including control activities to mitigate risks, other entities may automate entire processes whereby the PRPs arising in the process are fully addressed by automated controls embedded into the technology used in the process.

Think about whether there are interdependencies between the Intelligent Tool and other IT systems and whether individuals at the entity are appropriately involved in the process from initiation of a transaction to its recording in the general ledger.

During the process of integrating Intelligent Tools into business and financial reporting processes, identify PRPs throughout the planned revised process. Note that some PRPs may be addressed by automated controls that are part of the implemented technology while others may continue to be addressed by manual control activities. For automated controls, identify the RAFITs and the applicable GITCs addressing those RAFITs.

Does process understanding differ for AI?

In many cases, Intelligent Tools perform the same tasks as humans, and understanding how AI replaces the human element in a process or control may help identify whether:

- there are new PRPs (or changes to existing PRPs) or new RAFITs; and
- how to frame a response to the identified PRPs/RAFITs.

Some of the PRPs or RAFITs that are introduced when using AI relate to a lack of understanding and expertise of sophisticated models, relying on IT systems that are a 'black box', bias concerns, and data quality and integrity issues. Therefore, as entities use AI, managing PRPs and RAFITs through process control activities and GITCs, where applicable, becomes increasingly important and having a robust control environment becomes even more critical.

Understanding the level of human involvement is a key consideration for AI. When a human is involved in reviewing or reperforming the output from AI before it progresses through the process, the entity is placing reliance on the manual control activity. This is comparable to a control where a manager reviews a preparer's documentation. The focus remains on the human element of the review, where the manager thoroughly examines and validates the output, regardless of whether it was generated by a human or AI.

As AI becomes more sophisticated, entities may determine that incorporating human involvement earlier in the process is necessary to mitigate the risks.

What does 'human in the loop' mean?

'Human in the loop' refers to a concept in AI solutions where human involvement is incorporated at one or more stages of the process. It means that humans are actively participating and providing input or oversight to the AI solution's operations with the goal to find a balance between the automation capabilities of AI solutions and the need for human oversight.

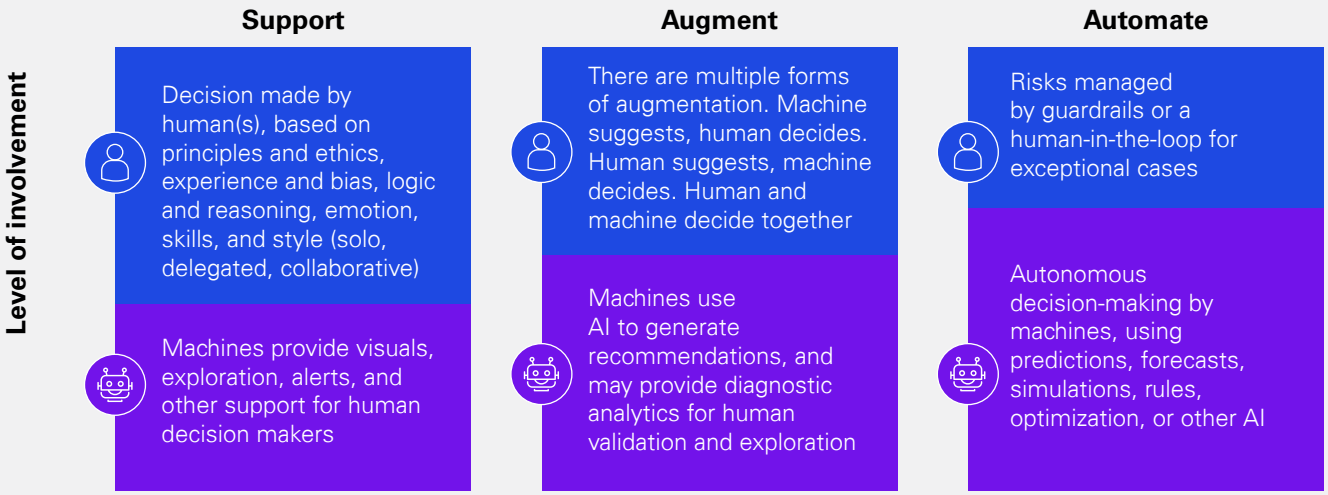
The purpose of including humans in the process is to validate reliability, including accuracy, and ethical considerations in AI solutions. By involving humans, potential errors or biases in the AI algorithms can be identified and corrected. It also allows for human judgment and expertise to be incorporated into decision-making processes where AI may fall short.

For example, the AI solution may perform automated tasks or processes, but human intervention continues to be required for certain critical or complex decisions. This involvement can take various forms, such as reviewing and labeling data, validating outputs, making judgments, or providing feedback to improve the solution's performance. There are also varying levels of human intervention as illustrated in the below table. Management's risk assessment is informed by the level of human involvement.

Artificial intelligence for decision-making

Artificial intelligence enhances our decision intelligence, drastically improving, or even automating, the way we make decisions.

