ISOM4300 (L1) - Information Systems Control and Assurance

Fall 2025-2026

L1: Tue Thu 10:30AM - 11:50AM

COURSE INSTRUCTOR	**TA**
Prof. Garvin Percy Dias percy@ust.hk	Sophie Gu imsophie@ust.hk
Room: LSK4037	LSK4065
Ph: 2358 7654	2358 7653
Office Hours: By appointment	

COURSE OVERVIEW

This is the final course for BBA(IS) students who want to pursue their study in the field of IS Auditing. Students will equip themselves with the knowledge of IS Controls; IS Assurance; Systems Security, Efficiency and Effectiveness; Safeguard of Assets; and IT Governance.

Students will also be able to take the Certified Information System Auditor (CISA) examination after taking this course.

Main Topics include:

- Introduction to IT Auditing
- Auditing Change Management
- IT Service Delivery and Support
- Business Continuity and Disaster Recovery
- Protection of Information Asset

COURSE ASSESSMENT and GRADING POLICY

This course will be assessed using criterion-referencing and grades will not be assigned using a curve. The grade for the course will be based on the following weight:

DISTRIBUTION	**%**
Individual Assignments	27%
Midterm Exam	25%
Quiz	20%
Final Exam	28%

Late submission Policy

To ensure fairness for students who submit assignments on time, a penalty for late submission is listed as follows:

- Late submission within 12 hours, 25% penalty will be applied.
- Late submission between 12 to 24 hours, 50% penalty will be applied.
- Late submission for more than 24 hours will not be accepted.

Course AI Policy

You are prohibited from using generative artificial intelligence (AI) to produce any materials or content related to the assessment task.

COURSE SCHEDULE (Tentative)

Date	Lectures	Optional Readings	

Course Introduction			
Sep 2	Introduction CISA Candidate Guide		
Module 1: IS Audit Process			
Sep 4	Introduction to IT Auditing	Internal Audit Charter COBIT 5 ISACA IS Audit Standards and Guidelines Risk Assessment Rules	
Sep 9			
Sep 11	Role Of IT Auditor Review Questions		
Sep 16			
Sep 18			
Module 2: Auditing Change Management			
Sep 23	Auditing Change Management		Assignment 1 release
Sep 25	Auditing Change Management		
Sep 30	Auditing Change Management		

Oct 2			
Oct 7	Public Holiday		
Oct 9	Review Questions		
Oct 14	Review Questions		Assignment 1 Due
Oct 16	Midterm Review		
Midterm Exam			
Oct 21	In class Midterm Exam	Closed book	
Module 3: Auditing IT Service Delivery and Support			
Oct 23	Auditing IT Service Delivery and Support		
Oct 28			
Module 4: Business Continuity and Disaster Recovery			
Oct 30	BCP & DR Notes- Part I		Assignment 2 release
	BIA Questions		

	BIA Questions and Response 1		
	BIA Questions and Response 2		
Nov 4	Business Impact Analysis		
	BIA Questionnaire RTO Exercise		
	BCP Simulation Exercise (HR)		
Nov 6	BCP Preparedness Planner	HKMA: Operational risk management Risk Management of e-banking Business continuity planning General principles for technology risk management	
	FEMA Standard Checklist Criteria for Business Recovery		
	Generic BCP and DR Plan		
	Reviewing BCP		
Nov 11	BCP & DR Notes - Part II		
Nov 13	BCP & DR Notes - Part II (Answers)		
	Trends in Audit Findings Regarding Disaster Recovery Preparations		
Nov 18	BCP and DR Practice Questions		
	BCP & DR Practice Questions (Answers)		Assignment 2 Due

Nov 20	**Supplementary Material**		
Module 5: Protection of Information assets			
Nov 25	Protection of Information assets		
Course Wrap up			
Nov 27	Q&A		

COURSE MATERIAL

ISACA - CISA Review Manual

- **ISACA**

http://www.isaca.orgLinks to an external site.

- **ISACA Hong Kong Chapter**

http://www.isaca.org.hkLinks to an external site.

ACADEMIC HONESTY

Students are required to act truthfully and honestly in their academic pursuit, and acquaint themselves with the University's policy on academic integrity and discipline. It is the policy of the University that there should be zero tolerance for academic dishonesty. Students who are found to have violated the principle of academic

integrity will be subject to academic disciplinary actions. The University Administration will regularly issue to members of the university community the information about nature and action taken on individual academic disciplinary cases.

