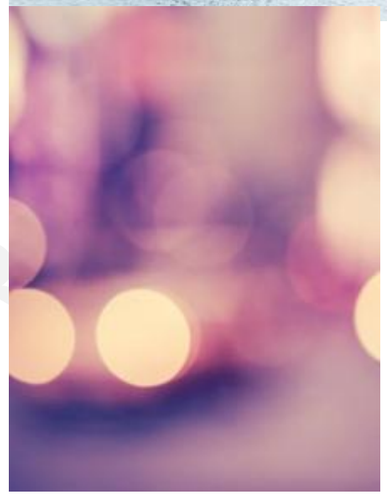
AUDITING ARTIFICIAL INTELLIGENCE

LIVE WEBINAR

EARN CPE

CPE TRAINER
cpetrainer.com



Agenda

- What is Artificial Intelligence?
- AI in Business Organizations and Regulation
- AI Models & Machine Learning
- Internal Control Framework and Business Risk
- Role of Internal Audit & Establishing Work Programmes

What is Artificial Intelligence?

How do you use AI in your daily life?

Chat GPT

Free offer ×

What do you mean by audit risk?

Audit risk is the **risk that an auditor expresses an inappropriate audit opinion when the financial statements are materially misstated.** In simple terms, it is the risk that the auditor **says the financial statements are correct when they actually contain significant errors or fraud.**

1. Simple Definition

Audit risk arises when:

- **Material misstatements exist** in financial statements, and
- **The auditor fails to detect them**, leading to an incorrect audit opinion.

Example:

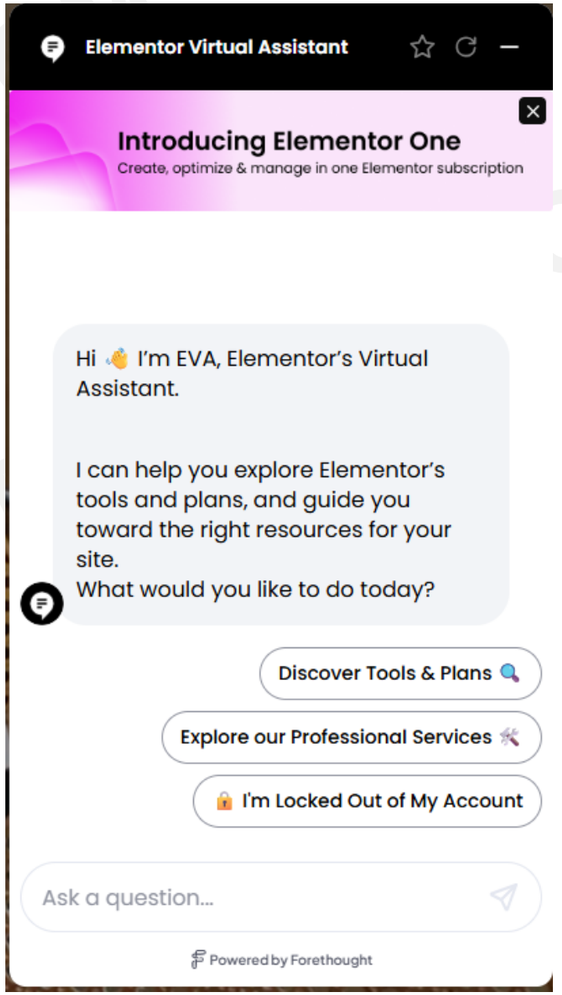
A company overstates revenue by $5 million, but the auditor does not detect it and issues an **unqualified (clean) opinion.** That situation represents **audit risk.**

---

2. Components of Audit Risk

- Risks?
- Confidentiality
- Consistency
- Accuracy
- Accuracy
- Responsibility

Service Chat Bots



Potential Use of AI in Internal Audit

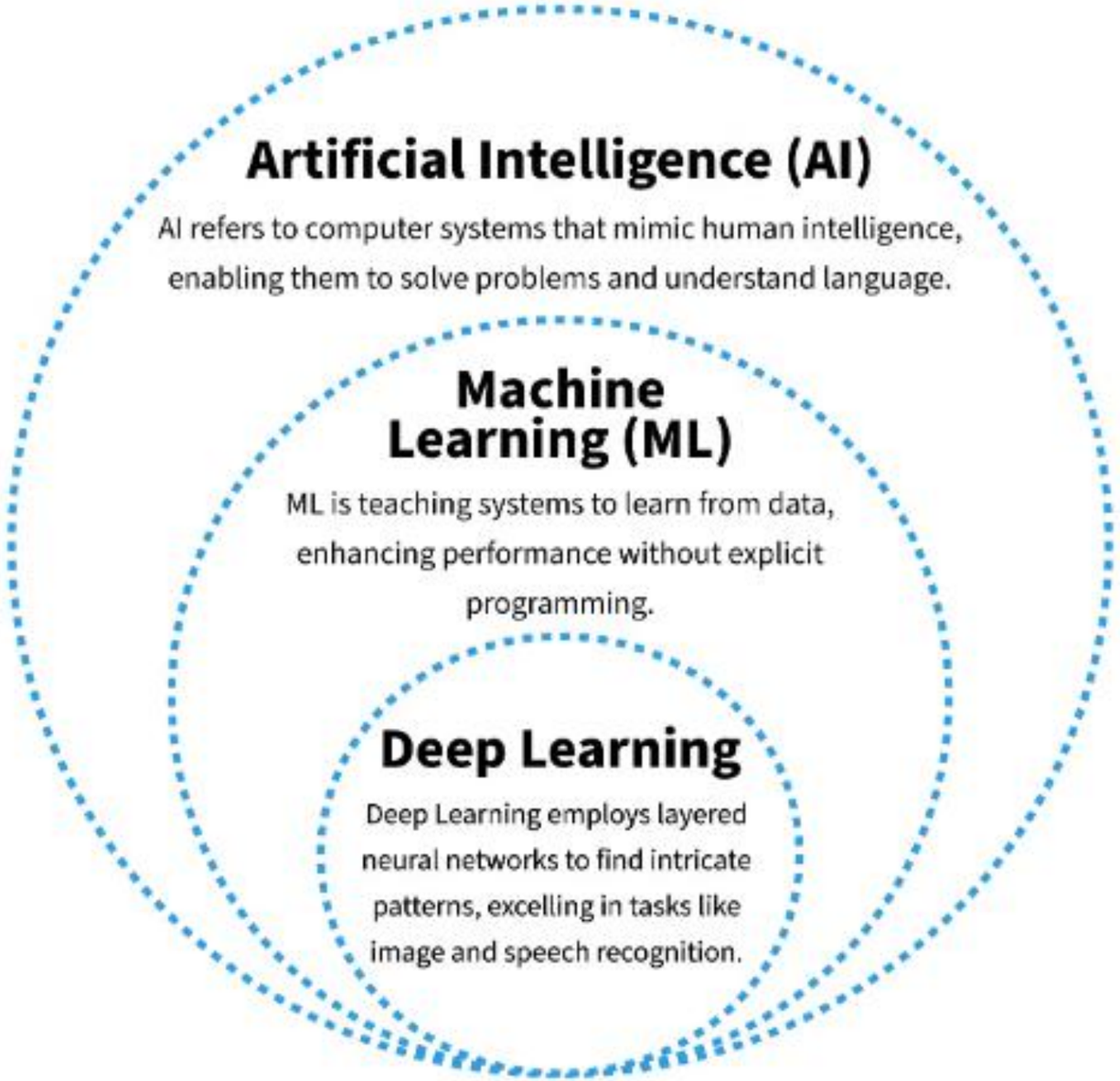
AUDIT

	Audit Process	Description
1	**Data Analytics**	• AI-powered tools efficiently process vast structured and unstructured data, identifying patterns, trends, and anomalies for further investigation.
2	**Continuous Auditing**	• Automation of data collection, verification, and analysis in real-time enhances audit quality and allows prompt issue detection.
3	**Fraud Detection**	• AI algorithms analyze transactional data to identify potential fraudulent activities, aiding auditors in focusing on high-risk areas..
4	**Natural Language Processing (NLP)**	• NLP extracts relevant information from contracts, financial statements, and textual documents, improving data analysis efficiency.
5	**Risk Assessment**	• AI analyzes historical data, industry trends, and financial ratios to guide auditors towards areas requiring closer scrutiny.
6	**Predictive Analytics**	• AI-powered models forecast financial outcomes, aiding auditors in assessing the reasonableness of projections.
7	**Anomaly Detection**	• AI identifies unusual transactions or patterns for further investigation.
8	**Document Review**	• AI automates the review of large volumes of documents, making the process faster and more accurate.

What is AI?

Artificial Intelligence (AI) refers to the branch of computer science and technology focused on **creating systems and applications capable of performing tasks that typically require human intelligence**.

These tasks include **learning, reasoning, problem-solving, understanding language, recognizing patterns, and making decisions.**



What is Artificial Intelligence?

Intelligent machine activity

Algorithms designed to reproduce human brain capabilities

Human-like reasoning

Ability to observe, learn, and solve problems

Beyond human capabilities

Processing vast amounts of data and identifying complex patterns

Artificial Intelligence refers to intelligent activity carried out by machines designed to mimic human cognitive functions. AI systems perceive their environment and respond in human-like ways, executing reasoning, observation, learning, and problem-solving functions with increasing sophistication.

While early AI focused on basic rule-following, modern systems can learn from data and experience, often exceeding human capabilities in specific domains like pattern recognition across millions of data points. This evolution has transformed AI from a scientific curiosity to a powerful business tool with applications across industries.

Machine vs Deep Learning

Aspect	Machine Learning Example	Deep Learning Example
Task	Predict spam emails	Recognize objects in a photo
Data Requirement	Relatively smaller datasets	Requires large datasets for training
Complexity	Simpler models like decision trees	Complex models with multiple neural layers
Human Intervention	Needs feature selection and engineering	Learns features directly from raw data

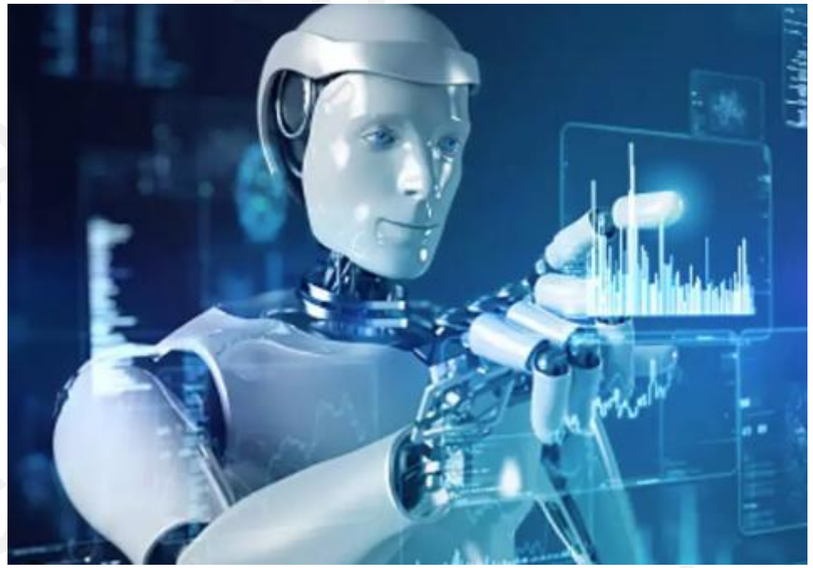
Examples:

- ❖ Spam Email Filtering
- ❖ Recommendations, eg Netflix
- ❖ Fraud Detection (pattern recognition – credit cards)
- ❖ Predictive Maintenance (sensors to track performance)

Examples:

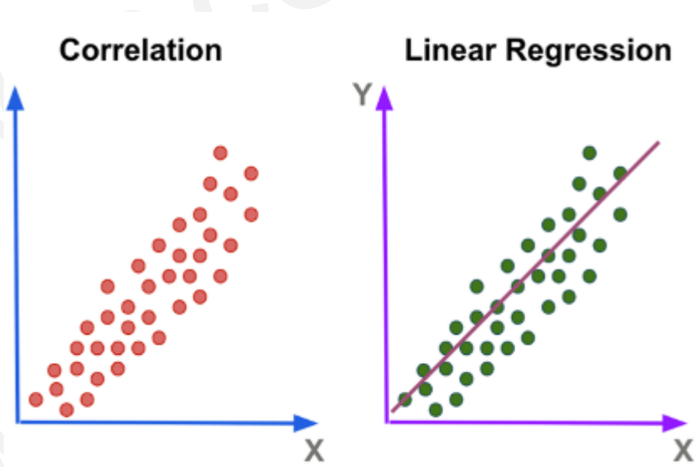
- ❖ Image Recognition
- ❖ Speech Recognition, eg Siri
- ❖ Autonomous Driving
- ❖ Language Translation
- ❖ Healthcare Diagnostics

Core Aspects of AI



1. **Learning**:
❖ **Machine Learning (ML)**: Systems improve performance based on data and experiences without being explicitly programmed.
❖ **Deep Learning**: A subset of ML using neural networks for tasks like image and speech recognition.
2. **Reasoning and Problem-Solving**:AI systems analyze information, make decisions, and solve problems autonomously or semi-autonomously.
3. **Natural Language Processing (NLP)**:Understanding, interpreting, and generating human language (e.g., chatbots, translation tools).
4. **Perception**:Processing sensory inputs like vision (e.g., image recognition) or sound (e.g., voice recognition).
5. **Autonomous Action**:Acting without human intervention, such as in robotics or self-driving cars.

