paradigm shift.

Assurance 2025 – New Content Added for 2025 Workbook

Please note that some chapters do not have any new content for 2025 so the omission of certain chapters in our review below is not an error.

This document is not intended to cover all points in the relevant sections: instead, we just want to give you an overview of the main points.

If you have also purchased access to our Certificate Level subscription package, don't forget to make use of the online quick-fire questions on these 2025 syllabus updates which are provided as part of our Assurance course: the quick-fire questions will get you working with the following content in an active way, which is always the best way to learn!

Chapter 1 Concept of and need for assurance

4.3 Legal and professional requirements

- The Financial Reporting Council (FRC) establishes the UK Corporate Governance and Stewardship Codes, along with standards for accounting, auditing, and actuarial work
- As the designated Competent Authority for Audit in the UK, the FRC issues auditing standards through its Codes and Standards Committee
- The UK government announced plans to abolish the FRC and replace it with the Audit, Reporting and Governance Authority (ARGA), initially anticipated for 2024 per the FRC's 3-Year Plan 2023-2026. However, delays in legislation mean that the ARGA's implementation date remains uncertain
- The FRC's Plan and Budget for 2024-25, released in March 2024, shifted strategic objectives away from focusing exclusively on ARGA's transformation and did not include ARGA implementation within the 2024-2025 timeline
- For exam purposes, it is assumed that the FRC continues as the regulator of the accountancy profession, with no additional details on ARGA's launch
- The FRC's Scope and Authority of Audit and Assurance Pronouncements (March 2023) provides detailed guidance on FRC-issued standards
- FRC standards include engagement standards for audits of financial statements, such as the International Standards on Auditing (ISA® Standards (UK)), and for other public interest assurance engagements, including interim financial reviews and prospective financial information examinations
- The FRC's Ethical Standard applies to financial statement audits, other assurance engagements specified by the FRC, and independent auditor reviews of interim financial information
- Quality management standards are also issued by the FRC, along with additional guidance for auditors in the form of Practice Notes, which help apply engagement standards to specific circumstances, and Bulletins, which offer timely guidance on new or emerging issues

4.7 Overall objectives of the auditor

- Technological advancements have meant that financial statements and the documents underpinning them are increasingly produced by automated processes. The auditor needs to be aware of automation bias
- Automated processes are widely used to produce financial statements, but auditors should be cautious of relying solely on their output
- Automation bias is defined as the tendency for humans to favour suggestions from automated systems and ignore contradictory information, even when the manual information may be correct

- Automated processes may be incorrectly configured, insufficiently tested, or break down, introducing risk and potential for misstatements
- Auditors should exercise professional scepticism when reviewing outputs from automated systems, being mindful of these risks

4.9 Bookkeeping recap

- Under a computerised system entries are made directly into the ledger system
- Modern computerised systems integrate different ledgers (nominal, receivables, and payables) so that entries update automatically, avoiding manual checks for discrepancies
- At the end of the financial period, general ledger accounts are balanced, and a trial balance (TB) is extracted, followed by any adjustments for accruals, prepayments, or errors to produce a final TB
- The statement of profit or loss (SPL) and the statement of financial position (SOFP) are created using the final TB
- Many computerised systems automate these processes, mapping trial balance accounts to relevant headings in the SPL or SOFP, with statutory year-end formatting potentially requiring a separate process

5 Introduction to Sustainability and Assurance

- Investors want to assess how well a company is managing its exposure to long-term ESG risks and assess the value of the company to inform investment decisions
- Investors are increasingly interested in how well companies are managing their Environmental, Social, and Governance (ESG) risks to evaluate long-term financial performance
- Companies' impacts on sustainability can financially affect their reputation, which, in turn, influences consumer demand and financial materiality
- Financially material information for investors includes disclosure topics and sustainability metrics that affect enterprise value
- The concept of double materiality (discussed further in Chapter 3) addresses both the impact and dependencies of sustainability, with different building blocks tailored for investors and broader stakeholders
- The International Federation of Accountants (IFAC) has developed visualisations to guide the creation of effective corporate reports in sustainability
- These visualisations use a "building block" approach, where Block One is designed to meet the needs of investors, and Block Two addresses broader stakeholders, such as consumers, civil society, and employees
- The distinct perspectives of these stakeholder groups on sustainability drive the tailored approach of each building block

