ACRA
Accounting And Corporate Regulatory Authority

NO. 1 OF 2025

AUDIT PRACTICE GUIDANCE

DELIVERING QUALITY AUDITS IN A TECHNOLOGY-DRIVEN ENVIRONMENT

Issued on 26 December 2025

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

Technology plays an increasingly crucial role in the business environment and audit landscape. This publication outlines essential factors for Accounting Entities (AEs) and Audit Practitioners to consider in delivering high quality audits in today's digital age.

Comprehensive risk assessment and monitoring processes ensure all relevant technological resources are operating as intended to support an effective System of Quality Management (SoQM). Section 2 outlines key steps to identify and assess technological resources relevant to the SoQM in driving quality audits.

Understanding the audited entities' IT environment is a crucial consideration when determining the nature, timing and extent of audit procedures in financial statements audits. Section 3 discusses how auditors' understanding of the audited entities' IT environment sets the foundation for a robust risk assessment and supports the design of effective audit responses.

Investment in resources plays a significant role in developing digital capabilities and utilising technological advancements in daily work. Section 4 provides information on different established initiatives including grants to assist the profession in progressing with digital transformation.

Looking ahead, technology will become integral to the audit practices. The audit profession must stay abreast of technological developments, manage emerging risks and invest in digital capabilities to ensure they remain relevant in a rapidly evolving environment.

2 SYSTEMS OF QUALITY MANAGEMENT

Introduction

Singapore Standard on Quality Management (SSQM) 1 *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements* require AEs to design, implement and operate a SoQM that facilitates proactive and continuous improvement of audit quality.

SSQM 1.32(f) requires AEs to establish the following quality objective (QO):

> *"Appropriate technological resources are obtained or developed, implemented, maintained, and used to enable the operation of the firm's SoQM and the performance of engagements"*

To achieve this QO, AEs must fully identify all relevant technological resources utilised and assess quality risks (QRs) to design and implement appropriate responses.[1]

[1] SSQM 1.8(b)

Risk Assessment Process

Checkpoint

Has your AE identified all relevant technological resources?

The IT environment encompasses applications, infrastructure, processes, and the personnel responsible for managing and executing those processes. Relevant technological resources include those directly used in, or are essential to support, both practice management and performance of audit engagements.[2]

A single IT application may encompass multiple functionalities, each leveraged by different business process owners and audit tool owners to fulfil varied objectives. Since SSQM components function in an integrated manner, it is crucial to collaborate with the appropriate business process owners and audit tool owners when determining all relevant technological resources, including their associated functionalities.

The following list identifies various technological resources pertinent to the SoQM.

IT applications used in practice management

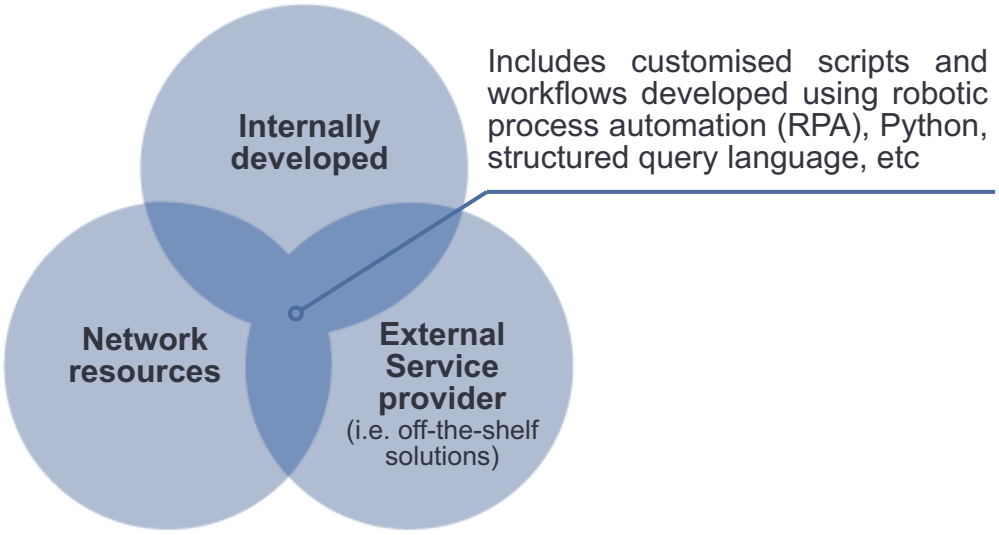
- Independence check system, partners' rotation tool used in relevant ethical requirements component
- Background and conflict check systems used in acceptance and continuance component
- Archival tracking and timesheet management systems used in engagement performance component
- Resource planning, learning management and performance evaluation systems used in human resources component
- Internal corporate communication, such as intranet, used in information and communication component

