Ch 12 PARAM

Thursday, 21 March 2024 12:12 AM

Ch 12 PARAM

12 Digital Auditing & Assurance

Part 1- Digital Auditing & Assurance

QNO DAA.100 **Advantages of Auditing Digitally** TITANIUM CNO -- DAA.020 — New Course – (SM23)

Briefly describe the advantages and challenges of Auditing digitally

Answer **Advantages of Digital Audit (Actually it is advantages of auditing digitally)**

(Shortcut -- Quality CARE)

Better Audit Quality: Technology's ability to evaluate large volumes of data quickly enhances audit quality by identifying areas requiring more testing, reducing the risk of overlooked misstatements or issues.

Lower Costs: Automation of previously manual processes reduces the time and cost of auditing.

Better Analytics: Advanced analytics capabilities enable management and auditors to identify trends and patterns, such as potential fraud, which are difficult to detect manually.

Improved Risk Assessment: Automation aids in the audit process and streamlines testing, improving risk assessment. This allows management and auditors to focus on areas with a higher risk of material misstatement and make informed decisions.

Enhanced Effectiveness & Efficiency: Digital audit tools and automation techniques standardize processes and automate routine tasks, such as reconciliation, saving time and costs.

Challenges -

Reluctance to change, challenges with data security and governance, choosing the right tool and automating the right process, ensuring standardisation and correct configurations to avoid error and bias, evaluating business benefits the organization wants to achieve with automation and the roadmap for digital strategy.

Digital Audit → Do audit of IT systems or existing systems → objective how IT usage can be improved.

Auditing Digitally → Using latest technologies to perform audit → Improving audit process

QNO DAA.200 **Stages In Understanding the IT environment.** TITANIUM CNO -- DAA.080 — New Course – (SM23)

What are the stages involved in understanding the IT environment and what key considerations auditor should consider?

Answer The **stages** involved in understanding of IT environment are: Understand – Identify – Assess.

Key Areas for an Auditor to Understand IT Environment

(Shortcut: FAST & Complex)

1. **Understand the Flow of transaction:** Understand the specific IT applications and aspects related to transaction flows and information processing. Recognize how program changes or database alterations affect these flows.
2. **Identification of Manual and Automated Controls:** Recognize the blend of manual and automated components in an entity's internal control. These characteristics impact the auditor's risk assessment of material misstatements.
3. **Identification of Significant Systems:** Recognize IT applications and infrastructure in relation to the flow of significant transaction information within the entity's system.
4. **Identification of the Technologies used:** Comprehend emerging technologies and their role in financial reporting. Evaluate risks from their use and consider involving experts. Emerging technologies include:
- Blockchain (e.g., token issuers, exchanges)
- Robotics
- Artificial Intelligence
- Internet of Things
- Biometrics

- Drones

5. **Assessing the complexity of the IT environment:** Understand that IT applications vary in complexity based on factors like automation, reliance on system reports, customization, business model, yearly changes, and emerging technology adoption. Assess the overall complexity of the IT setting.

QNO DAA.300 **Types of IT Dependencies.** TITANIUM CNO -- DAA.120 — New Course – (SM23)

Auditor should scope in ITGCs to tests when there are IT dependencies identified in the system. Briefly describe the types of IT dependencies.

There are five types of IT dependencies as described below:

(Shortcut: dependencies on CS-AIR)

Calculations: IT systems handle calculations, replacing manual processes. The system might apply a straight-line depreciation formula or calculate an invoice amount based on price and quantity.

Security: The IT environment ensures security and segregation of duties to prevent and detect errors, fraud, or unauthorized process mistakes.

Automated Controls: These controls in the IT environment enforce business rules. Examples include purchase order workflow approvals, specific format checks, non-duplication of customer numbers, and transaction amount limits.

Interfaces: These transfer data between IT systems. An example is moving data from a payroll subledger to the general ledger.

Reports: These are outputs from IT systems used for manual controls, business performance reviews, or by auditors for testing. Examples are vendor master and customer ageing reports.