Human Machine



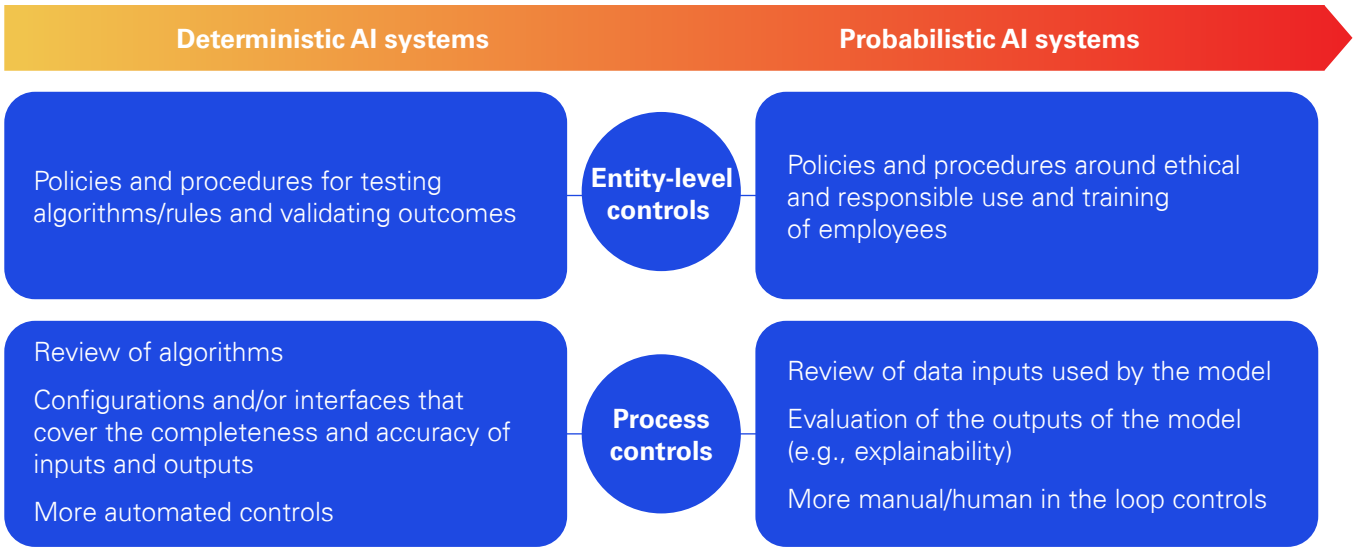
Source: Gartner

How do processes and controls differ when considering the AI spectrum?

Deterministic AI systems operate based on fixed rules and algorithms, leading to predictable and consistent outputs. Processes and controls for these systems may involve understanding how algorithms and rules are established, how implementation is tested, and the types of controls necessary to cover the completeness and accuracy of the outputs. An entity may use more automated process control activities for deterministic AI systems (e.g. configuration-type controls built into the tools) as their output may produce repeatable results.

In contrast, probabilistic AI systems make predictions or decisions based on probabilities and statistical models, resulting in uncertain outputs. As a result, a higher level of human involvement is often necessary to manage and control these systems and an entity may use more manual process control activities by nature as it takes more human intervention to review the outputs.

The processes around governing the use of AI are an important aspect for any solution; however, the focus may differ slightly depending on where the AI fits on the spectrum. Governing the use of deterministic AI systems may focus more on policies and procedures regarding the testing, validating, and monitoring of algorithms and rules used by the AI systems. With probabilistic AI systems, there may be more of a focus on having policies and procedures in place around the responsible use of the solution and training people on its use.



Why is it important to understand the type of Intelligent Tool incorporated into the process?

In some cases, the risks between Automation and AI are different and additional considerations, including involving those with subject matter expertise, may be necessary when evaluating the impact on the entity's internal controls. The following examples highlight how the control landscape may differ when a portion of the process and control activities performed by a human control operator is replaced by an Intelligent Tool. In the following table each example illustrates the process and/or control without, and then with, the use of an Intelligent Tool.

Relevant controls with human operator	How controls may change with Intelligent Tools
Data analytics example—When an entity enters into a rebate agreement, it houses the agreements in a controlled SharePoint repository. When a sale occurs, an employee calculates the rebate, and the rebate payable is entered into the entity's ERP system.	
• On a monthly basis, a staff accountant **performs a matching that compares the rebate amount per the agreement to the amount entered in the ERP system and calculates any differences outside the established thresholds.** For differences identified, the staff accountant researches and resolves the differences. • A control is performed by the accounting manager to review that (i) the staff accountant calculated any differences correctly and (ii) the resolutions for exceptions that have been identified for follow-up (those outside the established thresholds) have been appropriate.	• Alteryx replaces the steps in **bold**. • A control(s) is in place related to the tool's ability to appropriately identify differences and items for follow-up. • A manual control continues to be performed by the staff accountant to research and resolve differences and by the accounting manager to review the resolution for exceptions that have been identified for follow-up (those outside the established thresholds).