IT applications used in audit engagements

- Auditing platform with embedded workflows that facilitate the planning and execution of audit procedures
- Software and customised scripts developed to perform re-computation and/or reconciliation procedures
- Digital tools to extract, validate and/or analyse financial data

[2] SSQM 1.A98 and A99

These technological resources may be developed internally, acquired from external service providers, or provided by network firms, as depicted in the diagram below. It is incumbent upon the AEs to engage proactively with the service providers and network firms to attain a comprehensive understanding of the design of these technological resources, determine appropriate usage protocols, and assess any necessary modifications or enhancements to ensure their suitability within the SoQM.



AEs are reminded that they are responsible over the use of network resources in their SoQMs. The deployment of network resources may result in additional QRs and require further policies and procedures to be put in place, particularly in cases where IT infrastructure and readiness vary among network firms.

If specific technological resources are omitted and not monitored, AEs may face unaddressed risks that could compromise audit quality. Therefore, thoroughly identifying and understanding all relevant technological resources is essential when identifying QRs and designing appropriate responses.

Common pitfalls relating to identification of all relevant technological resources

Relevant IT applications used in practice management were often omitted. This has a consequential impact on the identification of QRs, design of key responses, as well as monitoring activities to evaluate the design, implementation and operating effectiveness of the SoQM.

For example, AEs often overlooked the identification of conflict check system that is used across various practices within their AEs. This omission resulted in lack of responses and monitoring activities over independence threats stemming from inaccurate and/or incomplete list of affiliated entities (i.e. corporate family trees) and full suite of non-assurance services rendered to the audited entities.

Checkpoint

Has your AE identified QRs in a comprehensive manner?

A risk-based SoQM is most effective when it considers the specific nature and circumstances of the AE and its engagements. The identification and assessment of QRs relating to technological resources depend on the complexity and phase of deployment, as well as the degree of reliance on external service providers and network resources.

Commonly identified QRs are as follows:

New technological resources are not adequately evaluated prior to deployment

Existing technological resources are not adequately maintained post deployment

Inadequate evaluation and ongoing monitoring of other technological resources provided by external service providers and network firms

Personnel are not familiar with the use of IT applications

Cyber threats that exploit vulnerabilities within the IT environment, leading to unauthorised access and/or changes to the data and IT applications

Checkpoint

Has your AE designed and implemented responses relating to the use of IT applications?

Technological resources should be implemented in a way that maximises audit quality and reduces QRs to an acceptably low level. The list below illustrates common responses implemented by AEs to address the identified QRs above:

Ensure new IT applications are appropriate for use prior to deployment or major modifications

- Certification process governing the design, functionality and use of IT applications
- User acceptance testing (UAT) on all possible scenarios or use cases developed by end-users
- Manage the rollout in a phased approach (e.g. pilot testing on selected engagements)

Ensure existing IT applications continue to operate as intended post deployment

- General IT controls (GITCs) (e.g. access and change management)
- IT helpdesk to provide timely end-user support for IT issues and tickets raised
- Periodic patch management to fix known issues and prevent future occurrences
- Solicit feedback from end-users and monitor adoption rates

Ensure other IT applications from external service providers and network firms are appropriate for use and continue to operate as intended

- Review the network reports on the adequacy of network controls and understand respective member firms' responsibilities to implement additional controls at the local level
- Review the service providers' certification reports (e.g. system and organisation controls (SOC) reports)
- Review the service providers' compliance with service level agreements and key performance indicators
- Periodic meetings with the service providers and network firms to review issues tracker and system updates