- A PDF with full-sized diagrams and commentary on this approach is available on the IFAC website

Chapter 3 Process of assurance: planning the assignment

3.3 Sustainability impact

- Climate-related risks are unique and undiversifiable, affecting all organisations to some degree, and must be considered when determining materiality and performance materiality in line with ISA (UK) 320
- Increasing numbers of investors are factoring sustainability and climate-related information into their economic decisions, including access to green finance, requiring auditors to account for this when determining materiality
- Auditors must consider whether qualitative disclosures on sustainability and climate-related issues are important to users of financial statements, and misstatements in these disclosures can be material
- Materiality in sustainability reporting is an evolving area, and the ISSB IFRS Sustainability Disclosure Standards offer a definition of materiality that suits the broader context of an audit and considers sustainability-related risks and opportunities that affect an entity's prospects
- The traditional view of materiality, focused on risks affecting an entity and its value, aligns with the concept of financial materiality, but sustainability introduces the concept of double materiality
- Double materiality involves assessing both the financial risks created by sustainability issues and the impact of an organisation's activities on people and the environment, with this approach adopted by the EU's CSRD

4.6 Risks in relation to going concern

- Management typically assumes that a company will continue to operate into the foreseeable future and uses the going concern basis when preparing financial statements
- The auditor must assess the risks of the company not being a going concern and plan accordingly during the audit planning stage, following ISA (UK) 570 guidelines
- Auditors are responsible for obtaining evidence about whether a material uncertainty related to going concern exists and whether management's use of the going concern basis for preparing the financial statements is appropriate
- At the planning stage, auditors must conduct risk assessment procedures to understand the entity's environment, financial reporting framework, and internal control systems, and assess how business risks related to going concern are addressed
- Auditors are required to consider the risk of management bias, particularly as it pertains to going concern assessments, and evaluate whether management has remained neutral in the preparation of financial information
- ISA (UK) 570 provides indicators of potential going concern issues, categorised into financial, operating, and other signs that may suggest trouble

    - Financial indicators include net liability positions, reliance on short-term financing, withdrawal of financial support by creditors, negative cash flows, and the inability to pay creditors or comply with loan agreements
    - Operating indicators include intentions to liquidate, loss of key management, significant labour difficulties, loss of major customers or markets, or the emergence of a strong competitor
    - Other indicators include legal proceedings, non-compliance with statutory requirements, or significant regulatory changes affecting the company
- The auditor must gather evidence in relation to management's assessment of going concern after completing the risk assessment

4.7.1 ISA (UK) 315 (Revised July 2020), Identifying and Assessing the Risks of Material Misstatement

- The example that follows demonstrates how business risks can arise from sustainability related dependencies that are adversely affected by climate change
- Business risks can emerge as a result of sustainability-related dependencies being negatively impacted by climate change
- These risks can affect an organisation's ability to operate and may create financial risks as well as reputational damage
- Examples of such dependencies include reliance on specific natural resources or regulatory frameworks that may change due to climate-related pressures
- Failure to address these dependencies effectively can lead to disruptions in operations and impair the company's long-term sustainability and prospects

Chapter 5 Introduction to internal control and information flows

2 Components of a system of internal control

- Businesses prioritise digital transformation and client systems use increasingly complex technologies which the auditor needs to gain an understanding of
- The auditor must exercise professional scepticism when assessing outputs from financial reporting systems that use complex technology to automate processes
- IT systems and controls may be managed by a service provider, and auditors need to assess whether the service provider's control over the data is reliable
- Auditors must understand the technology used by the organisation and how it impacts financial reporting processes and associated risks

2.6 Technological advances

- Organisations use technology to gain a competitive advantage, automate processes, and streamline operations, making digital transformation a priority across all areas, including the financial reporting process
- Digital transformation involves incorporating digital technology across all areas of an organisation, evaluating processes, products, and technology stacks to improve efficiency and speed up market delivery
- The auditor's focus is on digital transformations affecting accounting systems and the financial reporting process
- Key benefits of digital transformation include improved efficiency, automated processes, enhanced security, improved customer satisfaction, and upskilling of employees on emerging technology
- The complexity and size of digital transformation projects can vary, presenting risks such as financial losses due to unforeseen costs, employee resistance, integration difficulties, skills gaps, and outdated technology upon project completion