QNO DAA.400 **Cyber Risk** TITANIUM CNO -- DAA.140 — New Course – (SM23)

What does cyber risk explain it with some examples.

Answer **What is Cyber Risk:**

Definition: A cyber-attack is an unauthorized attempt to access a computing system or network intending to cause damage, steal, expose, alter, disable, or destroy data.

Common Cyber-attacks: The most common types of cyber-attacks include unauthorized access, data theft, exposure, alteration, disabling, or destruction.

Cyber Risk on SIP — MD's ID

Malware

Malware is software designed to harm computers or networks, and includes types like ransomware, trojans, and viruses.

Denial-of-Service (DoS) Attacks:

A Denial-of-Service (DoS) attack floods a network with false requests, disrupting access to services like email and websites. While usually not causing data loss, DoS attacks cost time, money, and resources to resolve.

Phishing:

Phishing is a cyberattack using email, SMS, phone, or social media to trick victims into sharing sensitive information or downloading malicious files, leading to potential viruses on their devices.

Spoofing:

Spoofing involves cybercriminals disguising as trusted sources to access systems, aiming to steal information, extort money, or install malware.

Identity-Based Attacks:

When a user's credentials are compromised, adversaries can impersonate them. For instance, using the same ID and password on multiple accounts can lead to access to unrelated accounts when one is breached.

Insider Threats:

Current or former employees can pose risks to an organization due to their access to the company network, sensitive data, IP, and knowledge of business operations, making them capable of executing attacks.

DNS Tunnelling:

DNS Tunnelling is a cyberattack using DNS queries to bypass security, allowing hackers to transmit data or deploy malware by encoding information in DNS responses.

IoT-Based Attacks:

An IoT attack targets Internet of Things devices or networks, letting hackers control the device, steal data, or add it to an infected group.

QNO DAA.500 **Impact of Cyber Risk** TITANIUM CNO -- DAA.160 — New Course – (SM23)

Sukanya, a CA final student, is of the view that cyber risks are issues of IT and result only in information loss to an entity. She also feels that many cyber-attacks are not directly targeted at financial systems and do not pose risk of material misstatements to financial statements of an entity. Is her view proper?

Answer The cyber risks are not an issue of IT alone. Rather, it is a business risk and has an effect on whole business organization. It affects entity's reputation and can lead to many other consequences which are listed below:-

- Regulatory costs
- Business interruptions causing an operational challenge for an organization.
- Data loss, reputational loss and litigation.
- Ransomware - more common these days where entire systems are encrypted.
- Intellectual property theft which may not only take the competitive advantage, but we may also result in any impairment/impediment charge because of the loss of IP.
- Incident response cost which could be for investigations & remediations
- Breach of Privacy, if personal data of a consumer is hacked it could have a significant impact on the organization.
- Fines and penalties

It may happen that many cyber-attacks are not directly targeted at financial systems. However, the access gained by the attackers may provide them the ability to:

- Manipulate or modify financial records
- Modify key automated business rules
- Modify automated controls relied upon by the management.

Further, auditor should consider whether cyber risk (like other business risks) represents a risk of material misstatement to the financial statement as part of the audit risk assessment activities. Focus should be on understanding the cyber risks affecting the entity and the actions being taken to address these risks.

QNO DAA.600 **Cyber security Framework** TITANIUM CNO -- DAA.180 — New Course – (SM23)

Briefly describe the cyber security Framework

The five pillars of Cybersecurity Framework:

1. Identify the Risk:
This involves understanding what assets you have (data, systems, applications) and what threats they face. Think of it like mapping your valuables and potential entry points for a burglar.

2. Protect the Risk:
Once you know what needs protection, implement safeguards like firewalls, access controls, and encryption. Imagine installing strong locks and an alarm system on your treasure chest.

3. Detect the Risk (Attacks):
Monitor your systems for suspicious activity that could indicate an attack. It's like having cameras and guards constantly watching for intruders.

4. Respond to the Risk:
If an attack happens, have a plan to contain it, minimize damage, and restore normal operations. This is like having a rapid response team to apprehend the burglar and secure the treasure chest.

