Disclaimer

- The materials of this seminar are intended to provide general information and guidance on the subject concerned. Examples and other materials in this seminar are only for illustrative purposes and should not be relied upon for technical answers. The Hong Kong Institute of Certified Public Accountants (The Institute), the speaker(s) and the firm(s) that the speaker(s) is representing take no responsibility for any errors or omissions in, or for the loss incurred by individuals or companies due to the use of, the materials of this seminar conference.

- No claims, action or legal proceedings in connection with this seminar brought by any individuals or companies having reference to the materials on this seminar will be entertained by the Institute, the speaker(s) and the firm(s) that the speaker(s) is representing.

Module C
Business Assurance
MPS on Major or Difficult Syllabus Topics (Part I)

Kattie Kwok

12 October 2017

Seminar Outline

Module C

- HKSA 315 *Identifying and assessing the risks of material misstatement through understanding the entity and its environment*
- HKSA 330 *The auditor's responses to assessed risks*
- IT controls

Questions and answer

HKSA 315 *IDENTIFYING AND ASSESSING THE RISKS OF MATERIAL MISSTATEMENT THROUGH UNDERSTANDING THE ENTITY AND ITS ENVIRONMENT*

HKSA 315

WHY must we obtain understanding?

- To identify and assess the risks of material misstatement (RMM) in the financial statements (F/S) whether due to fraud or error
- To enable the auditor to design and perform further audit procedures
- To provide a frame of reference for exercising audit judgement
- To evaluate sufficient and appropriate audit evidence
- To develop expectations for use when performing analytical procedures

HKSA 315

WHAT do we need to understand?

Entity and its environment (Chapter 8 of LP)

a) Relevant industry, regulatory, and other external factors

b) Nature of the entity

c) The entity’s selection and application of accounting policies

d) The entity’s objectives and strategies, and those related business risks that may result in RMM

e) The entity’s financial performance

HKSA 315

Internal control (chapter 11 of LP)

a) Control environment

b) Entity's risk assessment process

c) Information system relevant to financial reporting

d) Control activities relevant to audit

e) Monitoring of control

HKSA 315

a) Control environment

Overall attitude, awareness & actions of management on internal control system

Factors to consider:

- Management’s integrity & ethical values
- Commitment to competence
- Participation by those charged with governance
- Management’s operating style and style of financial reporting
- Organisation structure – segregation of duties
- Assigning authority and responsibility
- Human resources policies

HKSA 315

b) Entity's risk assessment process

The auditor shall obtain an understanding of whether the entity has a process for:

1. Identifying business risks relevant to financial reporting objectives;
2. Estimating the significance of the risks;
3. Assessing the likelihood of their occurrence; and
4. Deciding about actions to address those risks.

HKSA 315

c) Information system relevant to financial reporting

- Initiate, record, process, and report entity transactions;
- Resolve incorrect processing of transactions;
- Process and account for system overrides or bypasses to controls;
- Transfer information from transaction processing systems to the general ledger;
- Capture information relevant to financial reporting for events and conditions other than transactions; and
- Ensure information required to be disclosed is appropriately reported in the F/S.

HKSA 315

d) Control activities relevant to audit

Authorization

- Transactions should be approved by an appropriate person.

Performance reviews

- Reviews and analyses of actual performance versus budgets
- Comparing different sets of data
- Comparing internal data with external sources information
- Review of functional or activity performance

HKSA 315

Information processing

- General controls
- Application controls

Physical controls

- Physical security of assets for prevention of theft
- Authorization for access to computer programs and data
- Periodic counting and comparison with amounts shown on control records

Segregation of duties

HKSA 315

e) Monitoring of controls

- A process to assess the effectiveness of internal control performance over time
- One possible way of monitoring is through the company's internal audit (IA) function.
- Therefore, the auditor may want to consider using this IA function.
- To do that, auditor will need to first understand the IA function.

HKSA 315

HOW do we obtain those understanding?

- Inquiries of management and others within the entity
- Analytical procedures to highlight areas of high risk
- Observation and inspection of activities and operations of the entity

HKSA 315

Audit risk is the risk that the auditors give an inappropriate audit opinion when F/S are materially misstated.

Audit risk has two elements:

- RMM in the financial statements:
  - Inherent risk is the susceptibility of an account balance or class of transaction to a misstatement that may be material either individually or when aggregated with other misstatements, based on the assumption that there are no related internal controls.