2.6.1 Robotic Process Automation (RPA)

- RPA automates regular business tasks by capturing and interpreting existing software applications, following programmed instructions in a standardised manner
- Simple RPA actions include opening emails and transferring files, while more complex tasks involve calculations or data extraction from documents and the web
- RPA is effective when processes are standardised with unambiguous rules, involve few exceptions, and require extensive manual work
- Auditors must assess how RPA is used in organisations and test controls to evaluate the effectiveness of the automation in financial processes

2.6.2 Artificial Intelligence (AI)

- AI involves advanced computer systems performing tasks that typically require human intelligence, including learning from data, problem-solving, language processing, and making decisions autonomously
- AI can mimic human cognitive activities such as interpreting speech and images, interacting naturally, gathering information, and forming hypotheses based on data patterns
- Common financial applications of AI include cognitive automation (e.g., cash matching), cognitive engagement (e.g., virtual assistants), and cognitive insight (e.g., dispute resolution)
- Machine learning, a subset of AI, improves AI systems over time by learning from large volumes of data rather than being explicitly programmed
- AI plays an increasingly important role in data analytics, allowing auditors to analyse Big Data for risk assessment, fraud detection, and compliance monitoring
- Generative AI, which creates new content (e.g., texts, images, audio), is becoming more prominent but presents ethical challenges such as data privacy, bias, and transparency issues

2.6.3 Cloud computing and cloud accounting

- Cloud computing provides on-demand access to computing resources, including applications, storage, and servers, managed by a cloud service provider (CSP)
- Cloud computing offers increased flexibility, cost savings, and remote working potential but introduces risks such as loss of control over data and dependency on the CSP's controls for security
- Cloud accounting uses cloud-based software to perform accounting tasks, enabling integration with banking and recognition software for enhanced efficiency
- Risks related to cloud computing and accounting include data security concerns, with auditors required to assess the reliability of CSP controls and document their findings

2.6.4 Digital sign off and digital signatures

- Digital systems, particularly in paperless environments, rely on digital signatures and authorisation systems for approval processes
- A robust digital signature system should include an audit trail or log, capturing critical information such as signers' identities, dates, times, and any changes made to documents
- Auditors must evaluate the integrity of the digital signature systems used by the organisation and assess how secure they are

2.7 Cyber security risks

- Cyber security is a significant concern for organisations, with the World Economic Forum ranking cyber insecurity as the fourth greatest global risk
- Generative AI poses particular risks by helping attackers improve phishing techniques, creating convincing fraudulent communications such as emails or "deepfake" videos

- Remote working increases cybersecurity risks due to more devices and connections being used and the vulnerability of external networks (e.g., home Wi-Fi or public Wi-Fi)
- Organisations should follow the ICAEW's 10 actionable steps to protect against cyber threats, involving allocation of responsibilities, system maintenance, data backups, controlling employee access, and educating staff about risks

2.7.1 AI and Cybersecurity

- Cyber attackers can exploit AI to identify vulnerabilities in client systems and carry out attacks more efficiently and effectively
- Conversely, AI can be central to an organisation's cybersecurity strategy, monitoring and detecting threats, analysing network traffic patterns, and potentially stopping data breaches before they cause damage
- Care must be taken to ensure AI-driven security systems do not infringe on data privacy or raise ethical concerns

2.8 Emerging technology and auditing

- Auditors must understand the technology in place at their client organisations when assessing risks and related controls, employing professional scepticism during this evaluation
- These emerging technologies pose new challenges for auditors, particularly in assessing financial reporting processes and the integrity of controls over automated systems

Chapter 7 Purchases system

3.2 Controls

- The arrangements for controlling payments vary depending on the business nature, payment volume, and company size
- Bank payments include bank transfer requisitions, card payments, and BACS lists, all of which should have supporting documentation like invoices and reports
- Payments must be approved by appropriate staff, with the potential use of manual or digital signatures
- Electronic payment initiation should be handled by appropriate staff members
- Corporate cards should only be issued to approved personnel, ensuring proper control and accountability
- Authority to authorise bank transfers and BACS payments should be designated clearly with authorisers separate from those who prepare the transfers or BACS listings
- Specific authority limits should be set for approval of payments to minimise risk
- Payments must be recorded promptly in the nominal ledger to ensure financial records are up to date