5. Recover from Risk:
After an attack, analyze what went wrong and improve your defenses to prevent future incidents. Think of it as patching up any weak spots in your security system and training your guards to be more vigilant.

QNO DAA.700 **Advantages and disadvantages of remote audit** TITANIUM CNO -- DAA.220 — New Course – (SM23)

What are the advantages and disadvantages of remote audit?

Answer **Advantages and Disadvantages of remote audit:**

Advantages.

Shortcut: No Selection FEE)

No disruption: The time required to gather evidence can be spread over several weeks, reducing disruption to daily activities.

Selection: Remote audits widen the selection of auditors from a global network of experts.

First-hand evidence: Auditors can obtain first-hand evidence directly from the IT system if direct access is provided.

Flexibility (Enjoy Comfort): The audit team enjoys comfort and flexibility as they can work from a home environment.

Efficiency: Remote audits are cost and time-effective due to the elimination of travel time and expenses.

Disadvantages

(Shortcut: CVICS)

Connectivity: Network issues can interrupt interviews and meetings during a remote audit.

Visualization: There is limited or no ability to visualize the facility culture of the organization or the body language of the auditees. Time zone differences can also affect the efficiency of remote audit sessions.

Integrity: The opportunity for presenting doctored documents or omitting relevant information is increased, potentially requiring additional planning and different audit procedures. This also raises concerns about security and confidentiality violations.

Cultural and Legal Challenges: Auditors may face cultural challenges and a lack of knowledge about local laws and regulations could impact the audit. Certain audit procedures, like physical verification of assets and stock taking, cannot be performed remotely.

Security: Remote access to sensitive IT systems may not be allowed, necessitating an assessment of security aspects related to remote access and privacy.

QNO DAA.800 **Data Analytics** TITANIUM CNO -- DAA.240 — New Course – (SM23)

In an automated environment, the data stored and processed in systems can be used to get various insights into the way business operates. This data can be useful for preparation of management information system (MIS) reports and electronic dashboards that give a high level snapshot of business performance. In view of above you are required to briefly discuss the meaning of data analytics and example of such data analytics techniques.

Data Analytic Techniques.

1A. Data Analytics: Transforming raw system data into meaningful information via processes, tools, and techniques.

1B. Benefits:
- Discovers and analyses data patterns
- Identifies data anomalies.
- Extracts useful information.

2A. Audit Analytics: Analyzing large data to find actionable insights, trends, conclusions, and facilitating informed decisions.

2B. Efficiency in Audit: - Enhances the review process through more accuracy and efficiency.

2C. Improvement in Quality: - Enhances audit quality by allowing effective auditing of large IT data sets.

3. Methods:
- Computer Assisted Auditing Techniques (CAATs): Data analytics tools and visualization methods that increase audit quality.
- Auditors utilize various applications and tools for analyzing large data sets to improve audit quality.

4. Example: ACL
ACL - Audit Command Language (ACL) Analytics is a data extraction and analysis software used for fraud detection and prevention, and risk management. It samples large data sets to find irregularities or patterns in transactions that could indicate control weaknesses or fraud. ACL (Audit Command Language) is used to analyse and check complete data sets to perform Trial Balance reconciliations during the Audits. In such case scenarios, the entity provided the General Ledger dump and system Trial Balance. Using ACL, the completeness of the data can be ensured as the data set exceeded beyond the capacity of the excel and basic functions like record count, sum, pivoting can be performed within ACL where excel could not perform such actions.