HKSA 315

  - Control risk is the risk that a MM that could occur in an assertion and that could be material, individually or when aggregated with other misstatements, will not be prevented or detected and corrected on a timely basis by the entity's internal control.

- Risk that the auditor will not detect a MM in the F/S
  - Detection risk is the risk that the auditors' procedures will not detect a misstatement that exists in an assertion that could be material, individually or when aggregated with other misstatements.

HKSA 315

Risk assessment

The auditor shall identify and assess the RMM at:

(a) the financial statement level; and

(b) the assertion level for classes of transactions, account balances, and disclosures

to provide a basis for designing and performing further audit procedures.

HKSA 315

(a) Financial statement level

- Management integrity
- Management experience and knowledge
- Unusual pressures on management (i.e. plan to go public, bonuses tied to sales or profits)
- Nature of entity's business
- Industry factors, i.e. special regulations and reporting changes

HKSA 315

(b) Assertion level

- Accounts likely to be susceptible to misstatements
- Complexity of underlying transactions
- Degree of judgment involved in determining account balances
- Susceptibility of assets to loss or misappropriation
- Completion of unusual transactions particularly near the year end
- Transactions not subject to ordinary processing

HKSA 315

Significant risks

- Risk of fraud
- Its relationship with recent developments
- The degree of subjectivity in the financial information
- The fact that it is an unusual transaction
- It is a significant transaction with a related party
- The complexity of the transaction

Evaluate the design and implementation of the entity's controls in that area

HKSA 315

Risks for which substantive procedures alone do not provide sufficient appropriate audit evidence

- Highly automated processing with little or no manual intervention

The entity's controls over such risks are relevant to the audit and the auditor shall obtain an understanding of them.

HKSA 330 *THE AUDITOR'S RESPONSES TO ASSESSED RISKS*

HKSA 330

Overall responses to assessed risks of MM at the financial statement level

- Maintain professional scepticism
- Assigning more experienced staff
- Providing more supervision
- Incorporating additional elements of unpredictability in the selection of further audit procedures to be performed
- Making general changes to the nature, timing, or extent of audit procedures

HKSA 330

Audit procedures responsive to assessed risks of MM at the assertion level

- The auditor shall design and perform further audit procedures whose nature, timing, and extent are based on and are responsive to the assessed risks.

Tests of controls

Tests of controls (CT) are audit procedures designed to evaluate the operating effectiveness of controls in preventing, or detecting and correcting, material misstatements at the assertion level.

Walk-through tests

- To confirm their understanding of the control systems
- Pick up a transaction and follow it through the system

Tests of controls

Circumstances under which CT should be performed

- An expectation that the controls are operating effectively; or

- Substantive procedures alone cannot provide sufficient appropriate audit evidence at the assertion level

Tests of controls

Nature of audit procedures

Perform other audit procedures in combination with inquiry to obtain audit evidence, including:

- How the controls were applied at relevant times during the period under audit;
- The consistency with which they were applied; and
- By whom or by what means they were applied.

Tests of controls

Other audit procedures are performed:

- Inspection of documents
- Inquiries about internal controls which leave no audit trail
- Re-performance of control procedures
- Examination of evidence of management views
- Testing of internal controls operating on computerized systems
- Observation of controls

Tests of controls

Extent of audit procedures

- More persuasive audit evidence, the greater the reliance the auditor places on the effectiveness of a control

Tests of controls

Timing of audit procedures

Period or date to which the audit evidence applies

- Test controls for the particular time, or throughout the period, for which the auditor intends to rely on those controls

Audit evidence obtained during an interim period

The auditor shall:

- Obtain audit evidence about significant changes to those controls subsequent to the interim period; and
- Determine the additional audit evidence to be obtained for the remaining period.

Tests of controls

Audit evidence obtained in previous audits

- Auditor may choose to rely on that evidence for their effectiveness.

- The auditor shall obtain evidence about any change since the controls were last tested and shall test the controls if they have changed.

- Significant risk = shall perform testing in the current year

Tests of controls

Deviations from control

The auditor shall make specific inquiries to understand these matters and their potential consequences, and shall determine whether:

- The CT that have been performed provide an appropriate basis for reliance on the controls;
- Additional CT are necessary; or
- The potential risks of misstatement need to be addressed using substantive procedures.

Substantive procedures

Substantive procedures (ST) are audit procedures designed to detect material misstatements at the assertion level.