Ensure users are familiar with the use of IT applications

- Organise training courses (e.g. hands-on workshops)
- Develop user guides and audit methodology on consideration, execution and documentation requirements (e.g. working paper templates)
- Appoint "champions" to share success stories and user tips on a regular basis

It is essential that engagement teams possess the necessary knowledge to:

- Identify the relevant audit areas in which these IT applications may be used
- Use the IT applications as intended
- Analyse the outputs generated by the IT applications

AEs should only authorise the use of IT applications after all required evaluations have been completed and approved for use by the appropriate personnel and/or engagement teams (i.e. only permit the use of whitelisted tools).[3]

As technology continues to evolve rapidly, IT applications undergo frequent updates or replacements. To meet both current and future needs, AEs should conduct periodic reviews and ensure that their SoQMs remain relevant and responsive to changes in the IT environment.

[3] SSQM 1.A101

Checkpoint

Has your AE designed and implemented cybersecurity controls at enterprise level?

Unauthorised access to the IT environment can compromise confidential information and heighten the risks of data breaches, financial losses, legal consequences and reputational damage. Similarly, unauthorised changes to IT applications may result in these IT applications, along with related policies and procedures, not operating as intended. Such IT incidents can cause significant disruptions to business operations, often leading to downtime and reduced productivity.

Therefore, it is crucial for AEs to establish robust information security risk management frameworks and policies that address cybersecurity threats that can occur within the IT environment of the AE, external service providers and/or network firms.

Some AEs have adopted comprehensive cyber risk assessment frameworks that conform to international and/or local certifications to mitigate risks related to information security, cybersecurity and data protection.

The list below illustrates common responses implemented by AEs to address the identified QR relating to cyber threats in page 6:

Network security

- Firewall
- Virtual private network
- Date encryption at rest (e.g. hard disk, cloud storage)
- Data encryption in transit (e.g. transport layer security)
- Intrusion prevention and detection system
- Vulnerability assessment and penetration testing

Endpoint security for end-user devices
(e.g. laptops, tablets, smartphones)

- Disable universal serial bus ports for file transfers
- Disable web-based file sharing services
- Monitoring of email and/or web activities

Malware / Virus protection

- Anti-malware / Anti-virus software

IT security risk management over external service providers

- Conduct due diligence checks over the service providers (e.g. SOC reports on their information security management)
- Establish the terms of service (e.g. frequency of updates, how do the service providers address confidentiality of data)

Cybersecurity awareness

- Annual cybersecurity trainings
- Simulation exercises

Business continuity management

- Incident response plan
- IT contingency plan
- Periodic data backup and recovery test

Common pitfalls relating to cybersecurity risks and responses

AEs did not identify cybersecurity-related QRs and corresponding responses during the risk assessment process, and consequently, these were not subjected to monitoring activities when evaluating the design, implementation and operating effectiveness of their SoQMs.

Monitoring and Remediation Process

Checkpoint

Has the monitoring and remediation (M&R) team evaluated the design, implementation and operating effectiveness of key responses?

When determining the scope, nature, timing and extent of monitoring activities, M&R team should consider the assessments of QRs, the design of responses and any changes made to the SoQM during the evaluation period. At minimum, AEs should test the following responses:

- Key responses;
- Additional responses that address higher risks;
- New or modified responses in the current year; and
- Responses where exceptions were observed in the prior year.

The testing procedures must extend beyond mere inquiries with the response owner(s). It should also incorporate inspection of documents, reperformance or observation to enable an appropriate evaluation of inputs, assessments and execution by the response owner(s). In addition, the sample size should be calibrated according to the risk rating and frequency of the respective responses. Refer to Section 4.13 of the Audit Regulatory Report 2023 for further guidance on developing an effective testing plan.

Common pitfalls on monitoring activities

Monitoring activities were limited to making inquiries and ensuring the necessary approvals had been obtained from the response owner(s).

- For a UAT on new IT application, M&R team did not check:
  - The functionalities tested were complete
  - The samples tested were representative of the possible scenarios
  - The identified issues were resolved prior to deployment
- For ad-hoc installation of IT applications, M&R team did not review IT department's assessment on the intended use and security management of these IT applications
- Subsequent to these ad-hoc installations, M&R team did not verify whether the stipulated conditions were adhered to (e.g. installation timeframes, authorised personnel)

Common pitfalls on monitoring activities in relation to network resources

There was no evaluation on the monitoring activities undertaken by network firms relating to the reliability and operating effectiveness of network resources to support AEs in their annual SoQM evaluations.