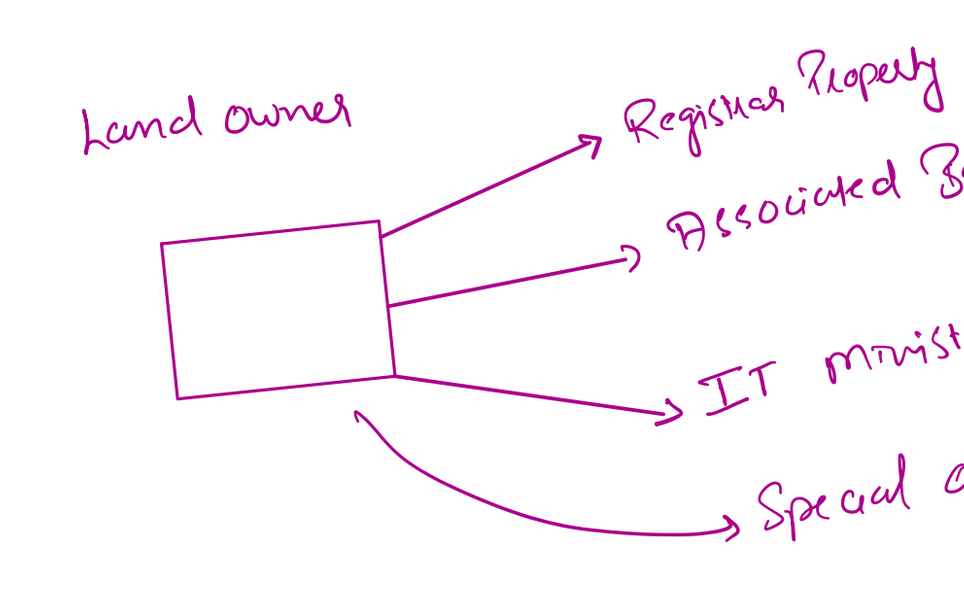
QNO DAA.900 **Examples of automated tools** TITANIUM CNO -- DAA.260 — New Course – (SM23)

Enterprises are adopting emerging technologies at a rapid pace to create synergies and harness the latest technologies. Give 3 examples of automated tools used as a part of emerging technologies along with the risk and audit considerations associated with these tools.

Answer **Automated Tools In Audit**

(Shortcut: BRAIN)

Blockchain
Robotic Process Automation
AI (Artificial intelligence)
Internet of Things
NFT (Non-Fungible Token)



Blockchain
- Decentralized and encrypted ledger.
- Transactions are validated and then replicated to participants.
- Sequential blocks prevent unauthorized modifications.
- Wide-ranging industrial benefits recognized.

Robotic Process Automation
RPA is a software technology that mimics human actions in interacting with digital systems, enhancing process efficiency, customer experience, and control effectiveness. Unlike humans, RPA bots can work continuously with increased speed, reliability, and accuracy.

AI (Artificial Intelligence)
AI allows machines or systems to think and learn using data-driven algorithms.Decisions arise from complex algorithms based on patterns or behaviours acquired over time.

Internet of Things
IoT involves connecting devices, such as cell phones, appliances, and machines, to the internet.

NFT (Non-Fungible Token)
NFTs are unique digital tokens that cannot be exchanged on a one-for-one basis like cryptocurrencies. They represent ownership of unique items, from photos and videos to artwork and collectibles. These digital assets are secured by blockchain, ensuring their uniqueness and authenticity.

QNO DAA.920 **Technological risks** TITANIUM CNO -- DAA.280 — New Course – (SM23)

Emerging technologies can bring great benefits, but they also come with a varied set of substantial risks. Give some examples of technology risks of digital system and the control considerations to consider while assessing technology risk

Answer **Some examples of technology risks where auditors should test the appropriate controls for relying on the digital systems (similar to concept of IT Risk)**

1. Access Control and Authorization:
- The possibility of information technology personnel gaining access privileges beyond those necessary to perform their assigned duties, leading to insufficient segregation of duties.
- Unauthorized access to data that might result in destruction of data or improper changes to data.
- Unauthorized changes to systems or programs.

2. Data Accuracy and Integrity:
- Reliance on systems or programs that are inaccurately processing data, processing inaccurate data, or both.
- Unauthorized access to data that might result in destruction of data or improper changes to data, including the recording of unauthorized or non-existent transactions or inaccurate recording of transactions (specific risks might arise when multiple users access a common database).
- Unauthorized or erroneous changes to data in master files.
- Inappropriate manual intervention.