Traditional Predictive Analytics



Key Characteristics

Traditional predictive analytics uses advanced statistical methods to estimate future events based on historical data. These techniques create mathematical models that capture important trends from past data, which are then applied to current information to predict outcomes or suggest optimal actions.

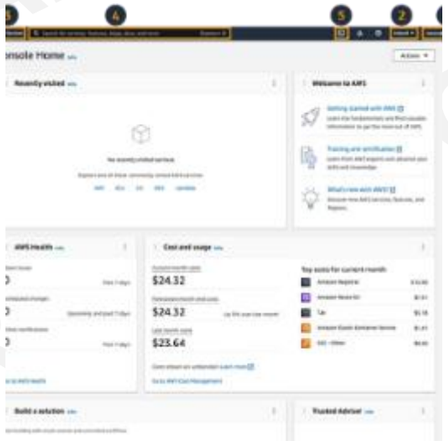
While powerful, these models have inherent limitations since past patterns don't always repeat in the future. However, historical data is often the only or most readily available information for analysis.

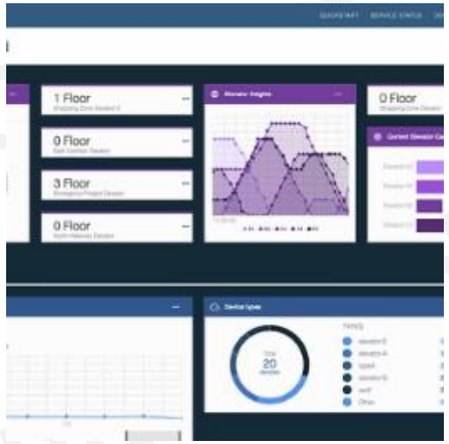
Common Techniques

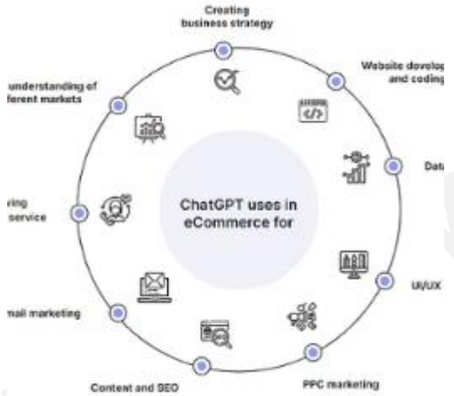
- Linear regression
- Logistic regression
- Clustering
- Factor analysis
- Time series analysis

These methods form the foundation of more advanced AI approaches and remain valuable tools in the analytics toolkit for specific use cases.

Enterprise Generative AI Applications







Major technology companies have developed enterprise-grade generative AI solutions that enhance efficiency, productivity, and creativity across various business functions. Microsoft Copilot integrates the GPT-4 language model into applications like Visual Studio Code and Microsoft Office, providing advanced code generation and content creation capabilities.

Amazon Q leverages AWS infrastructure to address specific business needs with real-time solutions and support. IBM WatsonX offers a comprehensive data and AI platform with tools for developing customized solutions, efficient data warehousing, and AI governance frameworks. These enterprise tools represent the commercialization of AI research into practical business applications.

Artificial Intelligence in Business Organizations & Regulation

Relevant IIA Standards for AI Auditing

Standard 9.1: Understanding Governance, Risk Management, and Control Processes

To develop an effective internal audit strategy and plan, the chief audit executive must understand the organization's governance, risk management, and control processes, including those related to AI systems.

Standard 3.1: Competency

Requires the chief audit executive to ensure that the internal audit function collectively possesses or obtains necessary competencies, which now includes AI-specific knowledge and skills.

Standard 3.2: Continuing Professional Development

States that internal auditors must continually develop their competencies through education and training, particularly important in the rapidly evolving field of AI.

Standard 1.3: Legal and Ethical Behavior

States that internal auditors must understand and abide by relevant laws and/or regulations, including making disclosures as required, which extends to AI regulations.

The AI Act: Europe's Regulatory Framework

Proposal and Approval

In April 2021, the European Commission approved a proposal for regulation establishing harmonized standards on AI. In May 2024, the Council of the European Union definitively approved the AI Law, with a 24-month transition period for effective application.

Key Objectives

The regulation aims to ensure AI systems in the EU market are secure and respect fundamental rights, improve governance and enforcement of existing legislation, and facilitate the development of a single market for legal, safe, and reliable AI applications.

Risk-Based Approach

The AI Act follows a risk-based approach, classifying AI systems based on their potential impact on health, safety, and fundamental rights. This classification determines the requirements and limitations for each type of AI system.

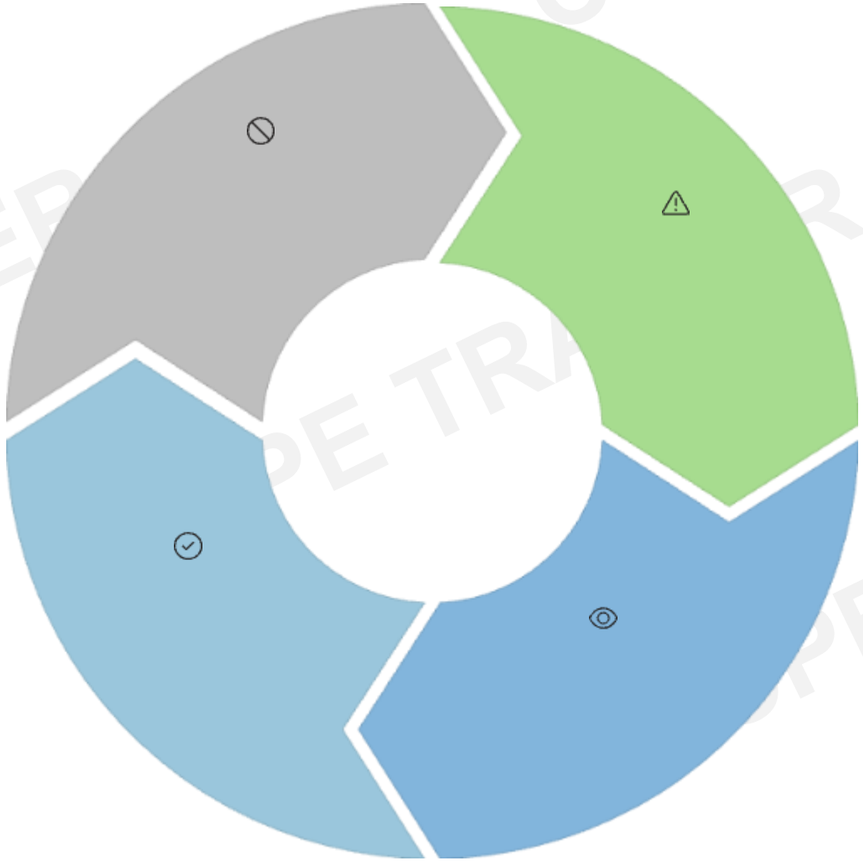
Classification of AI Systems Under the AI Act

Unacceptable Risk (Prohibited)

Systems for behavior manipulation, social scoring, or real-time remote mass biometric identification in public spaces (with limited exceptions)

Minimal Risk (Free Use)

The vast majority of AI systems currently in use, such as AI-enabled video games or spam filters



High Risk (Permitted with Requirements)

Systems in critical infrastructure, education, employment, essential services, law enforcement, migration, and justice administration

Limited Risk (Transparency Obligations)

Systems like chatbots where users should know they are interacting with AI

Classification of AI Systems Under the AI Act

1	2	3	4
Artificial Intelligence Systems with Unacceptable Risk (Art. 5)	**High-Risk Artificial Intelligence Systems (HRAIS, Art. 6)**	**Artificial Intelligence Systems with Specific Transparency Obligations (Art. 52)**	**Artificial Intelligence Systems with No or Minimal Risk**
Prohibited • Manipulation of behavior, opinions, and human decisions. • Classifiction of people based on their social behavior. • Mass biometric identification remotely and in real-time, with certain exceptions.	Allowed if the requirements of the AI for the ex-ante conformity assessment are met. • Key Aspects of the Regulation (Annex III). • Common regimes already subject to harmonized EU standard. • Additional list to be reviewed annually by the EAIB (Art. 84).	Allowed but subject to information/ transparency obligations. • Human interaction. • Use to detect emotions or determine categories based on biometric data. • Generation of manipulated content.	Allowed without restrictions.
EXAMPLE: Social scoring	**Example: Hiring**	**Example: Personification (bots)**	**Example: Predictive maintenance**

High-Risk AI Systems and Requirements

High-Risk AI Categories

- Biometric identification systems
- Critical infrastructure management
- Education and vocational training
- Employment and worker management
- Access to essential services
- Law enforcement applications
- Migration and border control
- Administration of justice

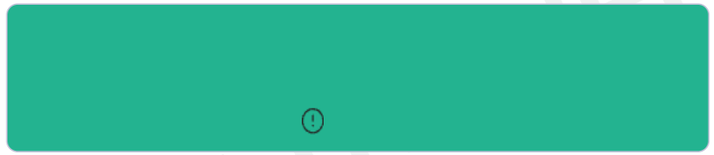
Key Requirements

- Appropriate risk assessment and mitigation systems
- High-quality data sets for training and validation
- Detailed activity recording for traceability
- Comprehensive documentation
- Clear information for users
- Appropriate human oversight
- High levels of robustness, security, and accuracy

Sanctions for Non-Compliance with the AI Act

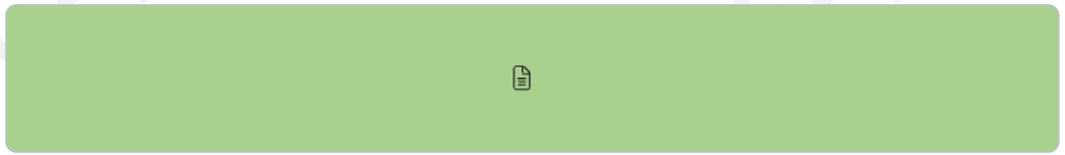
Prohibited Practices

Up to €35 million or 7% of annual worldwide turnover



Other Requirements

Up to €15 million or 3% of annual worldwide turnover



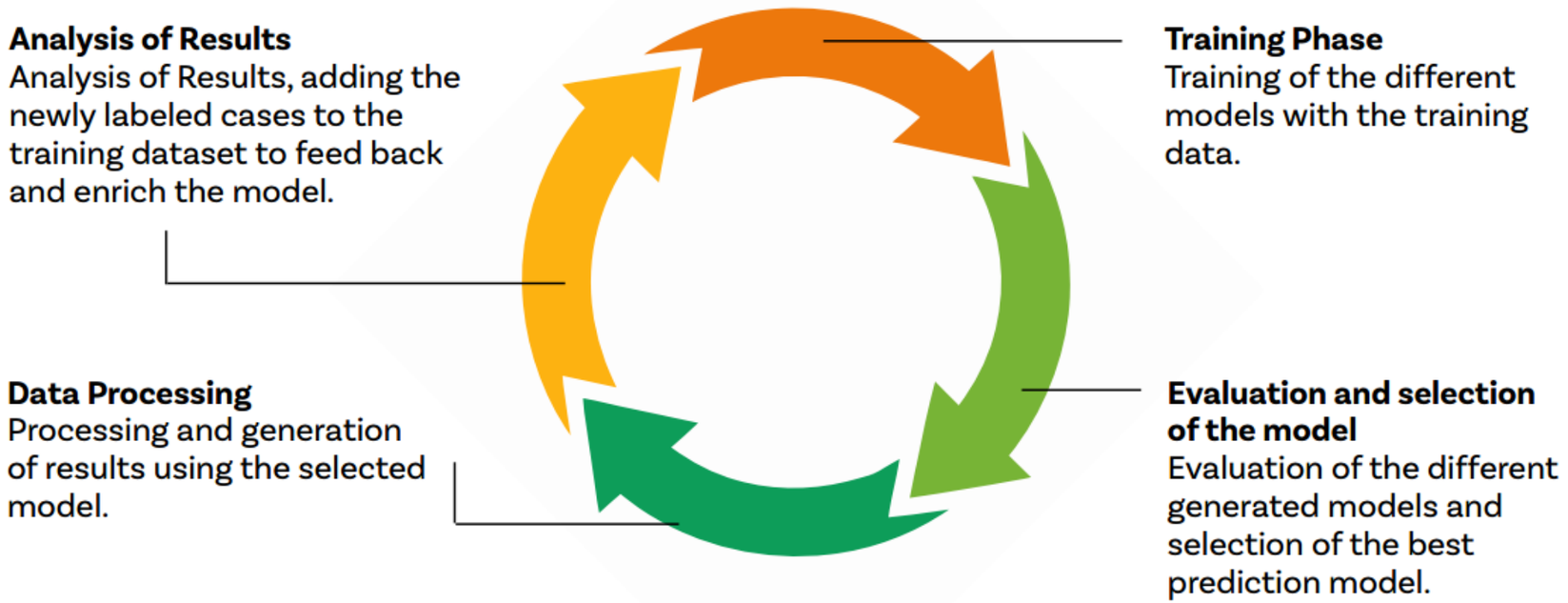
Misleading Information

Up to €7.5 million or 1.5% of annual worldwide turnover

The EU AI Act establishes a strict sanctioning regime that exceeds even the GDPR penalties. For comparison, GDPR's most serious sanctions are up to €20 million or 4% of annual turnover. The AI Act does consider a more proportionate sanctioning regime for small and medium-sized companies and startups, though specific details are to be defined.