Relevant controls with human operator	How controls may change with Intelligent Tools
RPA bots example—Daily feeds from the bank are recorded into the entity's ERP system.	
• A bot initiates a bank reconciliation, which is completed by a staff accountant. The bot extracts bank statement information from the bank website, enters the bank statement information into Excel and reads the ending balance. The bot then extracts the book balance from the general ledger and the outstanding checks from the treasury system, compares the balance to the bank balance, and calculates a difference. **The staff accountant then completes the reconciliation by validating that the balances agree to supporting documentation** and investigates the difference. In this case, the bot replaced certain manual tasks performed as part of the reconciliation; however, the staff accountant (control operator) manually reperformed the bot's activities and investigated the differences identified by the bot. • A control is performed by the cash manager to review the cash reconciliations prepared by the staff accountant and resolution/support for the differences outside the predetermined threshold.	• A bot replaces the step in **bold**. If the account can be reconciled within a predetermined threshold by the bot, no further review is completed by a staff accountant. If the cash account cannot be reconciled within a predetermined threshold, the bot is configured to route the reconciliation to a staff accountant for review, including investigating the difference. In this case, the bot is the control operator for all attributes of the reconciliation control and replaces a manual control in its entirety when the account can be reconciled within the predetermined threshold. As a result, the following controls are in place: • an automated configuration control* over the cash reconciliations within the predetermined threshold; • a control performed by the cash manager to review the cash reconciliations outside the predetermined threshold, including resolution/ support for the differences. *Additional considerations include identifying any RAFITs and GITCs that support the automated control and risk considerations addressed through entity-level controls as discussed in section 2.
Machine learning example—The entity has a process in place to review royalty statements to approve for payment annually.	
• A staff accountant performs a **matching of internal and external documents to calculate a variance and identify outliers outside the set range. A staff accountant goes through the outliers to determine which ones need further investigation. Some outliers may be explained by known seasonality, launch events or geography. In those examples the explanation for the outliers is known and no further investigation is needed**. The remaining outliers that fall outside the acceptable range are then investigated further before they can be paid. • A control is performed by the accounting manager to review that the staff accountant calculated any variances correctly and review of how the staff accountant resolved outliers that have been identified for follow-up.	Machine learning tool replaces the steps in **bold** by learning, through a combination of historical data and a reinforcement learning (i.e. a thumbs up or thumbs down) approach, how to flag a true variance that needs to be investigated (not one caused by seasonality, launch events, geography). As a result, the following controls are in place: • An automated control(s)* related to the tool's ability to appropriately match documents, calculate outliers, and to identify which outliers need follow-up is in place. • A control performed by the accounting manager to review how the staff accountant resolved exceptions that have been identified for follow-up continues to be in place. * Additional considerations include identifying any RAFITs and GITCs that support the automated control and risk considerations addressed through entity-level controls as discussed in section 2.

Relevant controls with human operator	How controls may change with Intelligent Tools
Gen AI example—An entity includes required property, plant, and equipment (PP&E) disclosures in its annual financial statements.	
• A staff accountant involved in the entity's financial reporting process **prepares the draft disclosure based on underlying supporting schedules and general ledger data.** • A control is performed by the accounting manager to review the draft PP&E disclosure to validate that the disclosure agrees to the underlying schedules and includes all information required by the applicable financial reporting framework.	• Gen AI* replaces the steps in **bold** and a staff accountant independently reviews and verifies the disclosure drafted before it is provided to the accounting manager for review. • The existing control does not change. *Additional risk considerations may need to be addressed through testing entity-level controls as discussed in section 2 and GITCs related to the implementation of AI as discussed in section 5.

4.2 Process control activities

Guidance: ICFR Handbook, 5. Process control activities

Control activities are the actions established through policies and procedures that drive management's directives to mitigate risks to the achievement of objectives. Below are some example controls that may be specific to or more applicable when an entity uses Intelligent Tools within its business and financial reporting processes. As with any control, the frequency of the control's operation will depend on the control objective (i.e. controls over the use of the tool may occur each time the control is performed or only when the tool is implemented or changes are identified).

What are example control activities for data analytic tools?

For some automation tools, like data analytic tools, their implementation may not be aimed at a comprehensive adoption throughout the entire entity and may be used solely for the purpose of automating specific process control activities. In these cases, they may function similarly to a control operator using an end-user computing application. For this reason, there may be less emphasis on entity-level controls that address risks over the development/acquisition, deployment and operation of data analytic tools. Instead, the risks may be addressed through control activities at the process level that address the design and implementation of the tool.

What are EUC applications?

EUC (End-user computing) applications are IT systems that end users, rather than computer programmers, use to create working applications. Entities often use end-user computing applications as part of financial reporting and business processes. Evidence for control purposes may be maintained in the form of an end-user computing schedule (e.g. spreadsheet software or simple databases).

Example control considerations for data analytics tools

- An accounting manager reviews the design of the routine. This includes determining that the Intelligent Tool being used is appropriate and reliable for the intended purpose and that the individual who designed the routine is competent to design, develop and execute it.
- An accounting manager reviews the macros and algorithms developed using the Intelligent Tool or use of existing functionality, logic, or formulas within the Intelligent Tool.
- The routine is housed in a controlled site or password protected to prevent unauthorized changes.
- A staff accountant evaluates the design of the routine each time it is used to demonstrate that the design has not been altered and to evaluate whether changes in data or other requirements do not impact the design of the routine.
- An accounting manager reviews the execution of the routine each time it is used by reviewing screen shots or be re-performing the steps performed by the staff accountant.

What are example control activities for RPA bots?

Example control considerations for RPA bots

- The design of the RPA bot, including the predefined rules the RPA bot is executing against and the process or control it is replacing, is reviewed to determine it is appropriate for the intended purpose.
- Manual or automated process control activities check that the logic is functioning as intended (e.g. configurations, interfaces, formulas).
- Reports on the RPA bot's performance are reviewed to determine if changes to the design are necessary.