Chapter 8 Employee costs

3.2 Payment of salaries by bank transfer or BACS

- A final report should be generated each month listing all amounts to be paid to employees and reviewed to identify any unusual amounts or unfamiliar employees
- Bank transfer lists should be carefully prepared and authorised to ensure accuracy and proper approval
- A comparison should be conducted between bank transfer/BACS lists and payroll records to ensure consistency
- The wages and salaries nominal ledger account must be maintained and reconciled to ensure records are correct and up to date
- The employee responsible for actioning the payments should not be the same individual who prepared the payroll, ensuring segregation of duties
- If possible, a report should be generated to identify any changes in employee bank details made during the month, and these changes should be verified for authenticity

3.3 Tests of controls

- Inspect the final report summarising all amounts due to be paid to employees for evidence of review and follow up any unusual items
- Review payroll records, postings, and corresponding documentation supporting bank transfers/BACS payments to confirm the employee making the payments did not prepare the payroll
- Review the monthly report of any changes to employee bank details to check for evidence that these changes were reviewed and the reasons for each change were investigated
- For salaries, ensure that comparisons are made between the monthly payroll net pay summary and examine a certified bank list showing payments made to employees via bank transfers

Chapter 10 Documentation

2.1 Automated and electronic working papers

- Most audit firms now use automated or electronic working papers, and a large proportion of audit files are stored electronically, reducing reliance on paper documentation
- Supporting documents are typically scanned and stored electronically, allowing easy retrieval and reducing the risk of losing physical papers or them becoming damaged
- Electronic working papers can be easily backed up, and firms should establish procedures and guidelines to ensure that backup processes happen regularly, preventing loss of data or work
- Remote sharing of electronic working papers, documents, and files within the audit team (e.g., via shared remote access) facilitates collaboration, especially important when working with clients that operate from multiple locations
- All members of the audit team can access an electronic audit file simultaneously, streamlining workflows, while physical files would need to be passed around or shared one at a time

Chapter 11 Evidence and sampling

1.3 Automated tools and techniques

- Automated tools and techniques (ATT) refer to technology that aids in performing risk assessment procedures or obtaining audit evidence
- These tools have evolved due to advancements in data analytics, increasing the automation and speed at which auditors can assess data
- ATTs eliminate the need for manual tailoring, making audit processes more efficient

1.3.3 Data analytics

- Data analytics involves the process of collecting, organising, and analysing large sets of data to identify patterns and gain insights that can inform an organisation's strategic decisions
- Big data refers to datasets that are so large or complex that traditional database software cannot capture, store, manage, or analyse them effectively
- AI has significantly improved data analytics capabilities, allowing auditors and organisations to analyse larger datasets, from more sources, at faster speeds
- Modern data analytics enables organisations to derive insights from vast datasets, driving innovations and productivity improvements
- Audit Data Analytics (ADA) is a subset of automated tools and techniques focusing on analysing, modelling, and visualising data for audit planning and performance
- ADA enhances audit quality by assisting auditors in identifying outliers or high-risk transactions, enabling better risk management and efficiency
- ADA provides the ability to audit entire datasets, allowing for a more comprehensive risk assessment compared to traditional sampling methods
- ADA can be utilised at the audit's planning stage to identify patterns, correlations, and deviations from expected outcomes, guiding further specific risk assessment procedures
- Analytical review techniques, such as heat maps, bar charts, and pie charts with drill-down functionality, can be employed to visualise trends and identify areas needing further investigation
- ADA enables auditors to analyse general ledger data to identify fraud or error risks, such as large, round-sum transactions near period ends
- Relationships between transactions can be analysed to improve auditors' understanding of client systems and detect potential fraud risks, including segregation of duties analysis
- ADA helps automate substantive analytical procedures, reducing manual effort and improving accuracy
- Auditors can apply ADA to analyse all transactions in a population, stratify populations, and identify outliers for further review

- In cases where testing 100% of a population is impractical, ADA supports sample selection and extrapolation of results for substantive testing
- ADA allows auditors to manipulate data to test the impact of different assumptions, such as those made during going concern assessments
- Revenue trends can be analysed by product or region, providing deeper insights into an organisation’s financial patterns