They consist of:

- tests of details
- substantive analytical procedures

Overall requirements

- Perform substantive procedures for each material item
- Significant risk = shall perform tests of details

Substantive procedures

Nature of audit procedures

Depending on the circumstances, the auditor may determine that:

- Performing substantive analytical procedures only
- Only tests of details are appropriate
- A combination of substantive analytical procedures and tests of details

Substantive procedures

Substantive analytical procedures

- More applicable to large volumes of transactions
- Auditors should investigate any unusual items deviated from expectation
- Consider any expected relationship and obtain adequate explanations and appropriate corroborative evidence
- Consider any relationships from known conditions
- To apply analytical procedures, information needs to be sufficiently complete and accurate
- Should be applied when controls are more reliable

Substantive procedures

Tests of details

- For testing accounts balances, i.e. existence and valuations

- Objective to obtain sufficient and appropriate audit evidence at the assertion level

Substantive procedures

Extent of substantive procedures

- The extent of ST may depend on the results from CT

Factors to consider when determining the sample size:

- Auditor's assessment of the RMM
- Auditor's desired level of assurance
- The use of other ST to test the same assertion
- Other factors such as the level of tolerable misstatement and the appropriate use of stratification would affect the sample size

Substantive procedures

Timing of substantive procedures

Performing substantive procedures at an interim date

Factors to consider whether to perform ST at an interim date:

- The control environment and other relevant controls.
- The availability at a later date of information necessary for the auditor’s procedures.
- The purpose of the substantive procedure.
- The assessed risk of material misstatement.

Substantive procedures

- The nature of the class of transactions or account balance and related assertions.
- The ability of the auditor to perform appropriate ST or ST combined with CT to cover the remaining period