Artificial Intelligence Models & Machine Learning

Types of Machine Learning: Supervised Learning



Continuous improvement of the model based on supervised learning.

In **supervised** learning, **algorithms make predictions based on patterns** identified in historical labeled data. The system **learns relationships between target variables and other model features** from this known data, establishing rules that can be applied to predict outcomes for new information.

Common algorithms include d**ecision trees, gradient boosting, random forest, support vector machines (SVM), and Naive Bayes**. These techniques are widely used in financial customer scoring, industrial predictive maintenance, disease detection, and cybersecurity applications.

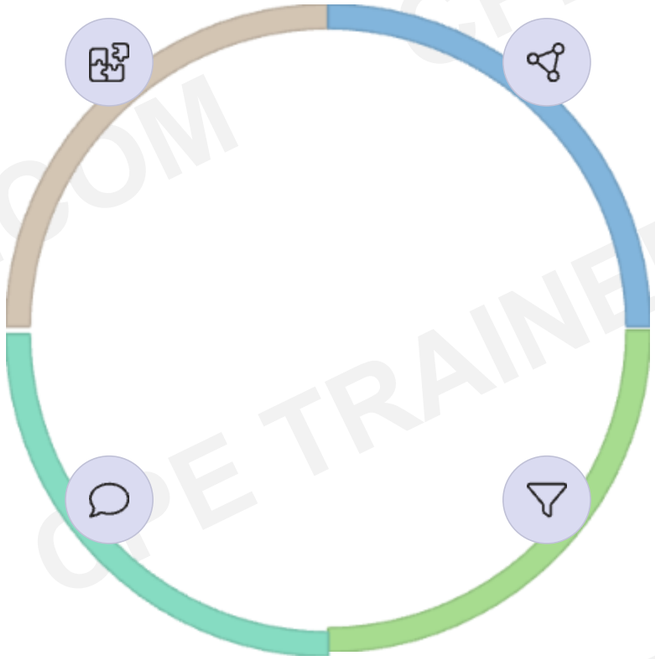
Types of Machine Learning: Unsupervised Learning

Pattern Discovery

Algorithms identify hidden structures in unlabeled data

Anomaly Detection

Identifies outliers and unusual patterns



Clustering

Groups data points based on similarity measures

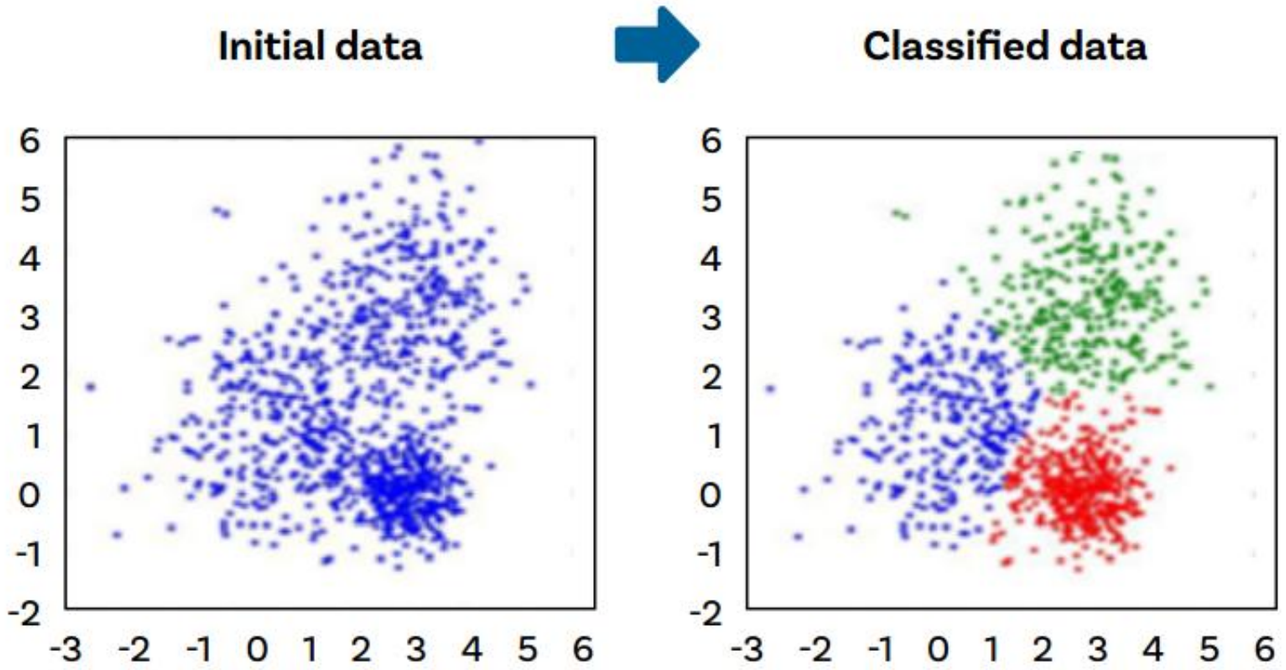
Dimensionality Reduction

Simplifies data while preserving important information

Unsupervised learning algorithms operate without labeled data, producing knowledge solely from input information. These algorithms **self-organize data** into groups based on common characteristics, exploring relationships to structure or organize information according to inherent patterns.

Common unsupervised learning algorithms include **k-means clustering, isolation forest, and neural networks**. Modern computing power has overcome previous limitations, enabling significant advances in these techniques. Applications include image and voice recognition, medical diagnostics, and anomalous information detection.

Types of Machine Learning: Unsupervised Learning



Data Classification in Unsupervised Environments.

Reinforcement Learning: Learning Through Experience

Agent Explores Environment

The AI agent interacts with its environment through actions

Receives Feedback

Environment provides rewards or penalties based on actions

Updates Strategy

Agent adjusts behavior to maximize future rewards

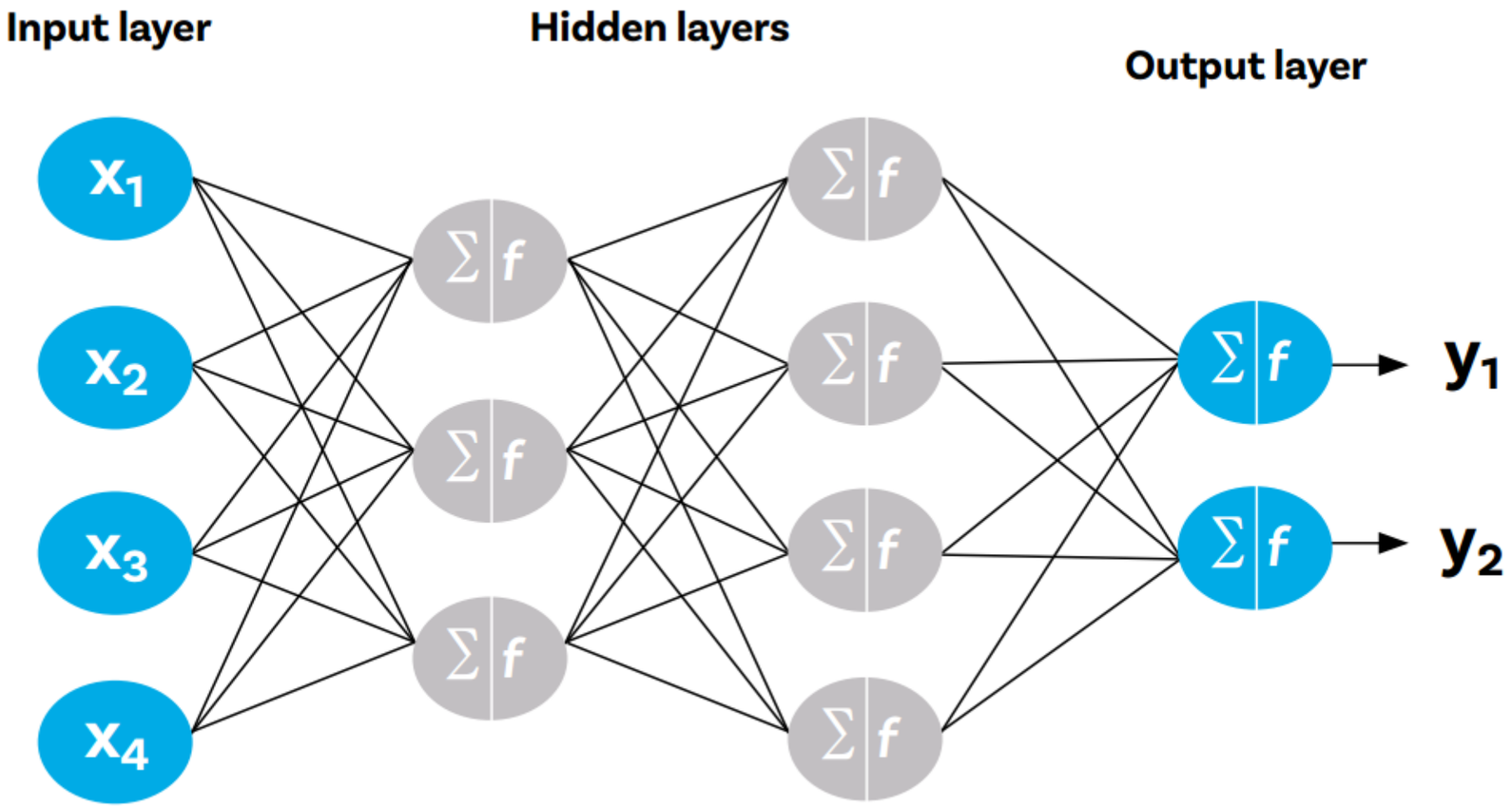
Iterative Improvement

Process continues until optimal strategy is found

Reinforcement learning uses a reward-based trial and error system to train AI agents with minimal data. The algorithm navigates its environment, receiving rewards or penalties based on decisions made, allowing it to refine its strategy through iterations until finding the optimal approach.

This approach faces challenges: the agent must balance exploiting known strategies versus exploring new ones, and rewards may come long after relevant actions. Despite these difficulties, reinforcement learning succeeds in algorithmic trading, chatbot training, autonomous web browsing, video games, and recommendation systems.