What are example control activities for AI?

Process control activities play a crucial role in mitigating certain risks introduced by AI. As AI becomes more sophisticated, implementing more process control activities that focus on monitoring AI in use may be necessary.

As discussed above, the need for human oversight and involvement in controls for AI is an important consideration. For example, when an AI tool is used to forecast revenue projections, understanding what data sets were used to build previous revenue projections (e.g. historical sales, customer reports from the last 12 months, seasonality information) is critical. Because IT personnel alone would not have this business knowledge, it may be necessary to involve the business process owner who has this knowledge when developing and monitoring this AI tool.

As discussed in section 3, specific factors to focus on when developing controls over AI may depend on the type of AI implemented and the entity's framework for compliance. The example controls provided below highlight important considerations when monitoring the use of AI, and are grouped by factors often found in AI management frameworks of external groups (NIST, ISO, etc.), including KPMG's own trusted AI approach. These example control considerations are supported by a suite of GITCs discussed in section 5.

Factors	Example control considerations
Explainability or access to underlying algorithms/rules: Explainability refers to the entity's ability to understand how and why a conclusion was made by AI. When entities lack an understanding of why an algorithm generated a particular output, it can impede their ability to identify errors.	The ability of the entity to implement the following example process control activities may vary depending on whether the entity has access to the underlying algorithms. • The inputs that the model relies on to execute a task or decision are documented and reviewed by a manager. • The documentation maintained on how the model functions and makes its decisions is reviewed and re-evaluated quarterly. • Reports from model interpretability techniques (methods to gain insights into how the model makes decisions) or user feedback analysis are reviewed to evaluate the ongoing explainability of the model.
Reliability of the model: Reliability of the model refers to the ability of AI to consistently operate with its intended purpose upon implementation and overtime. Note: Reliability of the information used by the Intelligent Tool as part of the process is covered in section 4.3	The ability of the entity to implement the following example process control activities may vary depending on whether the AI employs static models or models that could potentially change over time and impact the entity's use. • Errors or discrepancies generated by the AI are logged and reviewed by a manager for further investigation and resolution and to determine if updates to the model are necessary. • The decisions underlying the design of the model are reviewed to determine if there are changes to the entity or its business that impact the design or functionality. • For third-party models that are developed outside the entity, the manager evaluates the technology is operating effectively for its intended purpose. The accounting manager reviews statements released by third parties that explain any updates to the model or algorithms, if applicable.
Data quality of the inputs into the model: Data quality refers to the accuracy, completeness, appropriateness, and quality of the data used to train and operate the Intelligent Tool. For example, large or more complex data sets could result in poor quality data used, which could result in erroneous or poor predictions or a failure to achieve the intended objective.	The ability of the entity to implement the following example process control activities may vary depending on whether the AI model is trained using prescriptive methods to determine the appropriate input to achieve a certain output or a model trained from large or more complex data sets. • The training data input into the model is reviewed by a manager to determine whether the data is relevant and reliable, and used for its intended purpose. • The training data input into the model is reviewed by a manager to determine it excludes bias per the entity's policies and meets regulatory requirements. • For third-party models, the manager evaluates the model the Intelligent Tool relies on and the data the model was trained on.
Prompts for Gen AI models	• New and changes to existing prompts are reviewed and approved. • Prompts are reviewed to determine their appropriateness. • Prompts are evaluated periodically to assess that the prompts remain sufficient and appropriate for the intended purpose and the results generated by the tool when using the prompt are appropriate. Changes to prompts are reviewed.

4.3 Information

Management is responsible for evaluating the reliability of information used in a control regardless of whether the information is obtained through AI or by conventional methods. Understanding the flow of information and data elements through the process that involves an Intelligent Tool is important to understanding how the reliability of that information has been assessed.

Reminders from the ICFR Handbook	
Internal information	**External information**
Management's evaluation of the reliability as it relates to internal information is whether it is complete and accurate.	Management's evaluation of the reliability of external information considers the information's nature and source.
Management's evaluation of the reliability of internal or external information maintained in the entity's IT systems involves understanding the flow of information and how the data risks associated with the information's completeness and accuracy are addressed.	

What data risks are present for information used by or processed through Intelligent Tools?

Guidance: ICFR Handbook, Question 6.4.50 | What are the data risks?

The following data risks apply to information used by or processed through Intelligent Tools:

Data risk	Additional risk considerations and examples specific to Intelligent Tools
Input	Does the Intelligent Tool need a certain format of information to successfully execute? For example: • Does the entity use standardized prompt libraries to enable relevant and reliable (i.e. complete and accurate) data to be entered?
Integrity	Is the entity using an Intelligent Tool that is an open-sourced model where data could be inappropriately altered during processing? For example: • Malicious attacks on prompts can occur when someone outside the entity intercepts a prompt and exploits vulnerabilities or bias in the model.
Extraction	Are there controls to address that the information extracted from the Intelligent Tool is complete and accurate? For example: • RPA Bots may produce output reports for a control owner to review, including possible exceptions and outliers. Does the entity have an automated process control activity over the configuration of the report or a manual process control activity over the RPA Bot to produce complete and accurate information? • If there are parameters or other set criteria entered into the Intelligent Tool (e.g. macros in Excel, Alteryx or PowerBI) to extract the correct information, are the parameters reviewed as part of the control? • If a Gen AI tool is used to provide information, are there manual process control activities to validate that the information produced is relevant and reliable?
Manipulation	How are changes to the information extracted from the Intelligent Tool controlled (e.g. controls to prevent changes to the information after it has been extracted) or reviewed for intentional changes (e.g. controls to check formulas, formatting, etc.)? For example: • Some entities use Data Analytics tools (e.g. macros in Excel, Alteryx or PowerBI) to further manipulate data into its intended format or data could unintentionally be manipulated during that process. • In some AI, a human may be involved in manipulating the output data to reprocess and run back through the model (e.g. further information necessary for final output or for purposes of training the model).

Is the information provided by a service organization?

Guidance: ICFR Handbook, 8. Service organizations

Using a service organization may provide access to specialized skills needed for using Intelligent Tools. However, using service organizations may result in unique risks because the entity does not control all aspects of the Intelligent Tool but retains responsibility for its ICFR. Assess the unique facts and circumstances of such arrangements to determine how they impact the overall risk assessment..

Service organizations that deploy AI may introduce risks related to data integrity, data privacy and explainability, among others.

These risks and controls in place at a service organization that respond to the risks may be documented in SOC 1® or SOC 2® reports.

How do the considerations over Intelligent Tools differ from those over EUC applications?

When the output from an Intelligent Tool is controlled by an end-user, there are similar considerations to think about such as end-user computing. Intelligent Tools may produce additional risks to consider if the final output is not subject to the same level of rigor and structure as applications processed in a more centrally controlled environment. Some automation tools, such as tools used by end-users to develop automated routines (e.g. Microsoft Excel, Alteryx, PowerBI) may have increased data integrity and manipulation risks given the output from these applications are typically stored on individual employee machines where it is editable. Think about these considerations when identifying PRPs and controls related to end-user computing.

5 General IT controls for Intelligent Tools

5.1 IT layers

Guidance: ICFR Handbook, Question 7.2.10 | "What are the layers of technology that comprise an IT system?"

Identifying the IT layer at which Intelligent Tools operate and/or where the data and information used by the Intelligent Tools exists is important because each layer may present unique risks.

For automation, often the application, database and/or operating system layers are relevant. For AI, the network layer may also be relevant. Determining whether the network layer is relevant involves thinking about the specific characteristics and deployment of the Intelligent Tools. The following scenarios are examples where the network layer may be relevant.

- Intelligent Tools communicating with external IT systems, which may involve data transmissions and retrieving information from APIs or databases.
- Intelligent Tools deployed as part of distributed systems or cloud infrastructure for solutions using cloud-based services like AI as a service (AIaaS), where the network layer is vital in addressing security risks for communication between the entity's IT systems and cloud-based AI services.
- Intelligent Tools receiving updates or patches over the network, where the network layer may be relevant to assessing the controls over these updates to support the integrity and security of Intelligent Tools.
- Intelligent Tools relying on network-based authentication and authorization mechanisms.

Determining whether the network layer is relevant to an Intelligent Tool is based on the specific characteristics of the tool, internal or external data exchanges, and security considerations associated with the network infrastructure supporting the Intelligent Tool environment.

Assessing the security configurations of network devices, firewalls and other network components may become important to protect Intelligent Tools against unauthorized access and potential cyber threats.

5.2 General IT controls

Action: Identify GITCs that address the risks arising from IT (RAFITs) when using Intelligent Tools for all relevant IT layers.

Risk and controls considerations related to Intelligent Tools

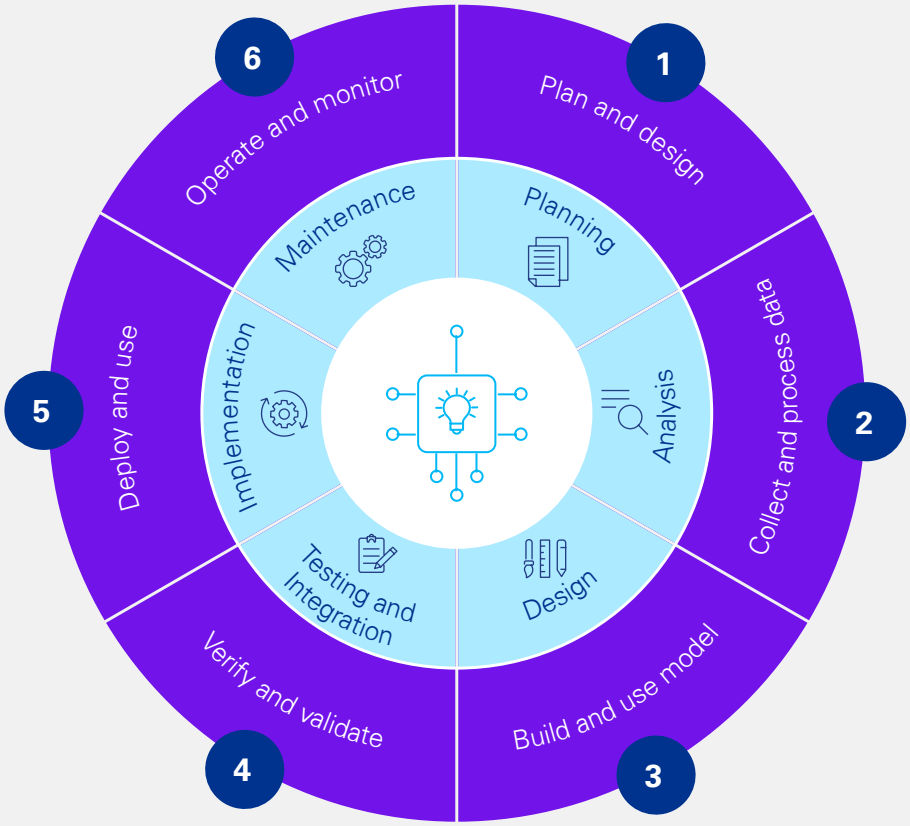
Guidance: ICFR Handbook, Question 7.2.40 | "What are the risks arising from IT and how are they identified?"