3. Data Availability:
- Potential loss of data or inability to access data as required.

4. System Maintenance and Updates:
- Failure to make necessary or appropriate changes to systems or programs.
- Unauthorized or erroneous changes to systems or programs.
- Inappropriate manual intervention.

5. Service Providers and External Threats:
- Risks introduced when using third-party service providers.
- Cybersecurity risks.

QNO DAA.940 **Emerging technologies** TITANIUM CNO -- DAA.320 — New Course – (SM23)

Give example of emerging technologies available for Next Generation Audit along with the risks associated with it.

Answer **Drone Technology:** Using drone technology in the remote locations for stock counts. Drones have great payload carrying sensors and cameras, thus they can photograph and physically examine the count of large quantities of fixed assets and inventory.

Augmented reality: The technology allows users to view the real-world environment with augmented (added) elements, generated by digital devices.

Virtual reality: VR goes a step forward and replaces the real world entirely with a simulated environment, created through digitally generated images, sounds, and even touch and smell. Using special equipment, such as a custom headset, the user can explore a simulated world and experience sensations such as flying or skydiving.

Metaverse: The metaverse is the emerging 3-D digital space that uses virtual reality, augmented reality, and other advanced internet technology to allow people to have lifelike personal and business experiences online. It represents a convergence of digital technology to combine and extend the reach and use of Cryptocurrency, Artificial Intelligence (AI), Augmented Reality (AR) and Virtual Reality (VR)

QNO DAA.960 **How to Audit BOT Based System** TITANIUM CNO -- Unique — New Course – (SM23)

A large passenger carrier is having an AI bot for passenger ticket booking with following processes:

User Interaction: The bot interacts with passengers through various channels such as a website, mobile app, or messaging platforms. Passengers can initiate a conversation with the bot by providing their travel details, preferences, and other required information.

Natural Language Processing (NLP): The bot utilizes natural language processing techniques to understand and interpret the passenger's queries and requests. It can process text or voice inputs and extract relevant information to facilitate ticket booking.

Query Handling: The bot responds to passenger queries related to ticket availability, fares, train schedules, seat preferences, and other relevant information. It can provide real-time updates and answers to common passenger questions.

Booking Process: Upon receiving a booking request, the bot collects the necessary details from the passenger, including travel dates, destinations, class preferences, and passenger information. It validates the inputs, checks seat availability, and calculates fares based on the carrier's pricing structure.

Integration with Booking Systems: The bot interfaces with the carrier's booking systems to check seat availability, reserve seats, and process payment transactions. It securely communicates with the backend systems to initiate the booking process.

Payment Processing: The bot facilitates secure payment transactions, allowing passengers to provide payment details and complete the booking. It may integrate with various payment gateways or services to process credit card payments, net banking, or other payment methods.

Confirmation and Ticket Generation: Once the booking is successfully processed, the bot generates a booking confirmation along with a unique ticket number. It provides the passenger with the necessary information, including the ticket details, train information, and any other relevant instructions.

Ancillary Services: The bot may offer additional services such as seat upgrades, meal selection, travel insurance, or other ancillary offerings. It can provide information and assist passengers in availing these services during the booking process.

Post-Booking Support: The bot can assist passengers with post-booking support, including itinerary changes, cancellations, or ticket modifications. It handles these requests, checks the carrier's policies, and processes the necessary changes as per the passenger's requirements.

Integration with Customer Support: The bot may be integrated with customer support systems to escalate complex queries or issues to human agents when necessary. It can provide a seamless transition from automated assistance to human interaction, ensuring a high level of customer service.

How to Audit above BOT Based System?

Answer **1. Audit Preparation:**
- Identify the objectives and goals of auditing the IRCTC ticket booking bot.
- Determine the scope of the audit, including the specific aspects of the bot's functionality and operations to be evaluated.
- Review relevant regulatory and compliance standards applicable to the ticket booking process.

2. Risk Assessment Procedures:
- Verifying compliance with regulations, policies, and procedures.
- Reviewing system architecture, design, and documentation.
- Evaluating security measures: authentication, access controls, and encryption.
- Testing the bot's functionality by simulating scenarios.