Neural Networks: Example



Example of a simple neural network with two hidden layers. Source: https://www.knime.com/blog/a-friendly-introduction-to-deep-neural-networks

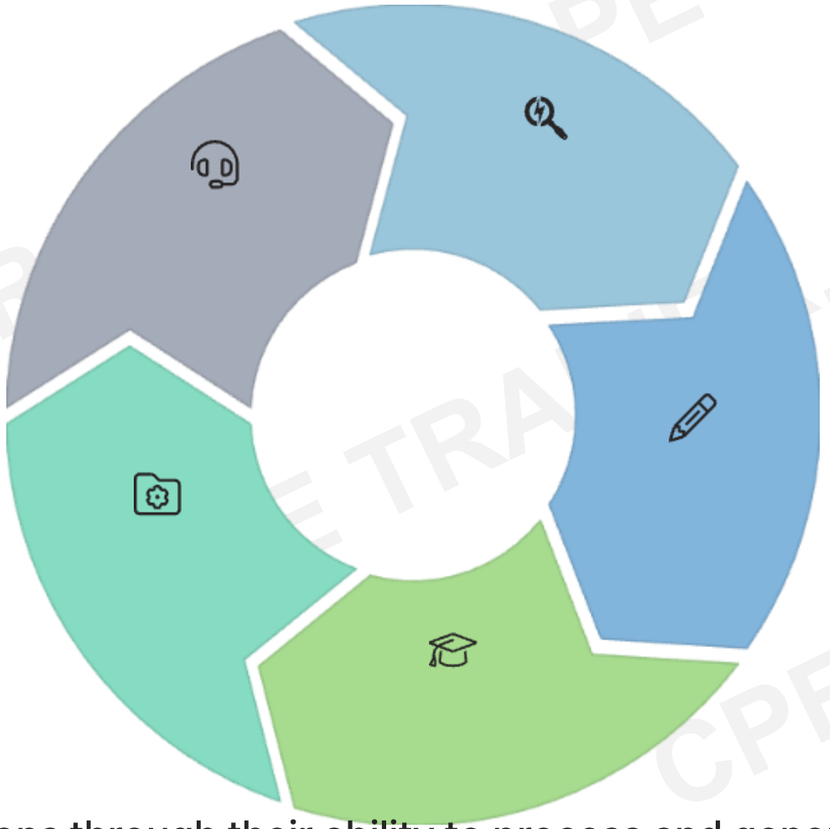
Business Applications of Large Language Models

Customer Service

Chatbots and virtual assistants providing 24/7 support

Process Optimization

Automating administrative tasks and workflows



Text Analysis

Processing documents, emails, and feedback for insights

Content Creation

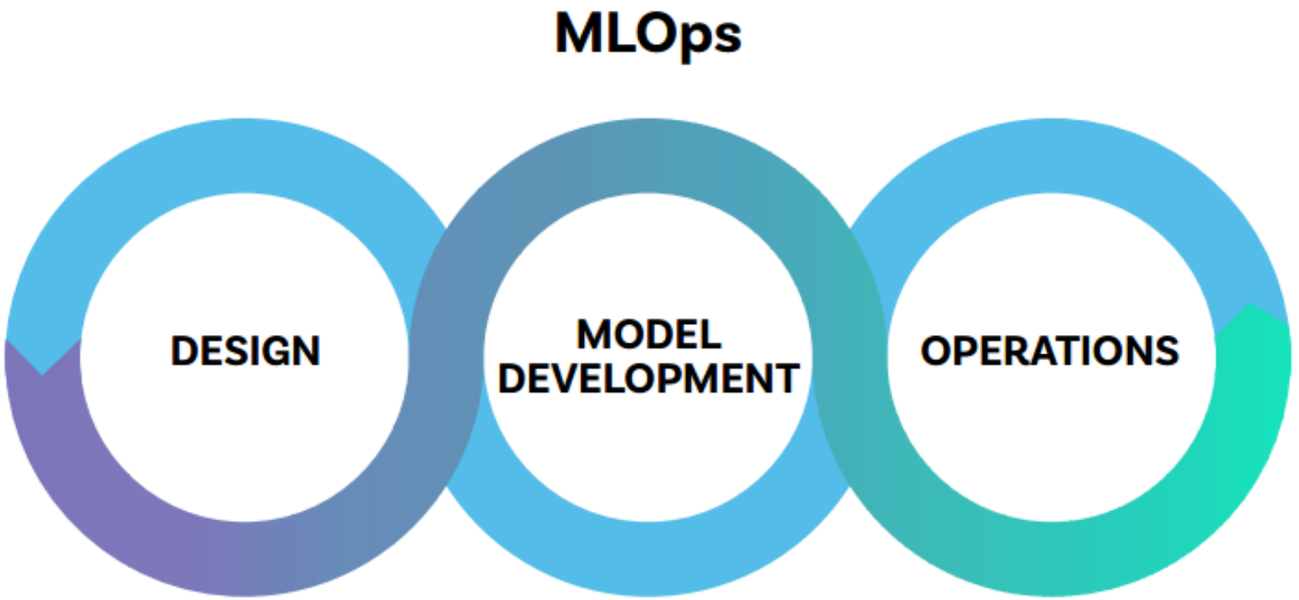
Generating reports, emails, and marketing materials

Training

Creating personalized learning scenarios and simulations

LLMs are transforming business operations through their ability to process and generate human language effectively. They power sophisticated customer service automation through chatbots that provide instant, accurate responses while reducing human workload. For content analysis, they can process massive document collections to extract meaningful insights and identify patterns across various text sources.

MLOps: Iterative Process



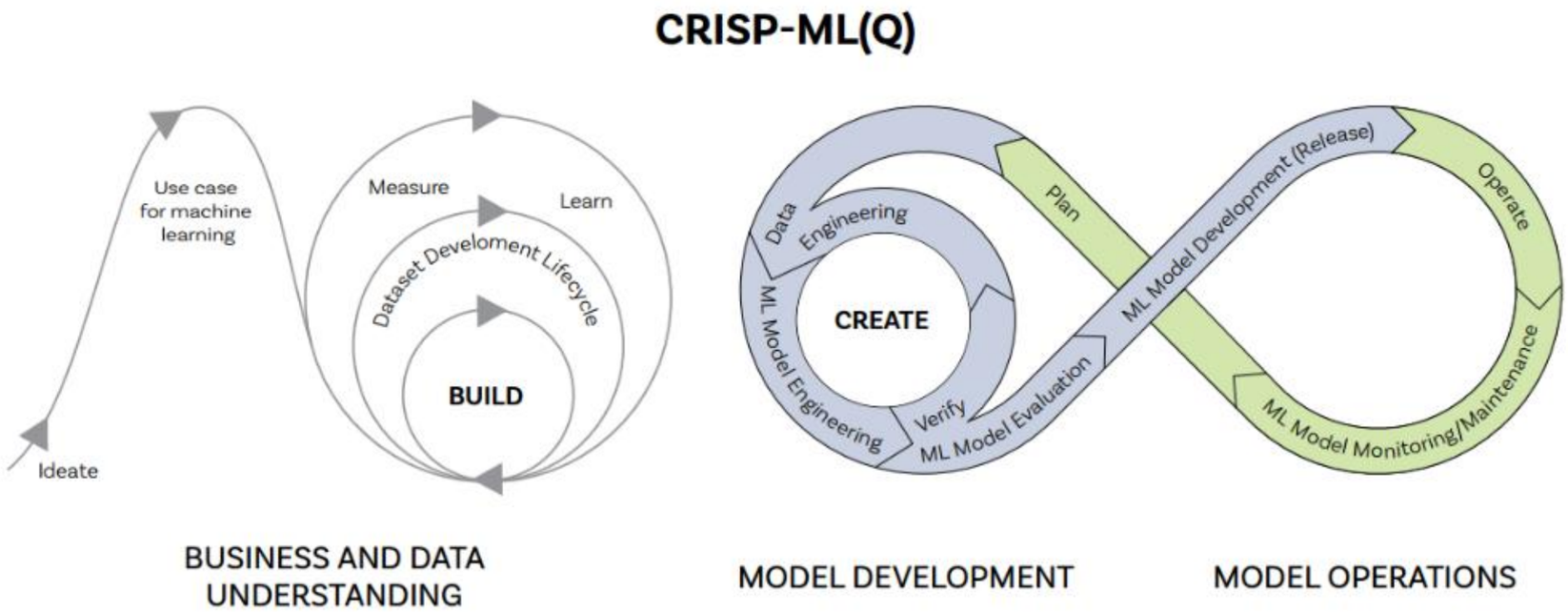
- Requirements Engineering
- ML Use-Cases Prioritization
- Data Availability Check

- Data Engineering
- HL Model Engineering
- Model Testing and Validation

- HL Model Deployment
- CI/CD Pipelines
- Monitoring and Triggering

The incremental iterative process of ML-OPS. Source: https://Ml-ops.org

Cross-Industry Standard Process for Development of Machine Learning Applications with Quality Assurance (CRISP-ML(Q)) methodology



Machine learning development life cycle according to methodology CRISP-ML(Q). Source: ml-ops.org.

The CRISP-ML(Q) methodology provides a structured approach to quality-assured machine learning development, aligning business needs with technical implementation. For auditors, the documentation and evidence produced during this process offer valuable insights for assessing operational effectiveness and business alignment.

Energy Consumption of Generative AI

650,000

kWh

Energy consumed training a model 10x smaller than ChatGPT

5,214

kWh

Average per capita energy consumption in Spain (2022)

2,638

MWh

Energy required for Meta's Llama model training

2,008

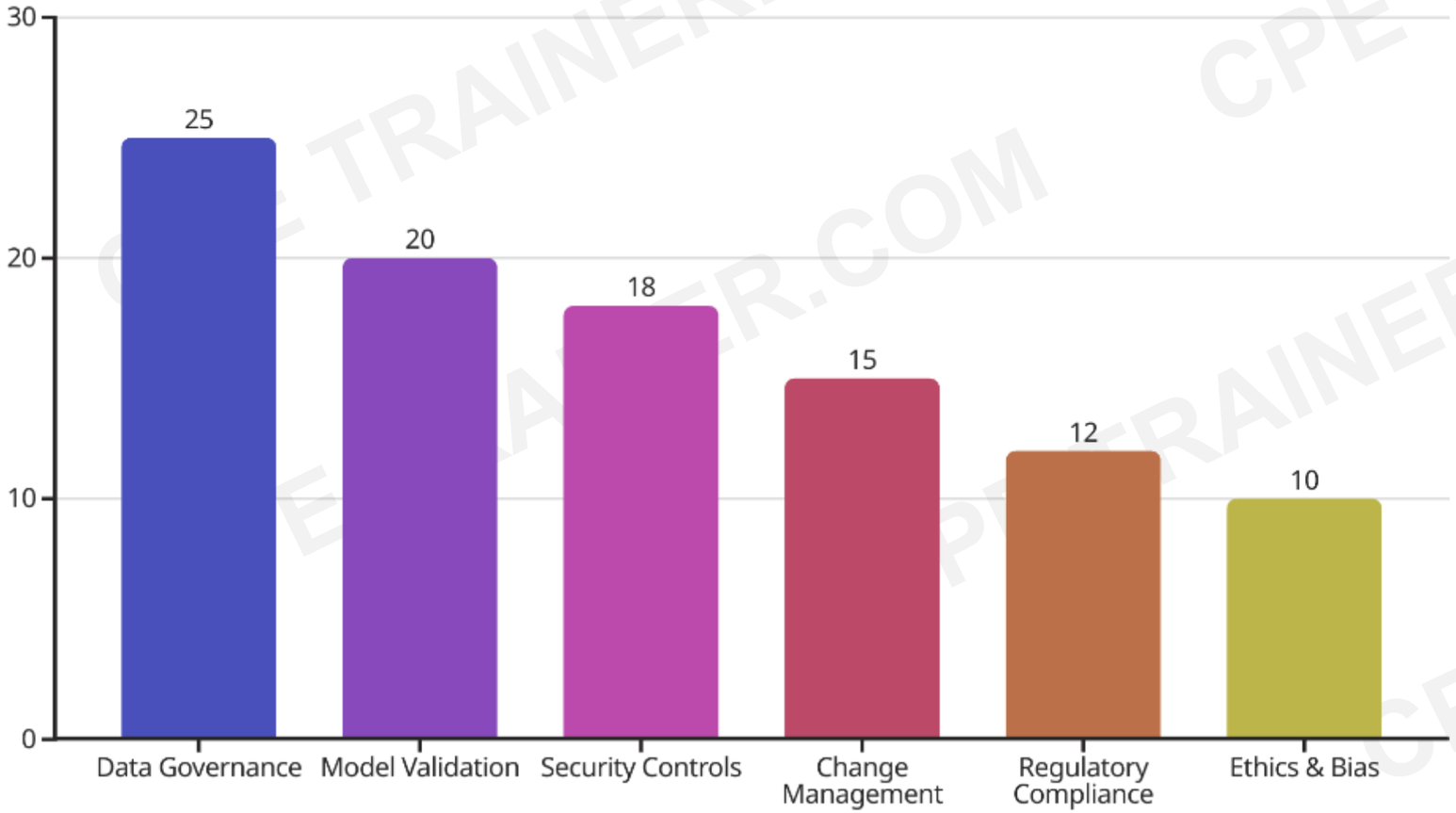
Years

How long a 150W refrigerator could run on Llama's training energy

Behind the remarkable capabilities of generative AI and large language models lies significant energy consumption reaching truly surprising figures. The environmental impact of these technologies presents a substantial challenge for organizations committed to sustainability goals and carbon footprint reduction.

Optimizing AI energy efficiency will be critical as adoption increases, likely requiring complementary technologies like renewable energy sources to mitigate environmental impacts. Auditors should consider these sustainability implications when evaluating the long-term viability and risk profile of AI implementations.

Key Audit Considerations for AI Systems



Model validation procedures ensure AI systems function as intended and produce accurate results. Security controls protect sensitive data and prevent unauthorized access or manipulation. Change management processes govern how models are updated, while regulatory compliance and ethics considerations address legal requirements and potential bias issues that could lead to discriminatory outcomes or reputational damage.