It is imperative that AEs obtain an understanding of the scope, nature, timing and extent of monitoring activities undertaken by network firms, as well as the results of those monitoring activities. This information is essential to determine whether additional monitoring activities, corrective actions or remedial actions are required by each member firm, and the corresponding impact on their annual SoQM evaluations. Refer to Sections 4.28 and 4.29 of the Audit Regulatory Report 2023 for further details on the key expectations regarding the use of network resources.

Checkpoint

Has the M&R team evaluated the findings and deficiencies relating to technological resources?

AEs are required to evaluate findings to determine whether deficiencies exist.[4] In conducting this evaluation, the following factors should be considered:

- Whether the findings impact integrity of data and reliability of IT applications such that they do not operate as intended;
- Whether there are interdependencies among IT applications that could result in pervasive impacts; and
- Whether there are compensating or mitigating responses.

AEs shall investigate the underlying root causes to develop an appropriate remediation plan. The insights gathered serve as important inputs to the SoQM in an iterative manner. For instance:

- In conducting the root cause analysis, AEs may uncover deeper issues that warrant attention or heightened risks; and
- In formulating the immediate, interim or longer term measures, AEs may introduce additional or modified responses to prevent and/or detect similar issues in the future.

The effectiveness of such remediation plan is dependent on whether the remedial actions are most relevant and responsive to the identified issues. Refer to Audit Practice Guidance No. 1 of 2024 for detailed steps to perform a proper root cause analysis and consequently design the appropriate remediation plan.

[4] SSQM 1.40

3 AUDITS OF FINANCIAL STATEMENTS

Introduction

Under the Singapore Standard on Auditing (SSA) 315 (Revised 2021) *Identifying and Assessing the Risks of Material Misstatement*, auditors are required to identify and assess the risks of material misstatement at both the financial statement and assertion levels. This provides a basis for designing and implementing responses to the assessed risks of material misstatement.[5]

Emphasis is placed on the auditor's understanding of the audited entity and its environment, including aspects of the IT environment that are relevant to the information system and the financial reporting process. Further detailed guidance on understanding the IT environment and GITCs can be found in Appendices 5 and 6 of SSA 315 (Revised 2021).

Additionally, SSA 315 (Revised 2021) recognises the auditor's use of automated tools and techniques in carrying out risk assessment procedures and obtaining audit evidence, which forms the basis for identifying and assessing risks of material misstatement.

Based on a thematic review conducted in 2023, automated tools (e.g. data analytics, RPA, optical character recognition) are commonly applied in the areas of risk assessment procedures, substantive procedures (e.g. journal entries test, three-way match) and review of financial statements. Refer to Sections 4.38 to 4.56 of the Audit Regulatory Report 2023 for further details on key considerations and good practices when deploying these automated tools in financial statement audits.

Risk Assessment

Checkpoint

Have you obtained an understanding of the audited entity's information system and processing activities?

Auditors shall obtain an understanding of the audited entity's information system and communication relevant to the preparation of the financial statements. This encompasses an evaluation of how key financial information and transactions are initiated, recorded, processed, corrected as necessary, and reported in the financial statements.[6]

This understanding may be obtained through:

- Engaging with relevant personnel to inquire about the procedures involved, from the initiation to the recording, processing and reporting of transactions;
- Reviewing the audited entity's policies, process narratives and flowcharts; and/or
- Performing walkthroughs by selecting sample transactions and tracing them through the applicable processes in the information systems.[7]

A robust understanding is critical to the identification of risks arising from the use of IT, as ineffective design or operation of the information processing controls and other relevant controls can compromise the integrity of information (i.e. the completeness, accuracy and validity of transactions and other information) in the audited entity's information.[8]

[5] SSA 315.11
[6] SSA 315.25
[7] SSA 315.A136
[8] SSA 315.12(e) and 12(i)

The nature and extent of the risks arising from the use of IT are influenced by the nature and characteristics of the audited entity's information system, which includes the specific IT applications and infrastructure employed to support the business operations. Higher risks arising from the use of IT are typically present when automated application controls are complex and management places substantial reliance on these controls to ensure the effective processing of transactions and/or the integrity of underlying information.[9]

Examples of audited entities that are highly dependent on IT applications include businesses that operate digital platforms (e.g. mobile and web-based applications) to support e-commerce sales, financial services, telecommunication services, online gaming and other activities.