As with traditional applications, identifying relevant RAFITs that could prevent the effective operation of the automated controls performed by Intelligent Tools and/or could affect the integrity of data used by Intelligent tools is necessary to determine the required GITCs. RAFITs that are relevant to the traditional applications are often also relevant when relying on Intelligent Tools and/or information. However, the use of AI may introduce specific risks outside of the traditional RAFITs. Accordingly, the sections below describe the traditional RAFITs that will likely be relevant and identify specific risks that may be introduced with the entity's use of AI across four GITC areas.

5.2.1 Program acquisition and development

Intelligent Tool implementations, like other traditional IT implementations, are expected to follow a SDLC, customized as necessary to respond to program development risks that may be unique to the Intelligent Tool. Understanding the similarities and differences between an entity's Intelligent Tool implementation process and its traditional IT implementation process may inform risk assessment. The following exhibit represents the traditional SDLC in blue and an example AI SDLC in purple to demonstrate these similarities and differences.

The example AI SDLC contains specific features that place more emphasis on data collection and preparation, model training and testing, and monitoring to allow the AI model to evolve over time.



Action: Think about the following RAFITs relevant to automated control activities configured within Intelligent Tools.

As with any new IT system acquisition and development, thinking about the following RAFITs related to acquiring and developing Intelligent Tools is important.

RAFIT	Example GITCs
IT system developments (new components or significant changes) are unapproved or do not function as intended.	Intelligent Tool acquisitions/developments are tested and approved prior to implementation into the production environment.
Incomplete, redundant, obsolete, or inaccurate data is migrated to the production environment of acquired, newly developed, or existing IT systems.	Conversion/migration of data from the legacy IT system to the newly acquired or developed Intelligent Tool are approved as complete and accurate.

Are there additional risks related to Intelligent Tools to think about for program acquisition and development?

Action: Think about the following specific risks that may be introduced by using AI and the example control considerations and inquiries that may be used to identify the GITCs that address these risks.

Additional risks may be relevant in the development or acquisition of AI within the framework of the regular SDLC. The following table provides example risks, control considerations and inquiries that may be used to identify the GITCs that address these risks.

SDLC step	Example risk	Example control considerations	Example inquiries
Build and use model	**Lack of explainability within the algorithm**: Complex AI models, such as deep neural networks, may lack interpretability, making it challenging to understand how the model arrives at specific predictions.	Using interpretable models and explainability techniques, and providing documentation on model decision-making processes.	• How are underlying algorithms, particularly those using deep learning algorithms, understood? • Are there specific tools, techniques or methodologies employed to enhance the explainability of the algorithms? • How does the entity document how the model works and communicate the explainability of AI to relevant stakeholders?
	Algorithmic Reliability: AI may make inappropriate decisions, based on biases and/or incorrect algorithms and training data.	Conducting algorithm training, assessing bias in model predictions, and adjusting models to reduce disparities.	• How are potential biases or inappropriate decisions in AI identified and mitigated? • Is there a documented process for evaluating and addressing bias concerns during the design phase? • What are examples of measures taken to support that AI algorithms are impartial? • What are the protocols for validating the accuracy and completeness, and relevance of the information used in AI (e.g. evaluation for bias, integrity, manipulation and extraction risks)? • How is access to the training and testing data managed, including situations when using an open-source AI?

SDLC step	Example risk	Example control considerations	Example inquiries
Verify and validate	**Data quality and bias:** Inaccurate, incomplete, or biased training and/or testing data can lead to biased and/or inappropriate predictions.	Separating training and testing data to avoid overlearning challenges that arise when AI's decision-making process is influenced by training data alone. Restricting access to training and testing data to authorized personnel. Rigorous data pre-processing, thorough data quality checks, and efforts to identify and address bias in the training and testing data	• What training data and testing data were used? • What is the period covered by the training and testing data (including relevant scenarios)? • How is training and testing data separated to avoid the risk of overlearning? • What steps are taken to support the quality and representativeness of training data and testing data, and how is bias identified and addressed? • What are the protocols for validating the accuracy, completeness and relevance of the training and testing data used in AI?
	Inadequate testing: Incomplete or insufficient testing of AI may result in undiscovered issues or unexpected behaviours.	Comprehensive testing, including unit testing, integration testing, and validation against diverse datasets, to uncover potential issues.	• What test procedures were implemented to provide for comprehensive coverage of the models' functionalities and potential use cases? • Was sufficient testing performed to determine that the AI algorithm is working as intended? • Are there specific criteria or standards against which the adequacy of testing is measured, and how are testing outcomes documented and reviewed?