When auditing AI-enabled business processes, internal auditors should prioritize several key areas to effectively assess risks and controls. Data governance represents the largest focus area, as the quality and integrity of input data directly impacts model performance and output reliability.

Internal Control Framework & Business Risk

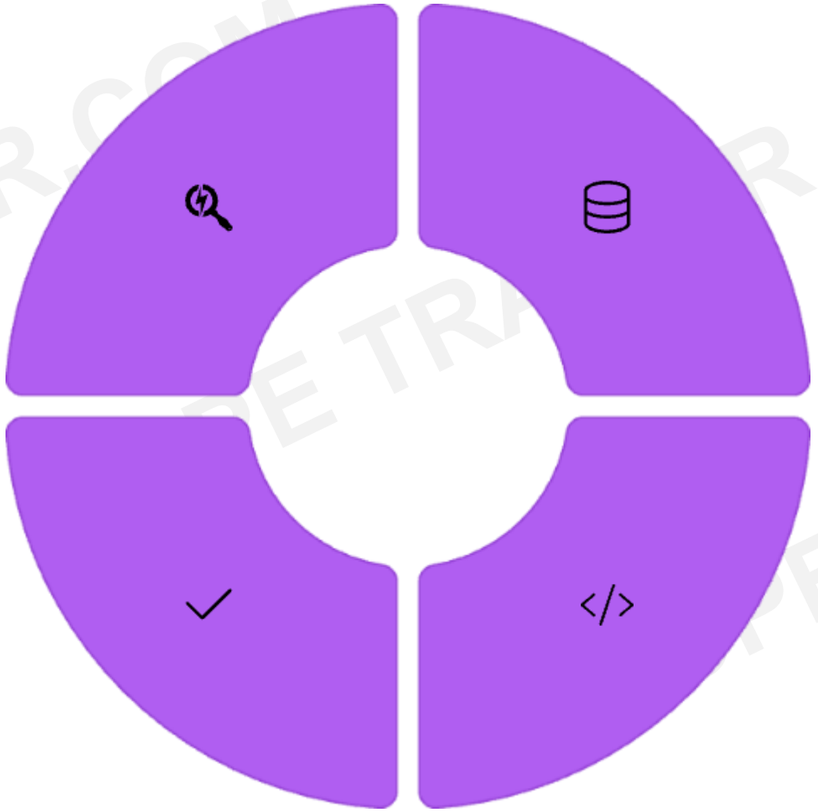
Key Activities in AI Internal Control

Continuous Risk Monitoring

Identification of general risks due to AI deployment, with specific risk assessment based on the complexity of algorithms and objectives pursued with each AI model.

Implementation Supervision

Develop sufficient implementation tests to guarantee that the deployment meets expected objectives. Obtain relevant approvals before going live.



Data and IT Architecture Supervision

Activities defined to guarantee access, treatment, privacy, protection, and destruction of data, especially those in predictive models of human behavior.

Review of AI Models

Ensure adequate understanding of algorithm operation and expected output. Define metrics and performance indicators for continuous monitoring.

Control Environment: Governance and Culture

Tone at the Top

The board and senior management must set the "tone at the top" regarding the importance of internal control for AI systems, including standards of conduct considered acceptable.

Ethical Framework

Promote the organization's commitment to integrity and ethical, social, and legal values to ensure AI-related activities and decisions align with these values.

Competency Development

Establish appropriate competency levels for the management and supervision of AI systems. Board members and management committee must understand key concepts of AI models.

Risk-Conscious Culture

Establish a risk-conscious culture, with controls, policies, and processes that guide people at all levels in performing their AI-related responsibilities.

Data Governance in AI Control Environment

Creation

Establish protocols for data collection ensuring quality, relevance, and compliance with privacy regulations.

Transformation

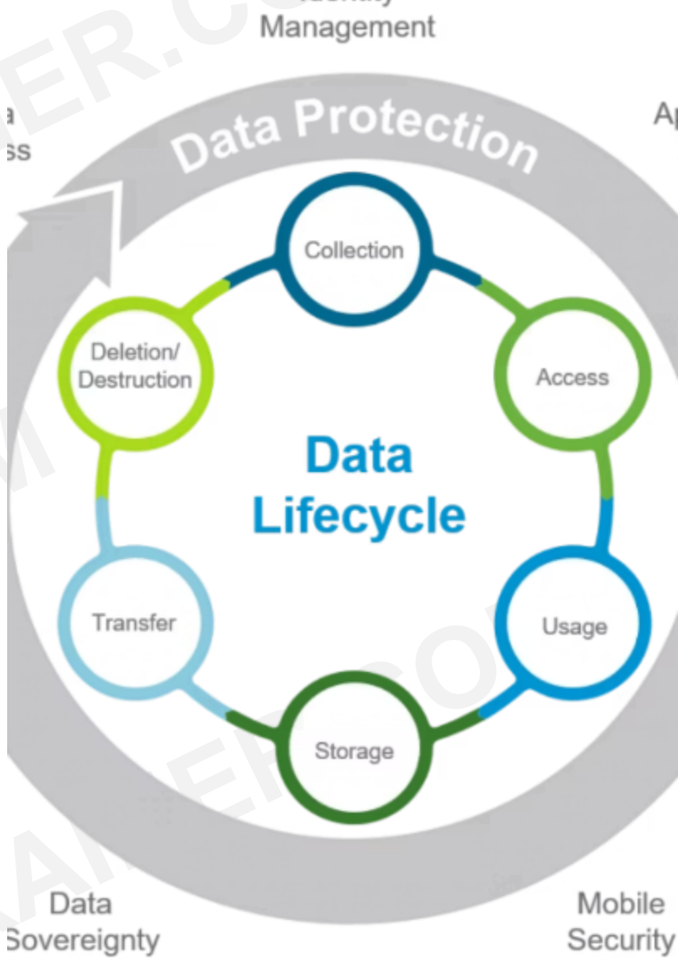
Implement controls over data processing, cleaning, and feature engineering to maintain data integrity.

Usage

Monitor how data is used within AI models to prevent unauthorized access and ensure appropriate application.

Destruction

Enforce proper data deletion procedures in compliance with retention policies and regulatory requirements.



Data governance is crucial throughout the entire lifecycle due to the massive volumes of data utilized by AI systems. Organizations must implement controls at each stage to ensure data quality, security, and appropriate usage.

Board and Senior Management Responsibilities

Strategic Oversight

Advise on whether the organizational strategy adequately considers the threats and opportunities of AI systems. Consider establishing a specific AI committee or assigning responsibilities to an existing committee.

Talent Development

Promote programs for knowledge and skills training specific to AI systems and adopt policies to attract, develop, and retain competent professionals in this area.

Risk Oversight

Identify risks of AI systems and incorporate them into the organization's risk models, defining the risk appetite for this technology category.

Control Evaluation

Supervise and evaluate the effectiveness of the governance model's internal control regarding AI models, focusing on both design and operation of control structures.

Categories of AI-Related Risks

Governance Risks

Related to internal structures, policies, methodologies, and decision-making processes. May impact management and leadership, independence in decision-making, and promotion of transparency and accountability.

Operational/Business Risks

Occur throughout the AI system lifecycle. Include processing errors, data risks, biases in results, or issues with data representativeness that affect business operations.

Financial Risks

Related to accounting operations and financial reporting. Consider situations where AI may impact the financial information presented or the organization's financial results.

Regulatory Risks

Linked to legal and regulatory compliance, such as GDPR or internal ethical codes. Includes risks related to AI activities that must align with company values and responsibilities.

Additional AI Risk Categories

Technological and Cybersecurity Risks

Associated with systems and cybersecurity of AI models. Evaluate whether models containing personal data are at risk of unauthorized access and use by third parties.

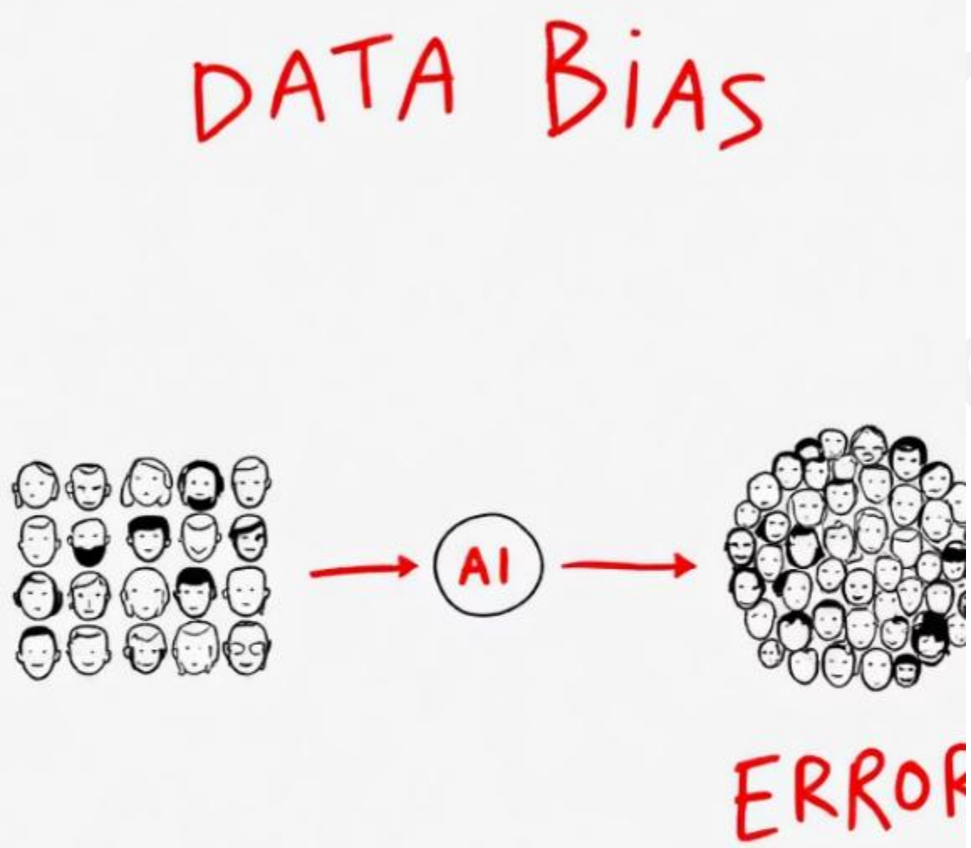
Reputational Risk

Derived from biases in models, regulatory sanctions, or exposure to external risks generated by third parties. Can significantly impact public perception and trust.

Sustainability Risk

Energy consumption required for AI systems (especially generative AI) can impact sustainability commitments related to greenhouse gas reduction, energy efficiency, or carbon footprint.

Organizations must comprehensively assess all risk categories when implementing AI systems. Each category requires specific controls and mitigation strategies to ensure responsible AI deployment that protects both the organization and its stakeholders.



Intrinsic Risks of AI Models

Data Use Risks

Incomplete or inaccurate data can cause unstable or incorrect algorithm results. Poor data selection may also have ethical repercussions by excluding certain information groups, resulting in discriminatory or biased models.

Algorithm Development Risks

Errors in programming and code development can cause unexpected or inadequate results. The development phase is critical, especially in sophisticated AI systems where any coding error can lead to inappropriate outcomes.

Output Interpretation Risks

Inability to interpret or incorrect interpretation of AI model outputs can lead to decisions with unwanted results. Neural network algorithms present greater risk of misinterpretation due to their complexity.

Control Activities: Best Practices

Comprehensive Documentation

Develop detailed procedures and risk/control matrices that identify the design of control activities and their key attributes. Include supporting documentation demonstrating control effectiveness and clearly define responsible parties.

Human Oversight

Design timely "human review" activities to monitor behaviors and results of AI algorithms. This ensures they reflect original objectives and are used in a legal, ethical, and responsible manner.

Monitoring Systems

Implement alerts and indicators to quickly identify deviations from initial AI algorithm objectives. These warning systems enable timely intervention before minor issues become significant problems.

Role of Internal Audit & Establishing Work Programs

Role of Internal Audit in AI Governance

Risk Assessment

Evaluate AI-specific risks including algorithmic bias, data quality issues, and regulatory compliance concerns.

Control Evaluation

Assess the design and operating effectiveness of controls over AI systems, including governance structures, development processes, and monitoring mechanisms.

Advisory Services

Provide insights on emerging AI risks and control practices, helping the organization stay ahead of regulatory requirements and industry standards.

Continuous Monitoring

Develop approaches for ongoing assessment of AI systems as they evolve and adapt through machine learning.

Audit Program for AI Systems





A comprehensive audit program for AI systems should cover key areas including the AI governance model, data architecture and IT systems, data quality, performance measurement, the "black box" factor in AI systems, and the human factor including algorithmic bias. Each area requires specialized audit procedures tailored to the unique characteristics of AI technologies.