Checkpoint

Have you identified the audited entity's IT applications, IT application controls (ITACs) and GITCs?

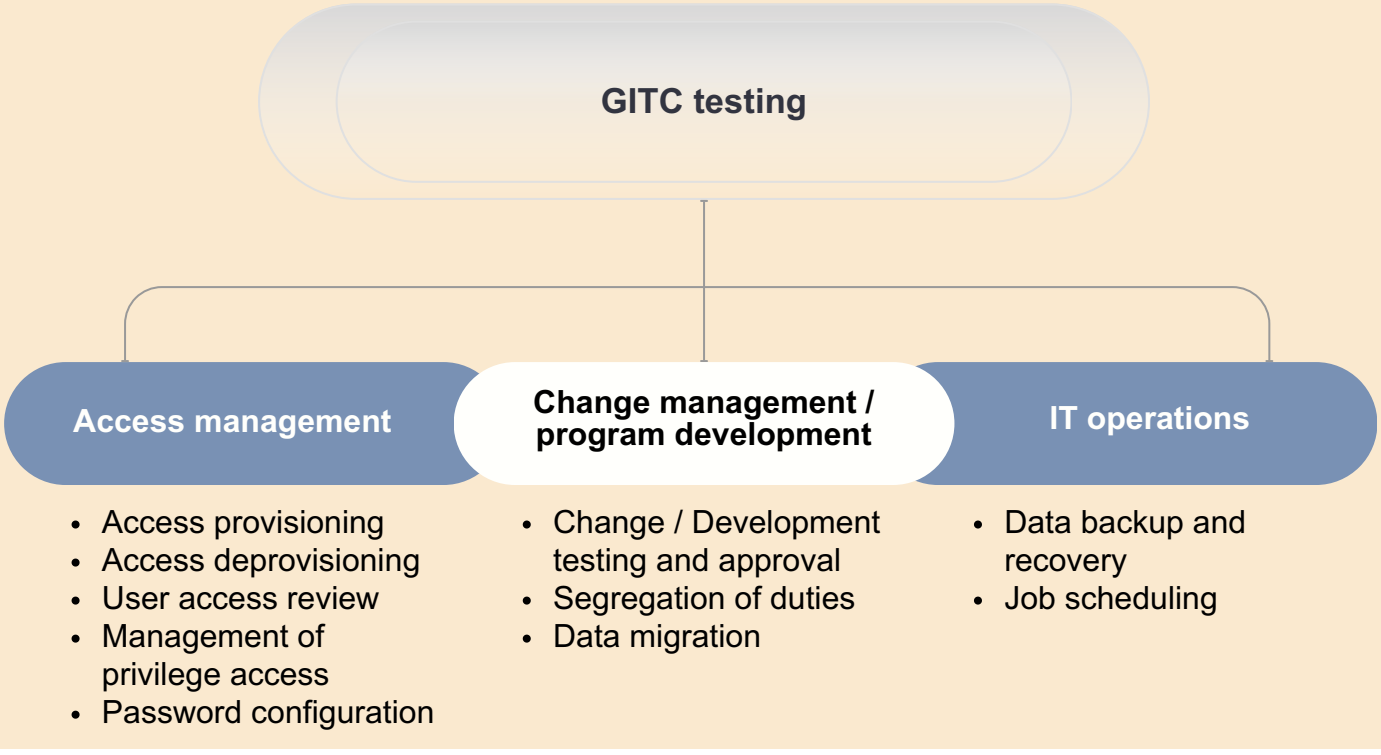
A well-constructed flowchart diagram facilitiates the identification of relevant IT applications and ITACs that may have a direct or indirect impact on the financial reporting process.