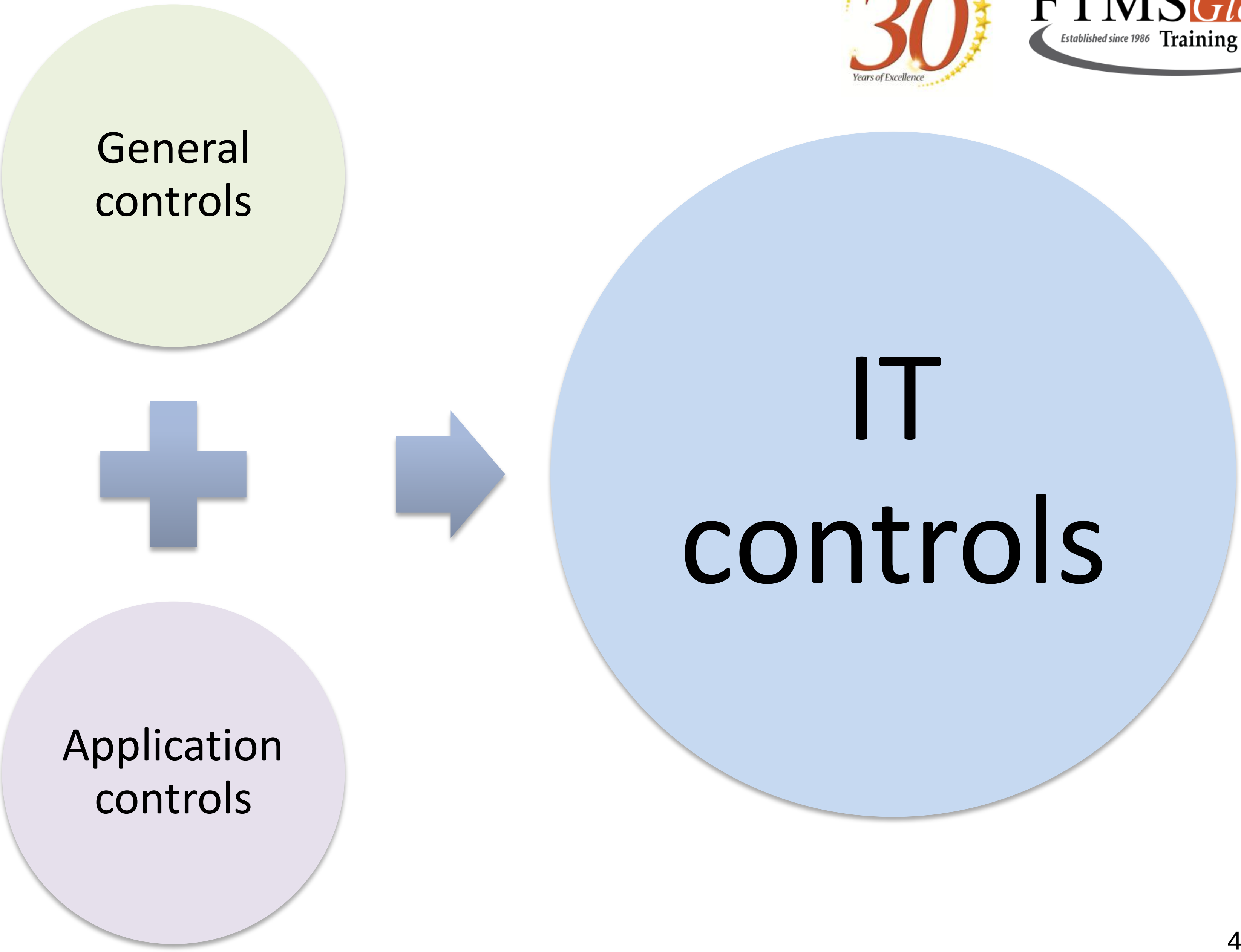
Substantive procedures

Procedures covering the period from the interim date to the period end

If ST are performed at an interim date, the auditor shall cover the remaining period by performing:

- substantive procedures, combined with tests of controls for the intervening period; or
- if the auditor determines that it is sufficient, further substantive procedures only

that provide a reasonable basis for extending the audit conclusions from the interim date to the period end.



General controls

Application controls

IT controls

General controls

It is policies and procedures helping to ensure the continued proper operation of information systems.

They commonly include:

- controls over data centre and network operations
- system software acquisition
- change and maintenance
- access security
- application system acquisition, development and maintenance

General controls

Development of computer applications

- Standards over systems design programming
- Full testing procedures
- Approval by computer users
- Segregation of duties so that those responsible for design are not responsible for testing
- Installation procedures so that data is not corrupted in transition
- Training of staff in new procedures
- Adequate documentation

General controls

Prevention of unauthorized changes to programs

- Segregation of duties
- Full records of program changes
- Password protection of programs so that access is limited to computer operations staff
- Restricted access to central computer by locked doors, keypads
- Maintenance of programs logs

General controls

- Virus checks on software
- Back-up copies of programs being taken and stored in other locations
- Control copies of programs being preserved and regularly compared with actual programs
- Stricter controls over certain programs by use of read-only memory

General controls

Testing and documentation of program changes

- Complete testing procedures
- Documentation standards
- Approval of changes by computer users
- Training of staff using programs

General controls

Controls to prevent wrong programs or files being used

- Operation controls over programs
- Libraries of programs
- Proper job scheduling

General controls

Controls to prevent unauthorized amendments to data files

- Password protection
- Restricted access to authorized users only
- Authorization of jobs prior to processing

General controls

Controls to ensure continuity of operation

- Storing extra copies of programs and data files off-site
- Protection of equipment against fire and other hazards
- Back-up power sources
- Disaster recovery procedures
- Maintenance agreements and insurance

Application controls

- Manual or automated procedures that typically operate at a business process level
- They can be preventative or detective in nature and are designed to ensure the integrity of the accounting records.
- The purpose is to ensure that all transactions are authorized and recorded, and are processed completely, accurately and on a timely basis.

Application controls may be useless when general controls are ineffective

Application controls

Controls over input: completeness

- Manual or programmed agreement of control totals
- Document counts
- Numerical sequence checks with manual follow-up of exception reports
- One-for-one checking of processed output to source documents
- Procedures over resubmission of rejected controls

Application controls

Controls over input: accuracy

- Programs to check data fields on input transactions:
  - Digit verification
  - Reasonableness test
  - Existence checks
  - Character checks
  - Necessary information
  - Permitted range
- Manual scrutiny of output and reconciliation to source
- Agreement of control totals (manual/programmed)

Application controls

Controls over input: authorization

Manual checks to ensure information input was

- Authorized
- Input by authorized personnel

Controls over processing

- Similar controls to input must be in place when input is completed, e.g. batch reconciliations
- Screen warnings can prevent people logging out before processing is complete

Application controls

Controls over master files and standing data

- One-to-one checking
- Cyclical reviews of all master files and standing data
- Record counts and hash totals used when master files are used to ensure no deletions
- Controls over the deletion of accounts that have no current balance