Internal auditors should develop strategies that address both the technical aspects of AI systems and their broader business implications, ensuring that AI applications align with organizational objectives while managing associated risks effectively.

Internal Audit's Role in AI Governance

Strategic Value

The internal audit function brings expertise in evaluating and understanding risks and opportunities related to meeting strategic objectives, including those aimed at AI deployment. Audit teams help assess, understand, and communicate how AI algorithms affect organizational value creation.

Independent Assurance

While maintaining independence and objectivity, internal audit provides crucial assurance on AI risks, governance, and controls. This includes evaluating both the design and operational effectiveness of internal control structures established under the organization's AI governance model.

Internal audit should include relevant aspects of AI in risk management evaluations and consider them in risk-based audit planning. The function plays a vital role in providing objective assessment of AI initiatives while helping the organization navigate this complex technological landscape.

Seven Critical Activities for Internal Audit

Risk-Based AI Inclusion

Include relevant AI aspects in risk assessment and audit planning. Evaluate the design and implementation of the AI governance model established by the organization.

Project Engagement

Actively engage in AI projects from start to finish by conducting systematic design audits. Report design control deficiencies promptly while maintaining independence and objectivity.

Algorithm Reliability

Provide assurance or assess management of risks related to the reliability of underlying algorithms and the data on which AI algorithms are based.

Ethical Alignment

Ensure internal controls exist and operate effectively to identify matters generated by AI algorithms that may affect the organization's code of ethics.

Additional Internal Audit Responsibilities

Control Structure Evaluation

Evaluate both the design and operation of internal control structures implemented as a result of the end-to-end governance model established in the company.

ESG Compliance

Supervise compliance with regulations related to environmental, social, and governance concerns, including controls designed to achieve resource efficiency objectives.

Results Reporting

Report the main results of AI risk assessments to the board, audit committee, and senior management. Highlight control deficiencies and suggest governance best practices.

The internal audit function must maintain independence while providing valuable insights on AI governance. By fulfilling these responsibilities, internal audit helps organizations navigate the complex risks associated with AI implementation while ensuring alignment with strategic objectives.

The Three Lines Model in AI Governance

The IIA's Three Lines Model provides six principles for defining roles and responsibilities in AI governance. The first line (management) owns and manages AI risks directly. The second line (risk management, compliance) provides expertise, support, and monitoring. The third line (internal audit) offers independent and objective assurance on the effectiveness of governance and risk management.

This model ensures appropriate oversight, risk management, and assurance services to the organization's stakeholders, creating a comprehensive governance framework for AI systems.

Six Key Internal Control Areas

Governance Model

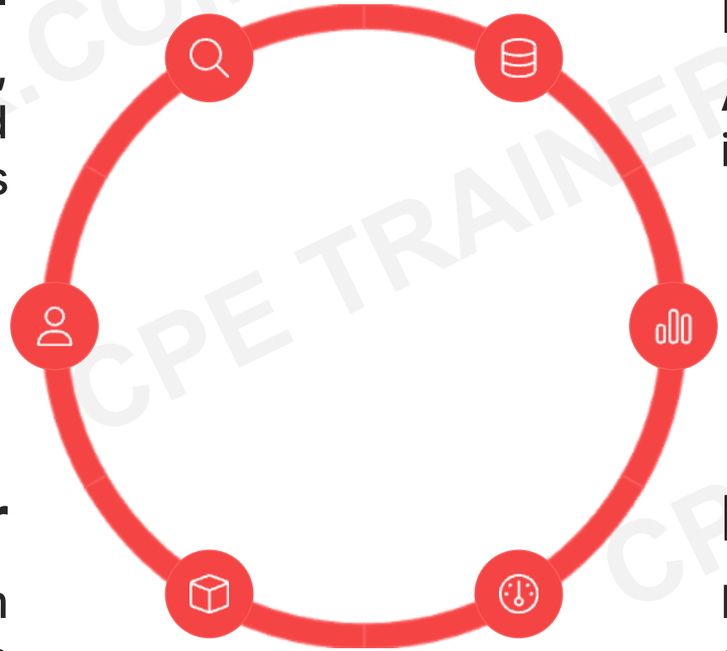
Organizational structure, responsibilities, policies, and oversight mechanisms for AI systems

Human Factor

Addressing ethical considerations and algorithmic bias

Black Box Factor

Controls to address risks from complex, unexplainable AI algorithms



Data Architecture

Access controls, security, and IT infrastructure supporting AI systems

Data Quality

Reliability, accuracy, and integrity of data feeding AI algorithms

Performance Measurement

Metrics and monitoring to ensure AI systems meet business objectives

Governance Model of AI Systems

Organizational Design

Organizations must establish appropriate governance models for AI systems with clearly defined responsibilities for design, implementation, maintenance, and monitoring. The structure should align with the complexity of AI models deployed.

Technical Expertise

Organizations need adequate experience and knowledge for deployment and maintenance, particularly for sophisticated AI models. Technical competence must be assessed and maintained through appropriate staffing and training initiatives.

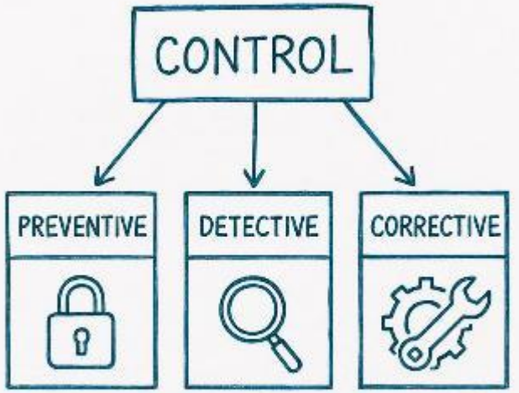
Strategic Alignment

Decisions about AI use cases must align with organizational ethical values and internal policies while complying with external regulations. Implementation strategies should include risk assessment and mitigation measures.

Resource Management

Organizations should measure and manage budgets and resources required for AI implementation, including ROI analysis during the design phase to justify investments and assess economic viability.

Governance Control Objectives



1 Appropriate Governance Structure

Implement a governance model appropriate to the complexity and risks of AI systems, including ROI analysis during design phase. Audit procedures include reviewing organizational structure, governance model design, and ROI analysis methodologies.

2 Clear Roles and Responsibilities

Define key roles and responsibilities for development and management of AI environments, ensuring qualified personnel with technical and business knowledge. Audit procedures include reviewing job descriptions, professional experience, and verification of qualifications.

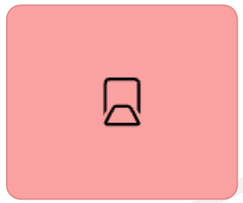
3 Adequate Policies and Procedures

Develop sufficient internal policies and procedures for AI governance, ensuring they're accessible, known, and applied organization-wide. Audit procedures include reviewing policy comprehensiveness and assessing implementation effectiveness.

4 Regulatory Compliance

Analyze impact of applicable regulations (e.g., AI Act, GDPR) and implement adequate compliance systems. Audit procedures include verification of regulatory compliance checklist and evaluation of compliance systems.

Additional Governance Controls



Centralized AI Inventory

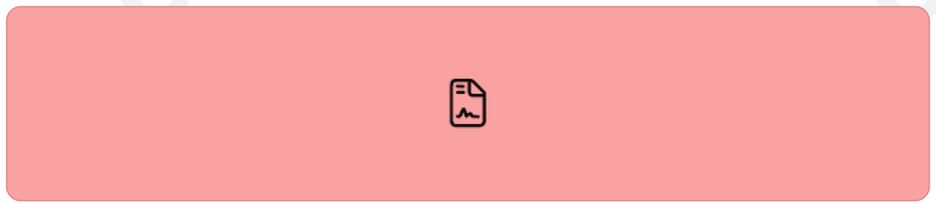
Maintain a centralized, updated inventory of algorithms subject to risk analysis

Risk Evaluation Model

Implement continuous risk assessment with GRC tools for monitoring

Financial Impact Controls

Establish mechanisms to identify AI models affecting financial reporting



Vendor Management

Define specific requirements for AI service or application providers

Environmental Monitoring

Track environmental impact of AI models on sustainability commitments

Data Architecture and IT Systems

Data Access Management

Organizations must control access to data generated and used by AI systems, including metadata and taxonomy. This requires precise definition of user roles and access permissions based on responsibilities.

Audit procedures focus on verifying formalized processes for access profiles, authentication protocols, and segregation of functions between roles such as operators, developers, and data owners.

Data Lifecycle Protection

Organizations must ensure privacy, security, confidentiality, and appropriate treatment throughout the entire data lifecycle, from collection to destruction.

Auditors should validate that data protection policies comply with applicable regulations, especially for sensitive data, and confirm that confidential data used in training generative AI models doesn't introduce external risks.

Change Management and Continuity

Organizations need procedures for architecture and data change management across development, test, and production environments, along with backup policies and recovery plans.

Audit procedures include verification of change approval processes, testing protocols, and examination of continuity and recovery planning documentation.

Data Architecture Control Objectives

User Access Controls

Implement formalized processes for access profiles and roles with appropriate authentication and permission management. Audit procedures include reviewing user registration procedures, access control mechanisms, and verification of segregation of duties.

Change Management

Establish procedures for architecture and data changes across development, test, and production environments. Audit procedures include validating approval processes, user acceptance testing, and implementation monitoring.

Security and Continuity

Define backup policies, continuity plans, and cybersecurity protection for AI systems. Audit procedures involve reviewing backup existence, recovery plans, and integration with organizational cybersecurity strategies.

Data Protection Compliance

Ensure data protection compliance with applicable regulations and prevent confidential data incorporation into external models. Audit procedures include reviewing protection policies and training mechanisms for models created by third parties.

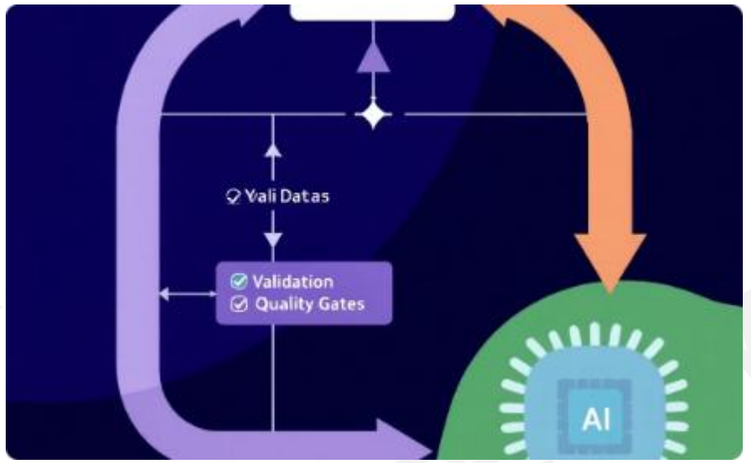
Data Quality Management

Data Reliability Assessment

Organizations must ensure reliability, accuracy, and integrity of data feeding AI algorithms. The enormous volumes of data required for AI performance make quality management a priority to guarantee effective algorithm operation.

Quality Control Processes

Formal procedures must be established for data reading, transformation, and quality testing. These procedures should include integrity checks, accuracy verification, and error handling to ensure reliable AI model inputs.



Continuous Monitoring

Data sources and repositories require continuous supervision with metrics and exception reports for analysis. For generative AI, specific control mechanisms must restrict use of personal or confidential data and prevent generation of inappropriate content.

Performance Measurement Control Objectives

1

Continuous Monitoring Procedure

Implement procedures for continuous performance measurement of AI models, including activities, parameters, reports, and metrics. Audit procedures include reviewing monitoring protocols and evaluating metric suitability.

2

Results Interpretation Protocol

Document procedures for interpreting algorithm results with tolerance margins and thresholds. Audit procedures verify interpretation requirements and confirm owners have sufficient expertise.

3

Back Testing Process

Establish back testing to measure model precision by replicating past results with historical data. Audit procedures include reviewing back testing methodology and independent reperformance.