Within each IT application, information processing controls may encompass automated computational logic, reconciliations and verifications (e.g. three-way match). These ITACs are designed to address risks to the integrity of information, ensuring the completeness, accuracy and validity of transactions and other information processed within the IT applications.

Where multiple IT applications are involved, it is essential to assess the interface controls to ensure data transfers between these IT applications are both complete and accurate.

Given the audited entity's reliance on automated controls, it is important to ensure that GITCs are operating effectively. These GITCs support the continued functioning of the IT environment, including the information processing controls and the integrity of information within the audited entity's information system.[10]

Testing of GITCs should address the three principal domains illustrated in the diagram below.



[9] SSA 315.A174
[10] SSA 315.12(d)

Checkpoint

Have you reviewed the audited entity's cybersecurity environment?

When reviewing the cybersecurity environment of the audited entity, auditors shall consider the following factors that may have a direct or indirect impact on the financial reporting process:

- The adequacy of cybersecurity controls (e.g. those listed in pages 8 and 9);
- The adoption and use of emerging technologies (e.g. artificial intelligence, machine learning, blockchains);
- Any recent changes to the information systems;
- Any IT-related findings (e.g. internal audits, compliance audits, International Organisation for Standardisation audits); and
- Any IT incidents (e.g. data leakages or breaches occurring within the IT environment of the audited entity or its service providers).

If a security breach is identified, the auditor shall assess the potential impact on the financial reporting process. This involves:

- Obtaining an understanding of the breach;
- Reviewing the design, implementation and operating effectiveness of related controls to determine the possible impact or potential misstatement in the financial statements;
- Determining the nature, timing and extent of further audit procedures necessary to address the related risks; and
- Evaluating whether the audited entity has provided adequate disclosures pertaining to the breach in the financial statements.[11]

Audit Responses

Checkpoint

Have you evaluated the audited entity's design, implementation and operating effectiveness of the relevant GITCs and ITACs?

The auditor shall design and perform tests of controls in accordance with SSA 330 *The Auditor's Responses to Assessed Risks under the following circumstances:*

- When the auditor plans to place reliance on the operating effectiveness of controls in determining the nature, timing and extent of substantive procedures; or
- When substantive procedures alone cannot provide sufficient appropriate audit evidence to address the risks of material misstatement at the assertion level.[12]

[11] SSA 315 - paragraph 19 of appendix 5
[12] SSA 330.8

Where the auditor intends to use system-generated reports as audit evidence, the auditor may either:

- Test the operating effectiveness of controls over the preparation of the reports and the relevant IT applications that are subject to risks arising from the use of IT; or
- Perform substantive procedures on the inputs and outputs of these reports.[13]

In instances where GITC deficiencies are observed, the auditor shall:

- Identify and evaluate any compensating IT control(s) that address the same risks arising from the use of IT; and
- Perform substantive procedures to determine whether these risks have materialised.

If the auditor determines there is insufficient evidence to rely on controls after performing above procedures, they must evaluate the impact on the audit strategy and planned substantive procedures per SSA 330.

Checkpoint

Have you reviewed the use of service organisations that are integral to the audited entity's information system?

A service organisation is defined as a third party organisation that provides services to the audited entity that are part of the audited entity's information systems relevant to financial reporting process.[14]

Examples of such services include custody and management of assets, hosting and operation of e-commerce platforms, cloud computing services, as well as execution of smart contracts on behalf of the audited entities.

If an audited entity uses a service organisation whose services affect how transactions are initiated, recorded, processed, or reported in the financial statements, the auditor shall obtain an understanding of those services and their effect on the audited entity's system of internal control and IT environment, in accordance with SSA 402 *Audit Considerations Relating to an Entity Using a Service Organisation*.[15]

A common approach involves obtaining and reviewing the service organisation's Type 1 and/or Type 2 SOC reports. In doing so, the auditor shall:

- Evaluate the professional competence and independence of the service auditor from the service organisation;
- Evaluate whether the specified date or period in the SOC reports are appropriate for the audited entity's financial reporting period. Where the periods do not align, a bridging letter may be required to cover any gaps that are not addressed by the SOC reports;
- Review the SOC reports for relevant IT applications and controls that may have a direct or indirect impact on the financial reporting process; and
- Perform further audit procedures on complementary user entity controls mentioned in the SOC reports that are relevant to the audited entity.[16]

If the SOC reports highlight any qualifications or deficiencies relating to the service organisation, the auditor shall assess the impact on the overall audit strategy and the planned audit procedures to address the associated risks.

