Certified Internal Auditor® (CIA®) Examination Syllabus
Part 3- Business Knowledge of Internal Auditing

	Proficiency Level
Domain I: Organizational Strategic Planning and Management	**25%**
1. Analyze the organization's strategic planning process and its integration with the risk management strategy, including but not limited to: • business context analysis • objective setting • alternative strategies evaluation • alignment to the organization's mission and values • risk appetite definition • control environment	Proficient
2. Examine how performance measures and controls are used by the organization to monitor the strategic plan and objectives, including but not limited to: • financial • operational • qualitative versus quantitative • productivity • quality • efficiency • effectiveness	Proficient
3. Examine existing organizational behavior (how individuals, groups, and organizations behave; tone at the top; etc.) and performance management techniques and their impact on the organization's culture, including but not limited to: • traits • organizational politics • motivation • job design • rewards • work schedules	Proficient
4. Describe management's effectiveness to lead and its impact on the organization's culture, including but not limited to: • mentoring • coaching • providing constructive feedback • guiding people • building organizational commitment • demonstrating entrepreneurial ability	Basic

The Institute of
Internal Auditors

5. Identify the risk and control implications of different organizational structures, including but not limited to: • centralized versus decentralized • flat versus traditional	Basic
Domain II: Common Business Processes	**45%**
1. Describe business processes and their risk and control implications, including but not limited to: • revenue and expense recognition • asset management • accounting • supply chain management • inventory valuation • accounts payable • procurement • compliance • third-party risk	Basic
2. Identify project management concepts, including but not limited to: • project plan • scope • timing • team • resources • cost management	Basic
3. Identify organizational change management concepts	Basic
4. Explain business continuity and disaster recovery concepts, including but not limited to: • business resilience • incident response plan • business impact analysis • business continuity plan • disaster recovery plan	Basic
5. Recognize crisis management and business response concepts for crises, including but not limited to: • riots • social unrest • natural disasters • adverse media • financial crises	Basic

The Institute of
Internal Auditors

6. Recognize finance and accounting concepts, including but not limited to: • types of financial statements • bonds • leases • pensions • intangible assets • research and development • consolidation • investments • fair value • partnerships • foreign currency transactions • capital budgeting • capital structure	Basic
7. Interpret financial analysis methods, including but not limited to: • horizontal analysis • vertical analysis • ratios related to activity • profitability • liquidity • leverage	Basic
8. Describe data types, data governance, and the value of using data analytics in business processes	Basic
9. Explain the data analytics process, including but not limited to: • define objectives • obtain relevant data • normalize data • analyze data • communicate results	Basic
Domain III: Information Technology	**30%**
A. IT Control Frameworks and Information Security	

• Recognize the purpose and applications of IT control frameworks, including but not limited to:
   • COBIT
   • ISO 27000
   • ITIL
	Basic

•	Explain the purpose and use of common information security and technology controls, including but not limited to:
	    • IT general controls
	    • encryption
	    • firewalls
	    • antivirus
	    • passwords
	    • multi-factor authentication
	    • biometrics
	    • digital signatures
		Basic

•	Recognize principles of data privacy and their potential impact on data security policies and practices	Basic
•	Recognize data governance and data management concepts	Basic

•	Recognize existing and emerging cybersecurity risks, including but not limited to:
	    • hacking
	    • piracy
	    • tampering
	    • ransomware attacks
	    • phishing attacks
		Basic

B. Application and System Software		

1.	Recognize core activities in the systems development life cycle and delivery and the importance of change controls throughout the process, including but not limited to:
	    • requirements definition
	    • design
	    • developing
	    • testing
	    • debugging
	    • deployment
	    • maintenance
		Basic

2.	Recognize the key characteristics of software systems and how they enable business processes and controls (automated and manual), including but not limited to:
	    • customer relationship management [CRM] systems
	    • enterprise resource planning [ERP] systems
	    • governance, risk, and compliance [GRC] systems
		Basic

3.	Recognize the risks related to systems and software integration and interface	Basic

C. IT Infrastructure and Operations	
1. Explain basic IT infrastructure and network concepts and identify potential risks and controls, including but not limited to: • server • mainframe • virtual machines • client-server configuration • gateways • routers • local area network [LAN] • wide area network [WAN] • virtual private network [VPN] • cloud services and models	Basic
2. Describe various IT roles, including but not limited to: • network administrator • database administrator • help desk	Basic
3. Recognize current and emerging technology practices and their impact on the organization and control environment, including but not limited to: • smart devices • internet of things [IoT] • artificial intelligence • blockchain • digital currency and assets • robotic process automation [RPA]	Basic
4. Explain IT processes and procedures in business continuity and disaster recovery, including but not limited to: • incident management • backup • recovery testing	Basic