4

Stress Testing Implementation

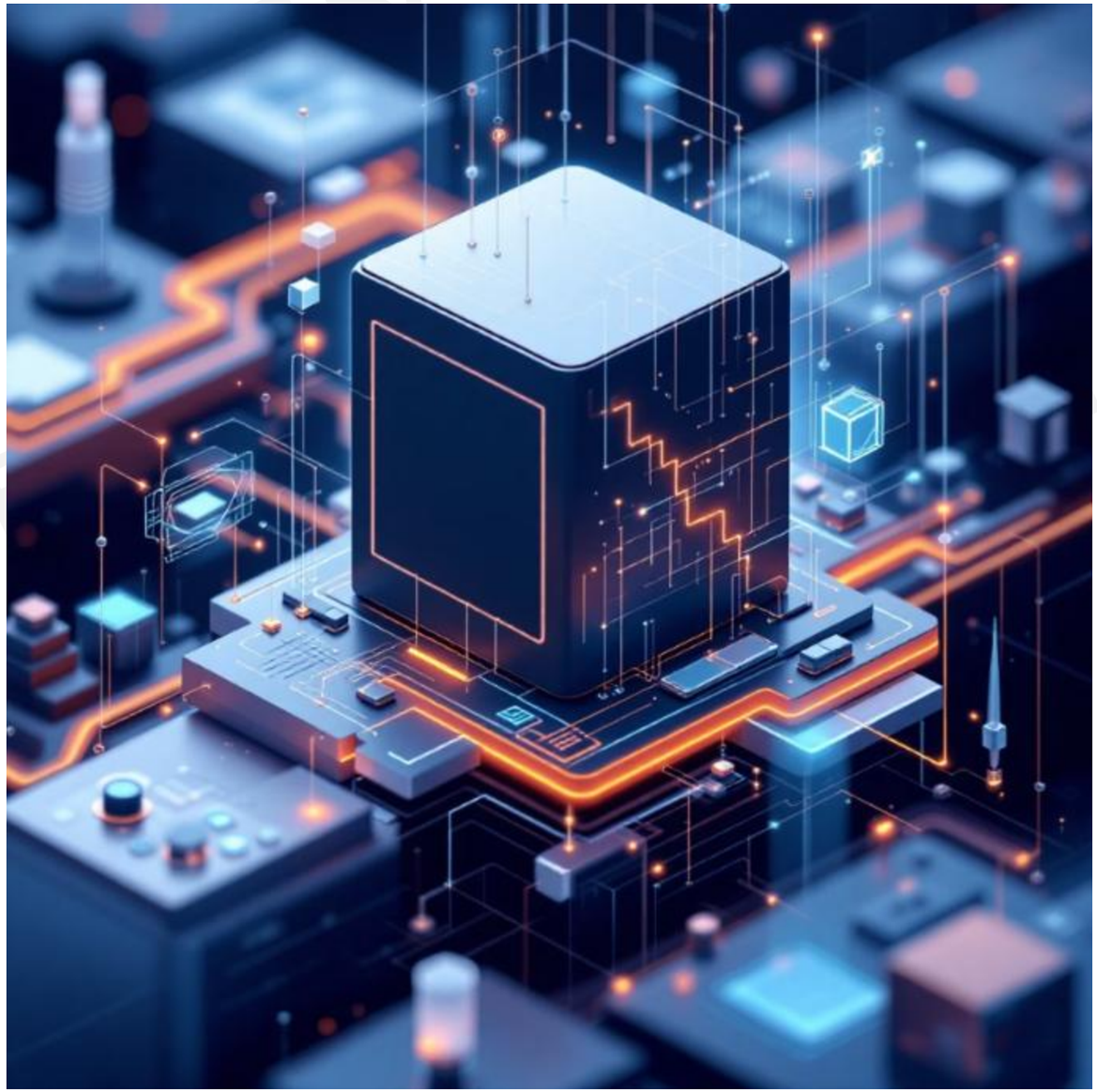
Conduct stress testing to measure expected results under extreme conditions. Audit procedures involve reviewing stress testing protocols and reperforming execution with modified input data.

The Black Box Factor in AI Systems

Defining the Challenge

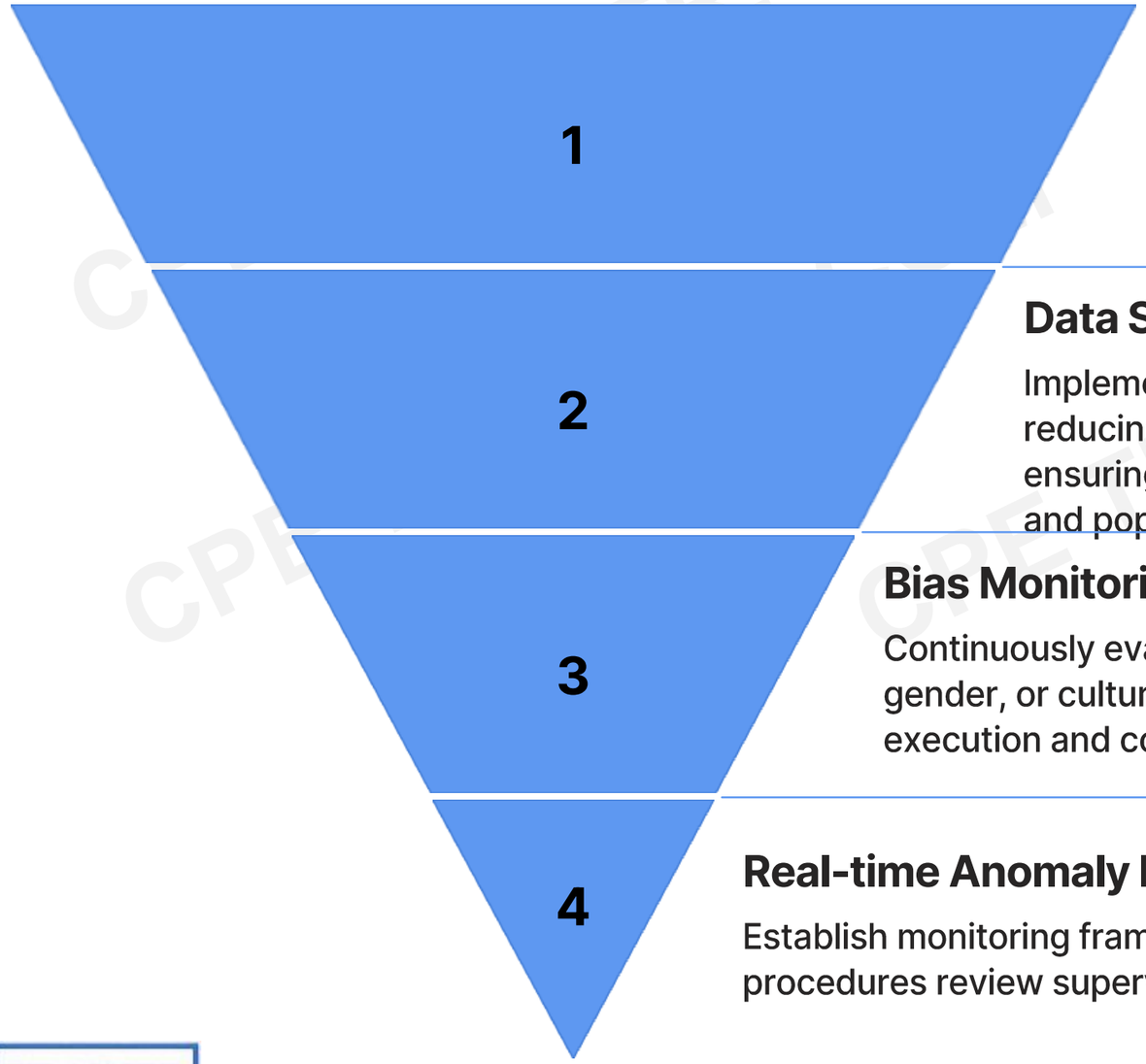
The "black box factor" refers to AI algorithms where internal execution mechanisms between input and output are difficult to understand or explain due to their complexity or sophistication.

This opacity increases risk intensity in organizations implementing complex AI algorithms. Consequently, robust internal control structures become critical to mitigate inherent risks from relying on algorithm results with high black box factors.



Organizations must implement controls to provide reasonable assurance about algorithm operations despite limited visibility into processing mechanisms. This includes sensitivity analysis, performance metrics, and continuous monitoring of both training data and operational outputs.

Black Box Factor Control Objectives



Sensitivity Analysis Procedure

Document procedures for analyzing model sensitivity to input data fluctuations, including precision metrics and predefined values for false positives/negatives. Audit procedures evaluate metric establishment and analysis of error rates.

Data Sufficiency Controls

Implement controls to ensure sufficient data for accurate model results, reducing de facto black box effects. Audit procedures review activities ensuring comprehensive data provision covering necessary time periods and population variations.

Bias Monitoring

Continuously evaluate possible biases related to ethical, political, ethnic, racial, gender, or cultural components. Audit procedures examine bias monitoring execution and corrective activities for identified issues.

Real-time Anomaly Detection

Establish monitoring frameworks to detect anomalies in end-to-end AI processes. Audit procedures review supervision indicators and evaluate measures taken to address anomalies.

Recovery Mechanisms for AI Systems

Identify Inefficiencies

Implement continuous monitoring to identify ineffective AI system processes, such as major incidents or inappropriate learning patterns

Activate Reversal

Deploy established reversal mechanisms to correct algorithm problems when inefficiencies are detected

Access Clean Data

Utilize access to "clean" historical data repositories to reset or retrain the system as needed

Verify Effectiveness

Confirm that recovery actions have successfully restored system functionality and performance

Audit procedures should include reviews of processes for identifying ineffective AI systems and assessing historical rollback activities to determine if they adequately addressed system failures. For generative AI models, auditors should also review technical documentation associated with the implemented version or model.

The Human Factor and Algorithmic Bias

Bias Prevention

Detecting and mitigating algorithmic bias

Human Oversight

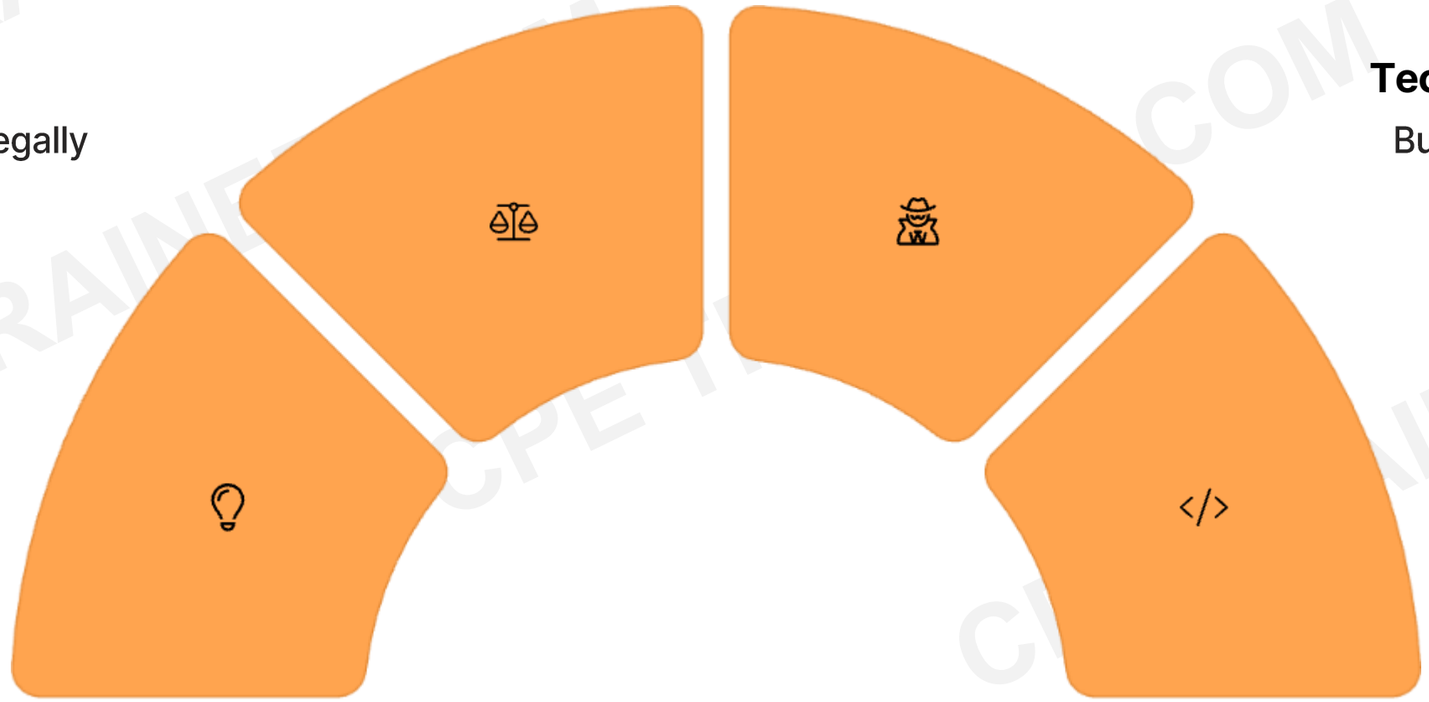
Maintaining appropriate supervision of AI decisions

Ethical Application

Ensuring results are used legally and responsibly

Technical Implementation

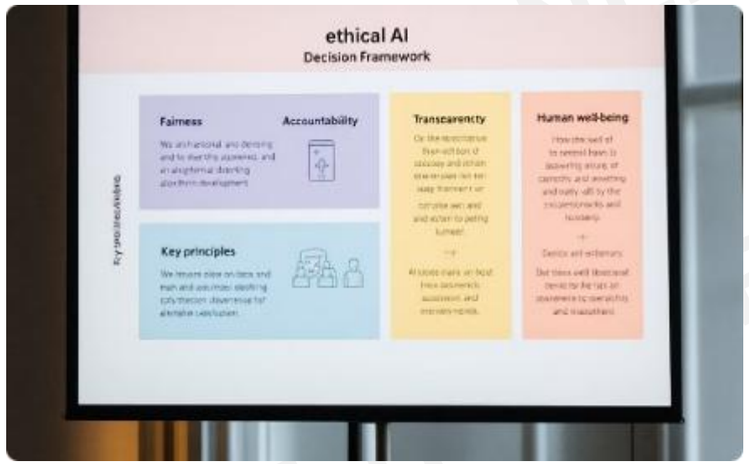
Building systems with bias detection capabilities



The human factor in AI system design, implementation, and maintenance is a critical consideration, particularly for unsupervised self-learning models with potential adverse impacts on society and business processes. Humans develop algorithms, so any error (intentional or unintentional) directly impacts AI system performance and results.