- Assessing bot performance: response times, scalability.
- Analyzing logs and audit trails for unusual activities.
- Examining data handling processes for encryption, storage, and data protection.
- Conducting penetration testing or vulnerability assessments.

3. Identify & Assess Risk
- Identify and assess potential risks associated with the ticket booking bot, such as unauthorized access, system failures, or inaccurate booking info.

4. Sampling Methodology:
- Decide on the appropriate sampling methodology for bot evaluation. This may involve selecting representative booking transactions or data for analysis.

5. Execution of Audit:
- Conduct the audit based on defined procedures, adhering to best practices and standards.
- Document findings, noting any issues or areas of improvement.

6. Audit Reporting:
- Compile the audit findings into a comprehensive report.
- Provide recommendations for addressing identified weaknesses, risks, or non-compliance issues.
- Present the report to relevant stakeholders.

7. Post-Audit Activities:
- Track the implementation of recommended actions.
- Ensure appropriate measures are taken to address any identified weaknesses.
- Periodically review and monitor the bot for performance, security, and compliance.

QNO DAA.980 **Case Study on Phishing Attack** TITANIUM CNO -- Unique — New Course – (SM23)

The CEO of a hotel realized their business had become the victim of wire fraud when the accounts payable executive began to receive insufficient fund notifications for regularly recurring bills. A review of the accounting records exposed a serious problem. Upon investigating it was noted that the CEO had clicked on a link in an email that he thought was from the trusted source. However, it wasn't and when he clicked the link and entered his credentials, the cyber criminals captured the CEO's login information, giving them full access to intimate business and personal details.

Answer **Type of Attack:** Social engineering, phishing attack.

A phishing attack is a form of social engineering by which cyber criminals attempt to trick individuals by creating and sending fake emails that appear to be from an authentic source, such as a business or colleague. The email might ask you to confirm personal account information such as a password or prompt you to open a malicious attachment that infects your computer with malware.

Result: The hotel's cash reserves were depleted. The fraudulent transfers amounted to more than ₹1 million. The hotel also contacted a cybersecurity firm to help them mitigate the risk of a repeat attack.

Impact: The business lost ₹ 1 million, and the funds were not recovered. Further there was loss of business reputation too.

Lessons Learned:
– Train the staff about the dangers of clicking on unsolicited email links and attachments, and the need to stay alert for warning signs of fraudulent emails. Engage in regular email security training.
– Implement stringent wire transfer protocols and include a secondary form of validation (Multi Factor Authentication)
– Have a cyber incident response plan ready to implement.

QNO DAA.985 **Audit of a Blockchain-Based Pilot Program** TITANIUM CNO -- Unique — New Course – (SM23)

XY Bank, headquartered in New York, offers a broad range of financial services including asset management, commercial banking, investment banking, and treasury and securities services.

The Five Indian banks in partnership with XY bank, provide a comprehensive range of banking services and products encompassing retail banking, corporate banking, international banking, and other financial services. All these banks have been significant contributors to the digitalization of banking services in India.

Under the pilot programme, the Indian banks will open on-chain Nostro accounts with XY Bank branch in Gift City. The blockchain-based system is expected to facilitate instant, 24x7 settlement between the accounts held at the US bank. Essentially, it will create a private intra-correspondent banking network, redefining the traditional banking hours and enabling seamless money transfer.

Answer The steps for performing an audit of a blockchain based pilot program.

➢ **Preliminary Understanding and Background Checks:**
- Obtain a comprehensive understanding of the blockchain-based pilot program, including its objectives, scope, and key processes involved.
- Review the partnership agreements, contracts, and legal documentation governing the relationship between the Indian banks and XY Bank.
- Identify the specific blockchain technology used, its functionalities, and the underlying smart contracts.

➢ **Assessment of Internal Controls and Security Measures:**
- Assess Internal Controls:
- Review policies and procedures related to the on-chain Nostro accounts, settlement processes, and money transfer mechanisms.
- Assess the governance framework, risk management practices, and compliance procedures established by the Indian banks and XY Bank.