[13] SSA 315.A169
[14] SSA 402.8(e)
[15] SSA 402.3
[16] SSA 402.13 and 14

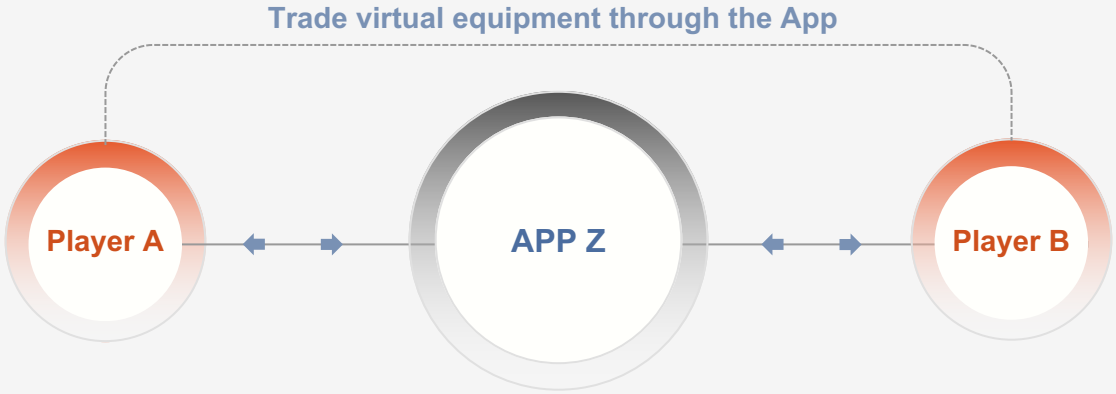
Case studies

The following case studies highlight additional factors that auditors should consider. These considerations may impact the auditor's judgement on the nature, timing and extent of audit procedures to be performed. Auditors are encouraged to review these case studies carefully to ensure that sufficient appropriate audit evidence is obtained to address the assessed risks of material misstatement.

Case Study 1

Background information

The audited entity operates a gaming application, App Z, in which players earn token rewards that can be redeemed for virtual equipment. Additionally, players can purchase virtual equipment or trade items with other players to enhance their gaming experience.



Auditor's evaluation

The auditor has determined that App Z is relevant to the financial reporting process as information relating to material account captions is processed in App Z.

The auditor intends to use system-generated reports as audit evidence. In doing so, the auditor performs substantive procedures on the system-generated reports by:

- Verifying cash receipts from players for the purchase of virtual equipment; and
- Performing substantive analytical procedures for the non-cash transactions (e.g. reasonableness tests on the redemption and trading of virtual equipment).

Additional considerations

Has the auditor obtained sufficient understanding of the relevant controls over non-cash transactions and their impact on financial reporting process?

- What is the volume and complexity of data being processed by App Z?
- What are the mechanisms for setting the redemption, purchase and trading prices within App Z?
- What is the extent of automated computations, report logic and/or parameters used to generate those reports?