Chapter 13 Substantive procedures – key financial statement figures

3.1 Confirmations from customers

- When it is reasonable to expect a response, auditors should plan to obtain direct confirmation of receivables to individual entries in account balances, as covered by ISA (UK) 505 (Revised October 2023) – External Confirmations
- External confirmations can also be obtained electronically, and they provide reliable documentary audit evidence when sourced directly from a third party outside the client entity
- Although not compulsory, external confirmations are a valuable tool, and auditors should use other procedures to ensure sufficient evidence supports all relevant assertions
- Auditors must ensure that confirmation requests are properly designed to provide evidence on the specified assertions and that responses are sent directly to the auditor
- It is important to ensure undelivered items are returned to the auditor's office, not to the client, for follow-up
- External confirmation: Audit evidence obtained via a direct response to the auditor from a third party, delivered in paper, electronic, or other media, such as web portals or digital interfaces (ISA (UK) 505: para. 6)
- Positive confirmation request: A request where the confirming party responds directly to the auditor, agreeing, disagreeing, or providing information related to the request (ISA (UK) 505: para. 6)
- Negative confirmation request: A request where the confirming party responds directly only if they disagree with the provided information (ISA (UK) 505: para. 6)
- ISA (UK) 505 prohibits the use of negative confirmations in audits conducted under ISAs (UK); the explanatory guidance for negative confirmations in the standard is not applicable in the UK
- Where exceptions occur (i.e., the information confirmed is different from the balance recorded), the auditor must investigate whether these indicate potential misstatements
- The auditor must also assess whether the exception is indicative of fraud, deficiencies in internal control, and how further procedures can provide sufficient appropriate audit evidence (ISA (UK) 505: para. 14-1)

3.1.1 Digital confirmations

- Auditors increasingly use specialist software to help streamline the confirmation process; digital solutions allow client authorisation, response tracking, and automated follow-ups
- ISA (UK) 505 refers to electronic methods such as accessing information held by third parties through digital means, including web portals or software interfaces

4.1 ISA (UK) 505 and bank confirmations

- ISA (UK) 505 (Revised October 2023) provides specific guidance for auditors when confirming information directly with banks, particularly regarding the confirmation of receivables and other balances
- Traditionally, confirmations with banks were carried out via confirmation request letters (bank letters), though electronic methods are now increasingly used
- Electronic platforms allow secure confirmation of balances with banks, once client authorisation has been obtained, and help streamline the process by enabling banks to respond quickly

Chapter 14 Codes of professional ethics and regulatory issues

2.4 Technology-related updates to the IESBA Code

- The IESBA Technology Working Group has undertaken a project to assess the impact of technology on accountants, aiming to ensure that the IESBA Code adequately addresses the behaviour expected of accountants in a tech-driven world
- The project led to several technology-related revisions published in a final pronouncement by IESBA, available online and effective from 15 December 2024
- The revisions include expanded guidance on technology and amendments to the subsections of the Code concerning professional competence, due care, and confidentiality
- The updates also provide additional guidance on how technology use may create threats to compliance with fundamental principles, as well as clarification on applying the Code in the context of these technological challenges

2.4.1 The IESBA Code and guidance on bias

- The IESBA Code addresses the impact of bias, especially automation bias, which may affect professional judgement in identifying, evaluating, and addressing threats to compliance with the fundamental principles (IESBA International Code of Ethics: para. 120.12 A1)
- Automation bias, a tendency to favour outputs from automated systems over human reasoning, even when contradictory information is available, is specifically highlighted in the Code
- A list of potential biases to be aware of when exercising professional judgement includes:
    - Anchoring bias: A tendency to give disproportionate weight to an initial piece of information
    - Automation bias: A tendency to overly rely on automated outputs, disregarding conflicting human conclusions
    - Availability bias: A tendency to place undue emphasis on readily available information or experiences
    - Confirmation bias: A tendency to focus on information that supports pre-existing beliefs while ignoring contradicting data
    - Groupthink: A tendency within groups to suppress individual creativity and reach decisions without critical analysis
    - Overconfidence bias: Overestimating one’s ability to make accurate judgements or assessments
    - Representation bias: Basing conclusions on patterns assumed to be representative
    - Selective perception: Viewing information through the filter of one’s expectations, which can distort objectivity (IESBA International Code of Ethics: para. 120.12 A2)