➢ **Review Security Measures:**
- Assess encryption methods, cryptographic key management, and secure transmission protocols used for data protection.
- Review measures taken to prevent unauthorized access, cyber threats, and potential vulnerabilities in the blockchain network.

➢ **Regulatory and Compliance Evaluation:**
- Evaluate Compliance and Regulatory Requirements:
- Review documentation and procedures related to customer due diligence, transaction monitoring, and reporting obligations.
- Ensure that the pilot program adheres to industry-specific standards and best practices.

➢ **Transaction Review and Reconciliation:**
- Test Transaction Validity and Accuracy:
- Validate that transactions are recorded and settled accurately on the blockchain, ensuring adherence to relevant regulations and contractual obligations.
- Perform reconciliations between on-chain Nostro accounts and the corresponding accounts held at XY Bank to confirm the accuracy of balances and transactions.

➢ **Business Continuity and Disaster Recovery Assessment:**
- Assess Business Continuity and Disaster Recovery: Evaluate the adequacy of backup and recovery procedures, redundancy measures, and failover mechanisms to ensure uninterrupted operations.
- Test the effectiveness of these plans by conducting simulations or examining historical incidents and response procedures.

➢ **Reporting and Recommendations:**

- Report Findings and Recommendations: Provide recommendations for improving internal controls, security measures, compliance procedures, and overall efficiency and effectiveness of the pilot program.
- - Communicate the audit results to the relevant stakeholders, highlighting areas of concern and suggesting remedial actions.

QNO DAA.990 **RPA Steps & Benefits** TITANIUM CNO -- Unique — New Course – (SM23)

A company is planning to use Robotics process automation (RPA) to streamline its hiring process. Earlier, the company used to hire from campuses of various management institutes leading to high recruitment costs, inefficient hire yield and resultant lack of diversity. How RPA can be used to automate the hiring process? List out tentative few such steps. What could be likely benefits of using RPA in hiring process?

Answer RPA can be used to streamline hiring process in a company. The tentative steps could include: -

➢ Place advertisements on social media/career advice sites.
➢ Link redirects candidate to a career site.
➢ Career site pulls information of candidate.
➢ An algorithm scans applicants for desired and suitable roles.
➢ Selected candidates may be asked to play online games to assess their skills.
➢ A certain percentage of those applicants are called for a video interview using an interview software.

The automated hiring process will reduce full time effort involvement, provide with a wider assessment range, reduce the impact of recruiter biases, increase the efficiency of mapping of interested candidates, reduce recruiting costs, increase hire yield, reduce time to hire, increase diversity.

QNO DAA.995 **Tests Performed by CAAT** TITANIUM CNO -- Unique — New Course – (SM23)

CA Y is planning to use CAATs extensively in audit of a company-be it for compliance tests or substantive tests. Can you list out examples of few situations (in brief) of tests performed by him using CAATs?

C-ELDER

Answer (i) **Identify exceptions:** Identify exceptional transactions based on set criteria. For example, cash transactions above ₹ 10,000.

(ii) **Identify errors:** Identify data, which is inconsistent or erroneous. For e.g.: account number which is not numeric.

(iii) **Verify calculations:** Re-perform various computations in audit software to verify the correctness of the results from application software confirm with the audit software. For e.g.: TDS rate applied as per criteria.

(iv) **Existence of records:** Identify fields, which have null values. For example: invoices which do not have vendor name.

(v) **Data completeness:** Identify whether all fields have valid data. For example: null values in any key field such as date, invoice number or value or name.

(vi) **Data consistency:** Identify data, which are not consistent with the regular format. For example: invoices which are not in required sequence.

(vii) **Duplicate payments:** Establish relationship between two or more tables as required. For example, duplicate payment for same invoice.

(viii) **Accounts exceeding authorized limit:** Identify data beyond specified limit. For example, transactions entered by user beyond their authorized limit or payment to vendor beyond amount due or overdraft allowed beyond limit.