5.2.2 Program change

Action: Think about the following RAFITs relevant to automated control activities configured within Intelligent Tools.

As with program changes for any IT system, thinking about the following RAFITs related to program changes for Intelligent Tools is important.

RAFIT	Example GITCs
Changes to IT programs/configurations were inappropriate (i.e. unapproved or do not function as intended).	Changes to Intelligent Tools programs/configurations undergo testing and approval by business and/or IT stakeholders before integration into the production environment.
Logical access to implement changes to IT system program or configurations into the production environment is inappropriate (i.e. unauthorized, or not commensurate with job responsibilities).	Access to implement changes to Intelligent Tools programs/configurations into the production environment for the relevant Intelligent Tool is configured to restrict access to appropriate individuals and segregated from the development function.

Are there additional risks related to Intelligent Tools to think about for program changes?

Action: Think about the following specific risks that may be introduced by using AI and the example control considerations and inquiries that may be used to identify the GITCs that address these risks.

Additional risks may be relevant related to program change of AI. The following table provides example risks, control considerations and inquiries that may be used to identify the GITCs that address these risks.

Example risk	Example control considerations	Example inquiries
Model drift and performance issues: Over time, AI may experience drift in performance or accuracy due to changes in data patterns. Failure to address this can impact the effectiveness of AI.	Implement monitoring mechanisms to detect model drift and continuously assess performance against predefined metrics.	• What procedures are in place to monitor the performance of AI over time? • How frequently is AI assessed for any signs of performance degradation or drift? • How are these assessments used to validate the effectiveness of the retraining processes? • Are there established benchmarks or performance thresholds that trigger a review and updates if model performance deviates? • How does the entity determine acceptable performance thresholds, and are these aligned with business objectives? • How has model drift been addressed in the past? • Is there a process to refresh or retrain AI to adapt to evolving data patterns? • How are training data managed and updated when updates are made to AI? • What protocols are in place for retraining AI after updates are made to the system? • How is the process of updating and retraining AI models integrated into the broader change management framework?
Training data updates: If AI is not retrained with updated and relevant data, then its performance and accuracy may suffer over time, impacting the system's effectiveness.	Establish a proactive and continuous retraining schedule for AI to remain adaptive to evolving data patterns, maintaining optimal performance and accuracy.	

5.2.3 Access to programs and data

Action: Think about the following RAFITs relevant to automated control activities configured within Intelligent Tools.

As with access to any IT system and its data, thinking about the following RAFITs related to access to programs and data for Intelligent Tools is important.

RAFIT	Example GITCs
Identification and authentication mechanisms are not implemented to restrict logical access to IT systems and data	Access is authenticated using passwords as a mechanism for validating that users are authorized to gain access to the Intelligent Tool.
Logical access permissions are granted (new or modified) to users and accounts (including shared or generic accounts) that are inappropriate (i.e. unauthorized, or not commensurate with job responsibilities).	Management approves the nature and extent of user access permissions for new and modified user access in Intelligent Tools.

RAFIT	Example GITCs
Logical access permissions are not revoked in a timely manner.	Access for terminated/resigned users is removed timely from Intelligent Tools.
Logical access to users and accounts (including shared or generic accounts) that can perform privileged tasks and functions within IT systems is inappropriate (i.e. unauthorized, or not commensurate with job responsibilities).	Privileged access (i.e. configuration, data and security administrators, those with ability to override decisions made by the Intelligent Tools) is configured to restrict access to IT personnel commensurate with job responsibilities. Privileged activity (e.g. human override of the Intelligent Tool's decisions) is monitored and reviewed to determine whether actions performed are in accordance with policy.

Are there additional risks to think about for access to programs and data?

Action: Think about the following specific risks that may be introduced by using AI and the example control considerations and inquiries that may be used to identify the GITCs that address these risks.

Additional risks may be relevant related to access to programs and data when using AI. The following table provides example risks, control considerations and inquiries that may be used to identify the GITCs that address these risks:

Example risk	Example control considerations	Example inquiries
Unauthorized access to the entity's data: the entity may use AI that is accessible by other entities, including the AI provider. This may result in the entity's sensitive data being exposed to other entities.	Use reputable AI providers, establish contractual agreements with the AI providers to support the entity's access control mechanisms, understand what access controls are in place at the AI provider and whether SOC1/ SOC2 reports are available to support their effectiveness.	• What access control mechanisms are in place for AI systems that are hosted outside of the entity's environment? • What contractual agreements with AI providers are in place related to access control mechanisms and how roles and responsibilities are divided between the entity and the AI provider? • Are SOC1/SOC2 reports available? Are they Type 1 or Type 2 reports? • Do they address the risk of unauthorised access to the entity's data?