The HKUST academic integrity site can be accessed at the following URL: https://ugadmin.ust.hk/integrity/index.html

LEARNING OUTCOMES

1. Understand the process of auditing information systems and the importance of providing audit services in accordance with IT audit standards to assist the organization in protecting and controlling information
    - Develop and implement a risk-based IT audit strategy in compliance with IT audit standards to ensure that key areas are included
    - Plan specific audits to determine whether information systems are protected, controlled and provide value to the organization
    - Conduct audits in accordance with IT audit standards to achieve planned audit objectives
    - Report audit findings and make recommendations to key stakeholders to communicate results and effect change when necessary
    - Conduct follow-ups or prepare status reports to ensure appropriate actions have been taken by management in a timely manner

2. Understand formal change management procedures to handle in a standardized manner all requests for changes to applications, procedures, processes, system and service parameters, and the underlying
    - Evaluate different kinds of system changeover techniques to shift various users from using the application from the existing system to the replacing system
    - Evaluate controls for the modified system to determine whether the system has been properly designed and developed
    - The risk associated with software development
    - Evaluate information systems maintenance practices to manage change to application systems while maintaining the integrity
    - Evaluate change management process to determine whether those changes are categorized, prioritized and authorized

- Conduct a review of the change management process to provide management with assurance that the process is controlled, monitored and in compliance with good practices
- Evaluate emergency change procedures to ensure emergency fixes can be performed without compromising the integrity of the system

3. Understand the process of information systems acquisition, development and implementation. Ensure that the practices for the acquisition, development, testing and implementation of information systems meet the enterprise's strategies and objectives.
   - Evaluate the business case for proposed investments in information systems acquisition, development, maintenance and subsequent retirement to determine whether it meets business objectives
   - Evaluate the project management practices and controls to determine whether business requirements are achieved in a cost-effective manner while managing risks to the organization
   - Conduct reviews to determine whether a project is progressing in accordance with project plans is adequately supported by documentation and status reporting is accurate
   - Evaluate controls for information systems during the requirements, acquisition, development and testing phases for compliance with the organization's policies, standards, procedures and applicable external requirements
   - Evaluate the readiness of information systems for implementation and migration into production to determine whether project deliverables, controls and the organization's requirements are met
   - Conduct post-implementation reviews of systems to determine whether project deliverables, controls and the organization's requirements are met

4. Understand information systems operations, maintenance and support. Ensure that the practices for the processes for information systems operations, maintenance and support meet the organization's strategies and
   - Conduct periodic reviews of information systems to determine whether they continue to meet the organization's objectives
   - Evaluate service-level management practices to determine whether the level of service from internal and external service providers is defined and managed
   - Evaluate third-party management practices to determine whether the levels of controls expected by the organization are being adhered to by the provider

- Evaluate operations and end-user procedures to determine whether scheduled and nonscheduled processes are managed to completion
- Evaluate the process of information systems maintenance to determine whether they are controlled effectively and continue to support the organization's
- Evaluate data administration practices to determine the integrity and optimization of databases
- Evaluate the use of capacity and performance monitoring tools and techniques to determine whether IT services meet the organization's objectives
- Evaluate problem and incident management practices to determine whether incidents, problems or errors are recorded, analyzed and resolved in a timely manner
- Evaluate change, configuration and release management practices to determine whether scheduled and nonscheduled changes made to the organization's production environment are adequately controlled and documented

5. Understand and be able to provide assurance that the enterprise's security policies, standards, procedures and controls ensure the confidentiality, integrity and availability of information
    - Evaluate the information security policies, standards and procedures for completeness and alignment with generally accepted practices
    - Evaluate the design, implementation and monitoring of system and logical security controls to verify the confidentiality, integrity and availability of information
    - Evaluate the design, implementation and monitoring of the data classification processes and procedures for alignment with the organization's policies, standards, procedures and applicable external requirements
    - Evaluate the design, implementation and monitoring of physical access and environmental controls to determine whether information assets are adequately safeguarded
    - Evaluate the processes and procedures used to store, retrieve, transport and dispose of information assets (e.g., backup media, offsite storage, hard copy/print data and softcopy media) to determine whether information assets are adequately safeguarded

6. Understand assurance or consulting services to confirm whether the business continuity and disaster recovery management strategy, processes and practices

meet organization requirements to ensure the timely resumption of IT-enabled business operations and minimize the business impact of a disaster

- Evaluate the organization business continuity plan to assess the adequacy and capability to continue essential business operations during the period of an IT or non-IT disruptions
- Evaluate the business continuity management practices to match organization requirements, objectives and budgets
- Conduct the business impact analysis in developing the business continuity plan to determine risk and impact due to all possible events
- Evaluate the recovery strategy with a combination of various measures based on cost, the criticality of the systems or process, and the time required to recover
- Evaluate various business continuity plan testing to determine whether overall preparedness for an actual disaster and the capability of the backup site meet the business requirement
- Evaluate alternate processing sites and backup methods to determine whether the acceptable recovery time and data loss can be met