- To mitigate the effects of bias, the Code advises several actions:
    - Seek advice from experts for additional perspectives
    - Consult with others to introduce challenges during the evaluation process
    - Engage in training on identifying and managing bias as part of professional development (IESBA International Code of Ethics: para. 120.12 A3)

2.2.11 High percentage of fees

- The percentage limits mentioned in the preceding paragraphs apply to both an individual entity or a group of entities and their subsidiaries
- In the 2024 revision of the FRC Ethical Standard (ES), changes were made to ensure that a collection of entities with the same beneficial owner or controlling party (who is not a corporate holding entity) are also subject to the percentage thresholds
- This ensures that a broader scope of entities are captured under the percentage thresholds, regardless of whether they are operating independently or as part of a group with common ownership or control

2.3.7 Information technology services

- The 2024 update to the ES added a new paragraph (5.53) providing specific examples of IT services that could create threats to integrity, objectivity, and independence for auditors
- The additions align with the IESBA Technology-related revisions to the Code, effective from 15 December 2024, as discussed in Chapter 14
- Examples of IT services creating threats include:
    - Acting as the sole access point to financial or non-financial information systems for the entity
    - Taking custody of or storing the entity's data or records, causing the entity's data or records to be incomplete
    - Providing electronic security or backup services, such as business continuity or disaster recovery, for the entity's data or records
    - Operating, maintaining, or monitoring the entity's IT systems, network, or website
- The transfer and retention of electronic data necessary for conducting the audit will not create any threats to independence

2.5.1 Long association of senior personnel with assurance clients

- The revision of the ES in 2024 included the addition of a useful table summarising the required rotation periods for audit partners, Engagement Quality Control Reviewers (EQCRs), and other senior audit staff
- This table is included under Section 3 of the ES, specifically in paragraph 3.22

Chapter 16 Confidentiality

3 Where disclosure is required by the law

- Reporting of suspected money laundering, such as tax evasion, is required to be made to the National Crime Agency
- Disclosure is necessary to comply with the quality review process of a professional body
- The duty to disclose may arise in response to an inquiry or investigation by a professional or regulatory body

Glossary

Artificial Intelligence (AI) is a field dedicated to developing advanced computer systems capable of performing tasks that typically require human intelligence, such as learning, reasoning, sensory processing, language comprehension, and creative functions. AI systems are distinguished by their adaptability, autonomy, and ability to make informed decisions.

Audit Data Analytics (ADA) comprises automated tools and techniques used to analyse, model, and visualise data to support audit planning and execution.

Automated Tools and Techniques (ATTs) involve technology used in risk assessment procedures and to gather audit evidence.

Automation Bias describes the human tendency to rely on automated decision-making system recommendations, even when contradicting correct information provided independently.

Big Data refers to datasets that are too large for conventional database software to capture, store, manage, or analyse effectively.

Cloud Accounting is the practice of conducting accounting functions via cloud-based software, often provided as a service, which allows management and balancing of accounting records remotely.

Cloud Computing enables on-demand internet access to various computing resources, such as applications, servers, storage, and development tools, hosted by a cloud service provider.

Data Analytics is the process of gathering, organising, and analysing large data sets to uncover patterns and insights that organisations can apply to future business decisions.

Digital Transformation is a strategic initiative integrating digital technology across an organisation, aimed at improving operational efficiency and speeding up product delivery by evaluating processes, products, and technology.

Double Materiality considers both sustainability issues posing financial risks to a company and those with material impacts on people and the environment.

External Confirmation provides audit evidence through a direct written response from a third party to the auditor, either in paper, electronic, or digital form, including access to third-party information via web portals or other digital means.

ISSB Materiality requires entities to disclose material sustainability-related risks and opportunities that could impact the entity's outlook, including information that, if omitted or misstated, could influence decisions made by primary users of financial and sustainability reports.

Machine Learning is the capacity of a computer system to learn and improve at tasks based on large datasets, without explicit programming.

A Negative Confirmation Request asks the confirming party to respond only if they disagree with the information in the request.

A Positive Confirmation Request requires the confirming party to respond to indicate agreement or disagreement with the information or to provide the requested details.

Robotic Process Automation replicates manual business processes through programming to follow conditional instructions, running alongside other software rather than replacing it.