Internal audit functions must consider ethical and moral implications of AI system outputs, ensuring results are used legally, ethically, and responsibly. AI systems should be tested throughout deployment, stabilization, and maturity phases to confirm they continue meeting designed objectives without deviations that compromise organizational principles.

Ethical Considerations in AI Implementation



Ethical Framework Development

Organizations should establish comprehensive ethical frameworks guiding AI development and deployment. These frameworks should outline core principles such as fairness, transparency, accountability, and respect for human autonomy that must be embedded in all AI systems.

Diverse Stakeholder Input

AI ethics committees should include diverse voices from various stakeholders, including technical experts, ethicists, legal professionals, and representatives from potentially affected communities. This diversity helps identify potential ethical concerns from multiple perspectives.

Ethics Training Programs

Organizations should implement ethics training programs for all staff involved in AI development, deployment, and usage. These programs should address ethical dilemmas specific to AI applications and provide guidelines for responsible decision-making.

Bias Detection and Mitigation Controls

Data Source Evaluation

Assess training data sources for potential inherent biases. Audit procedures should include reviewing data collection methodologies and sampling techniques to ensure representative and balanced datasets are used for model training.

Mitigation Strategy Implementation

Develop and apply mitigation strategies when bias is detected, including model retraining, algorithm adjustment, or implementation of compensating controls. Audit procedures should examine documented cases of bias detection and subsequent remediation efforts.

Automated Bias Detection

Implement automated tools and processes for identifying bias in AI models during development and operation. Audit procedures should verify the existence and effectiveness of these detection systems through testing of representative scenarios.

Continuous Monitoring

Establish ongoing monitoring protocols to detect emerging bias as models operate in production environments. Audit procedures should review monitoring frequency, methodology, and response protocols for addressing newly identified biases.

Audit Testing Approaches

Substantive Testing

Substantive testing focuses on direct verification of AI system outputs and operations through:

- Reperformance of model execution with controlled inputs
- Direct validation of algorithm results against expected outcomes
- Statistical sampling of system outputs for accuracy evaluation
- Independent recalculation of critical metrics and measurements

This approach provides direct evidence about system performance but may require significant technical expertise and resources.

Control Testing

Control testing examines the effectiveness of controls designed to mitigate AI-related risks through:

- Review of control design documentation and implementation evidence
- Testing operating effectiveness of key controls
- Evaluation of control owner competence and authority
- Assessment of control monitoring and exception handling

This approach focuses on the control environment rather than direct system testing, potentially offering broader coverage with fewer resources.

Regulatory Compliance Considerations

AI-Specific Regulations

European AI Act, sectoral AI regulations, and emerging global frameworks for AI governance

Data Protection Laws

GDPR, CCPA, and other privacy regulations governing personal data processing

Industry-Specific Rules

Financial services, healthcare, and other sector-specific regulatory requirements

Ethical Guidelines

Voluntary frameworks and industry standards for responsible AI development

Regulatory compliance assessment must precede detailed audit testing. The applicable regulatory framework will vary based on the AI system's purpose, data usage, and implementation context. Auditors should evaluate whether the AI system processes personal data, affects pricing decisions, facilitates market operations, or impacts financial reporting, as these factors trigger specific regulatory requirements.

Key Challenges in AI Auditing

Technical Complexity

The sophisticated nature of advanced AI algorithms creates challenges for auditors without specialized technical knowledge. This may require supplementing internal audit teams with data scientists or AI specialists who can effectively evaluate model performance and identify potential issues.

Mitigation strategies include developing specialized training programs for auditors, creating multidisciplinary audit teams, and establishing partnerships with technical experts within the organization.

Evolving Standards

The rapidly developing landscape of AI governance frameworks and regulations creates uncertainty about compliance requirements. Auditors must stay current with emerging standards while evaluating systems against principles that may not yet be formalized in regulations.

Regular monitoring of regulatory developments, participation in industry forums, and consultation with legal experts can help audit teams navigate this evolving environment.

Evidence Collection

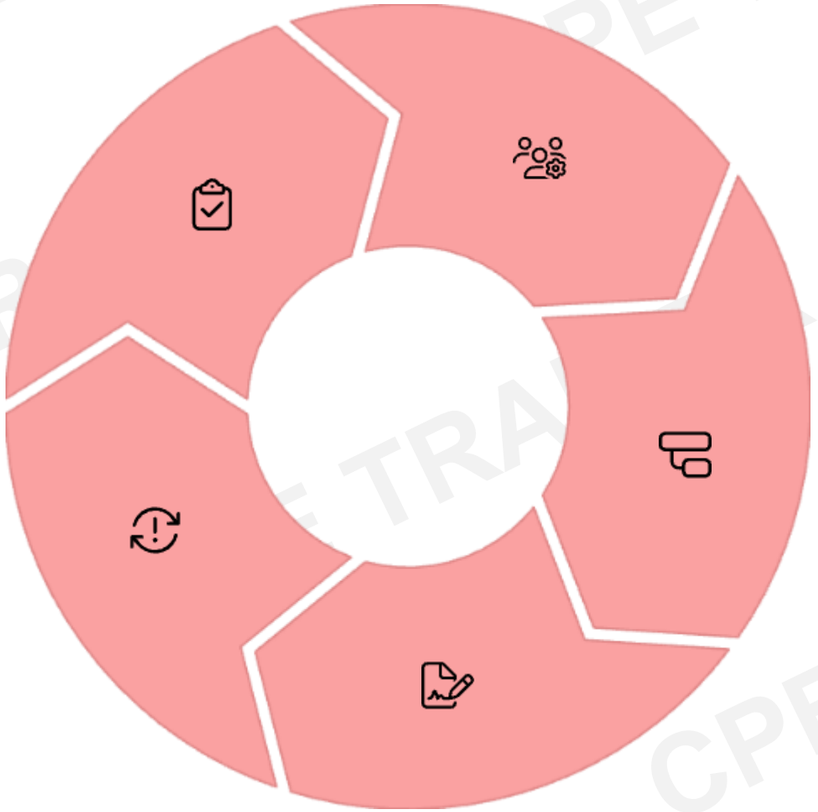
Traditional audit evidence collection methods may prove insufficient for AI systems, particularly when evaluating complex algorithmic decision-making. New approaches to testing and documentation are needed to provide assurance about system behavior.

Implementing specialized testing frameworks, developing AI-specific audit trails, and leveraging automated monitoring tools can enhance evidence quality and relevance.

Next Steps for Implementation

Assess Current State

Inventory existing AI systems and evaluate current control environment



Build Capabilities

Develop audit team skills and acquire necessary technical resources

Develop Audit Plans

Create risk-based audit schedules prioritizing high-risk AI applications

Execute Initial Audits

Conduct first wave of audits focusing on critical AI systems

Refine Methodology

Update audit approach based on lessons learned from initial implementation

Implementing this audit framework requires a strategic approach that recognizes organizational readiness and builds capabilities incrementally. Begin by conducting a comprehensive inventory of AI systems to understand the scope and complexity of the audit universe. Develop specialized skills within the audit team through training and strategic hiring while establishing partnerships with technical experts across the organization.

Interested in a 1-day on-line webinar (7 CPEs)?

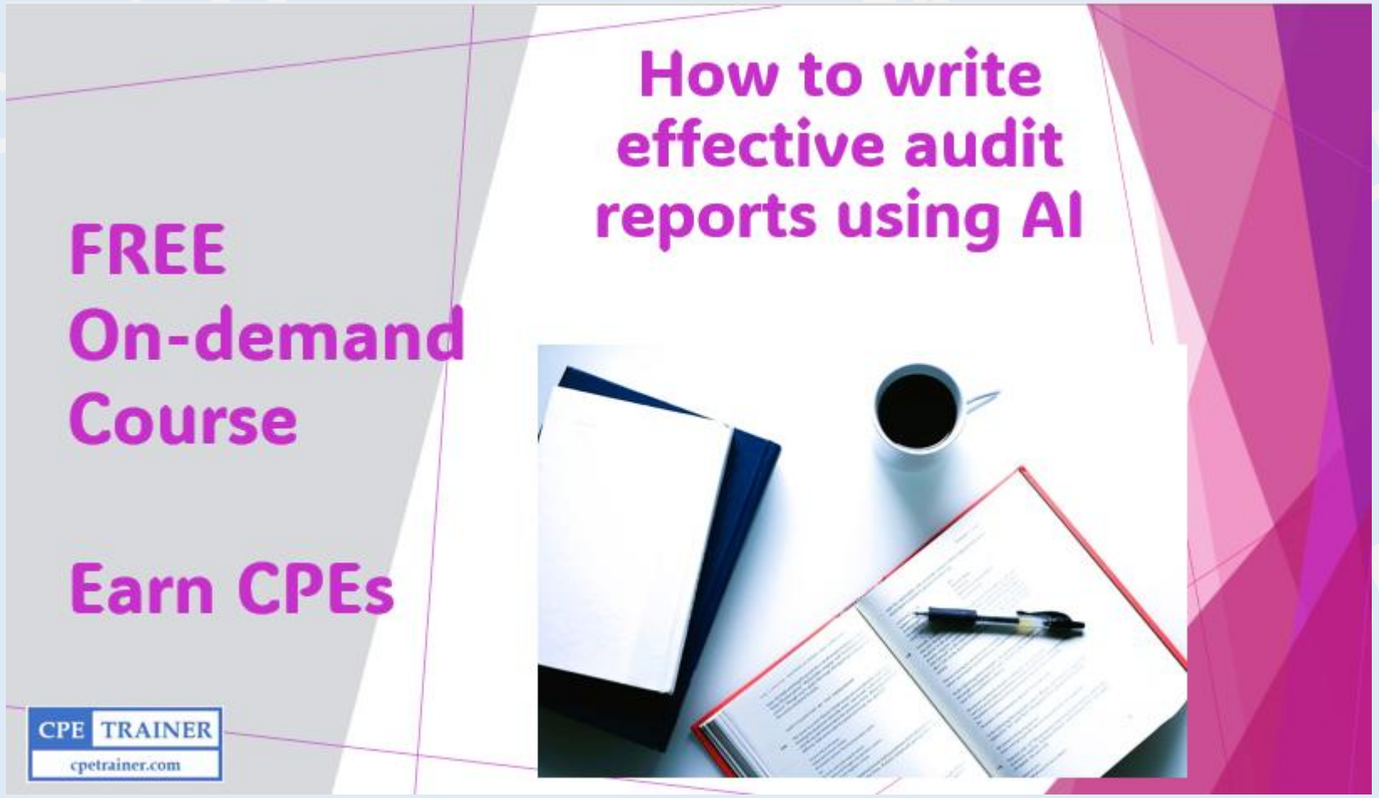
👉 Learn how to build an AI Audit Programme
👉 Implementing & managing AI efforts in an organization
👉 How to establish an AI Governance Policy
👉 Receive a template of AI Governance Policy

✅ Contact the IIA Kazakhstan: IIA-Kazakhstan@iiachapters.org

✅ Earn 7 CPEs!

Interested? Enrol in the FREE On-Demand Video Course

✅ [Enrol here!]



✅ Earn 1 CPE!


CERTIFICATE
Of Completion
is presented to
Amanda Armstrong
For participating in the course
How to Write Effective Audit Reports Using Artificial Intelligence
CPE Credits (1 CPE = 1 hr training): 1.0 (e.g. GARP)
CPE Credits (1 CPE = 50 min training): 1.2 (e.g. IIA, ACFE, ISACA)
June 28, 2024
Isabella Arndorfer
CPE TRAINER
cpetrainer.com

[www.cpetrainer.com]

CPE TRAINER
cpetrainer.com