Example risk	Example control considerations	Example inquiries
Unauthorized access: AI may have access to programs and data beyond their intended use, leading to unauthorized access and potential misuse. *(Risk relevant when AI is the Control Operator)*	Implement access controls and least privilege principles, and regularly review and update permissions across relevant technology layers for Intelligent Tools to have only the necessary access.	• What access control mechanisms are in place for AI systems aimed to determine whether they only have access to programs and data within their intended scope? • How are least privilege principles implemented to restrict access and prevent AI from having unnecessary privileges? • In the context of AI as the Control Operator, how is the risk of unauthorized access and potential misuse monitored and mitigated?
Human-in-the-loop challenges: The involvement of humans in the decision-making process may result in inconsistent, biased, or corrupt AI output.	Establish clear guidelines for human involvement, implement standardized data input protocols, and provide training to support consistent and accurate data input.	• What guidelines or protocols exist to manage the involvement of humans in the decision-making loop when interacting with AI? • How are standardized data input protocols implemented to minimize inconsistencies, biases or errors introduced by human involvement in the AI decision-making process? • What training programs or initiatives are in place to support individuals involved in the decision-making loop in providing consistent and accurate data input to AI? • Are there specific controls or validation processes established to address and rectify any inconsistencies, biases or errors that may arise due to human-in-the-loop challenges?

5.2.4 Computer operations

Action: Think about the following RAFITs relevant to automated control activities configured within Intelligent Tools.

As with computer operations for any IT system, thinking about the following RAFITs related to computer operations for Intelligent Tools is important.

RAFIT	Example GITCs
System jobs, processes and/or programs do not function as intended, resulting in incomplete, inaccurate, untimely or unauthorized processing of data.	Based on a defined frequency, processing errors are monitored to determine whether failures in system jobs, processes and programs (e.g. backup jobs) are resolved.
Logical access to make changes to system jobs, processes and/or programs is unauthorized or not commensurate with job responsibilities.	Access to update system jobs, processes and programs (e.g. backup jobs) in Intelligent Tools is configured to restrict access to appropriate individuals commensurate with job responsibilities.

Are there additional risks to think about for computer operations?

Action: Think about the following specific risks that may be introduced by using AI and the example control considerations and inquiries that may be used to identify the GITCs that address these risks.

Additional risks may be relevant related to computer operations when using AI. The following table provides example risks, control considerations and inquiries that may be used to identify the GITCs that address these risks.

Example risk	Example control considerations	Example inquiries
Ineffective monitoring and alerting: Failure to establish effective monitoring and alerting mechanisms for AI may result in delayed detection of performance issues, anomalies, or security incidents.	Implement real-time monitoring, set up alerting systems, and establish clear response protocols for addressing issues promptly.	• How is the performance of AI monitored? • What procedures are in place for detecting anomalies, performance issues or security incidents in real-time? • What alerting mechanisms are in place to notify relevant personnel about potential issues with AI? • How quickly are alerts triggered and communicated to the appropriate parties once an anomaly or performance issue is detected? • Are there established KPIs or performance metrics that are regularly monitored for AI? • How are these KPIs determined, and what thresholds trigger alerts or further investigation? • How are the monitoring and alerting mechanisms for AI integrated into the broader IT operations monitoring framework?

5.3 GITCs executed by AI

AI may be developed to autonomously execute GITCs (i.e. act as control operator), thereby minimizing the need for human involvement. Through advanced algorithms, such as machine learning, AI can make informed decisions, adapt to dynamic scenarios and carry out control activities.

What are example GITCs that an Intelligent Tool may be responsible for executing?

The following is a list of example GITCs that an Intelligent Tool may be responsible for executing.

GITC area	Examples of GITCs
Program development and program change	• Coding—AI can develop source code that will be implemented into production • Testing automation—AI can execute unit tests, support comprehensive test coverage and identify potential test cases that human developers might overlook • Change request authorization—AI can determine and authorize changes, so that only authorized and properly documented changes are implemented • Quality assurance—AI can oversee the implementation process to validate changes and identify potential issues before deployment • Documentation and reporting—AI can facilitate the documentation of change management processes, supporting complete and accurate recording of essential information, such as change logs, system specifications, user manuals and impact assessments
Access to programs and data	• User access management—AI can identify segregation of duties conflicts, monitor activities performed by privileged users, including resolution of any outliers, and perform access controls (e.g. granting and revoking logical access based on users' roles and behaviour) • User authentication and identity management—AI can be used in access methods like multi-factor authentication, including facial recognition and voice authentication
Computer operations	• Job scheduling and monitoring—AI can automate the scheduling and monitoring of batch jobs to support timely execution and to detect processing errors • Processing errors—AI can monitor and resolve processing errors • Security monitoring—AI can be used to identify potential security breaches by analysing network traffic, user behaviour and system logs, helping to detect anomalies and protect sensitive data (e.g. AI can utilize machine learning models that are trained on access behaviour patterns to help detect suspicious activities over the entity's network)

For further information

AI presents an incredible opportunity in today's rapidly evolving business landscape. Check out the additional firm resources including AI in financial reporting and audit: Navigating the new era and KPMG's generative AI resource page, which includes featured AI insights, AI events, and AI webcasts and replays.

Contact us

Doug Besch
E: dbesch@kpmg.com

Samantha Demty
E: sdemty@kpmg.com

Denae Hajovsky
E: dhajovsky@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: **kpmg.com**