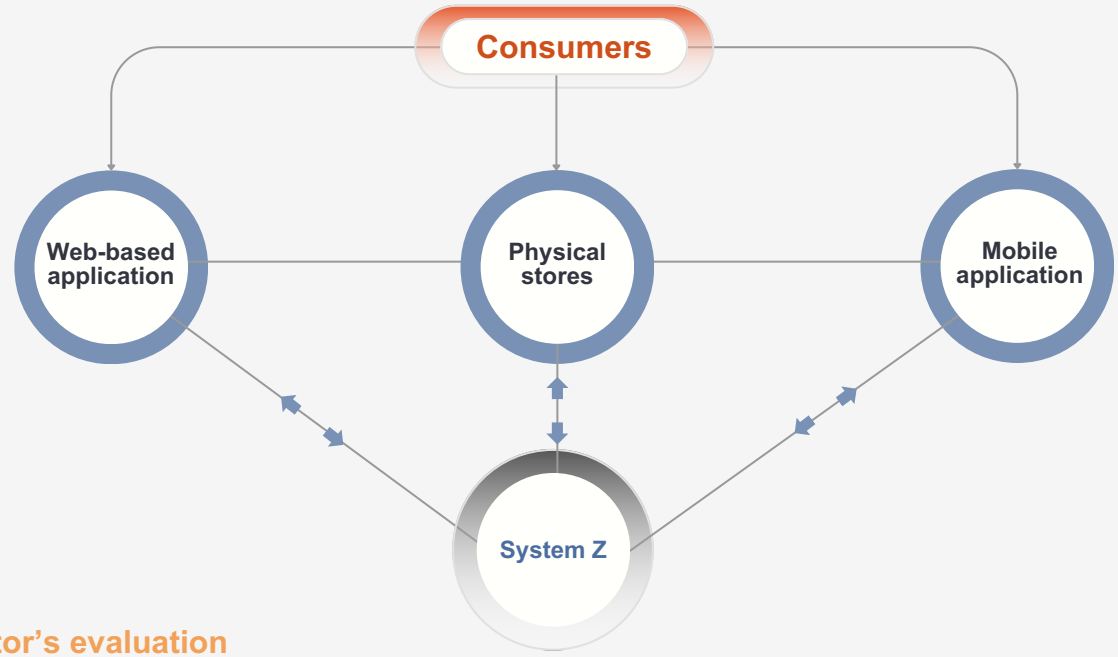
It is important to note that given the audited entity's highly automated business model, substantive procedures alone may not provide sufficient appropriate audit evidence to address the risks of material misstatement.

Case Study 2

Background information

The audited entity operates multiple retail stores. In 20X1 and 20X2, the audited entity launched web-based and mobile applications respectively. The audited entity's primary operating system, System Z, is integrated with both the web-based and mobile applications. Consumers can:

- Purchase items at physical stores, web-based or mobile applications;
- Receive their purchased items via self-collection at physical stores or home delivery; and
- Earn cash rebates that can be used to offset their next purchases.



Auditor's evaluation

The auditor has determined that System Z is relevant to the financial reporting process for the following reasons:

- Information relating to material account captions is processed in System Z; and
- There is reliance on data and reports generated by System Z.

Accordingly, the auditor engaged an IT specialist to review the relevant ITACs and GITCs associated with System Z.

Additional considerations

Given that consumers can initiate and complete purchases via either web-based or mobile applications, has the auditor obtained a sufficient understanding of these applications and their impact on the financial reporting process?

- What is the volume and complexity of data processed through each application?
- What are the mechanisms for setting prices and recording cash rebates?
- How extensive and complex are the interfaces between System Z and the respective applications?
- Have there been any significant changes to the web-based application from 20X1 to 20X2? If yes, do the changes have a direct or indirect impact on the audited entity's financial reporting process?

4 INITIATIVES TO SUPPORT DIGITAL TRANSFORMATION

The AE Survey 2025 shows a 7% rise in AEs using two or more technology solutions, reflecting strong digital adoption. To further support Small and Medium Practices (SMPs) in their digital transformation, the following initiatives and grants are available:

Enterprise Development Grant and Productivity Solutions Grant

Launched by Enterprise Singapore, these grants offer funding support for qualifying projects focused on driving innovation and enhancing productivity, including the automation of current processes through the implementation of IT solutions.

The Productivity Solutions Grant for Accountancy Sector provides funding support for industry specific solutions, such as external audit management, practice management and data analytics.

Chief Technology Officer-as-a-Service

Led by Infocomm Media Development Authority, this programme provides SMPs access to digitial transformation consultants, who provide advisory services at no cost. SMPs will receive tailored recommendations of digital solutions based on their business needs and profiles.

About Accounting and Corporate Regulatory Authority

The Accounting and Corporate Regulatory Authority (ACRA) fosters a vibrant and trusted business environment that enables innovation and growth, contributing towards making Singapore the best place for business.

ACRA regulates the registration of businesses, and their financial and other reporting obligations. We also oversee the public accountancy and corporate service provider sectors. ACRA plays a critical role in developing the accountancy profession, and sets accounting standards for companies and various other entities in Singapore.

For more information, please visit www.acra.gov.sg