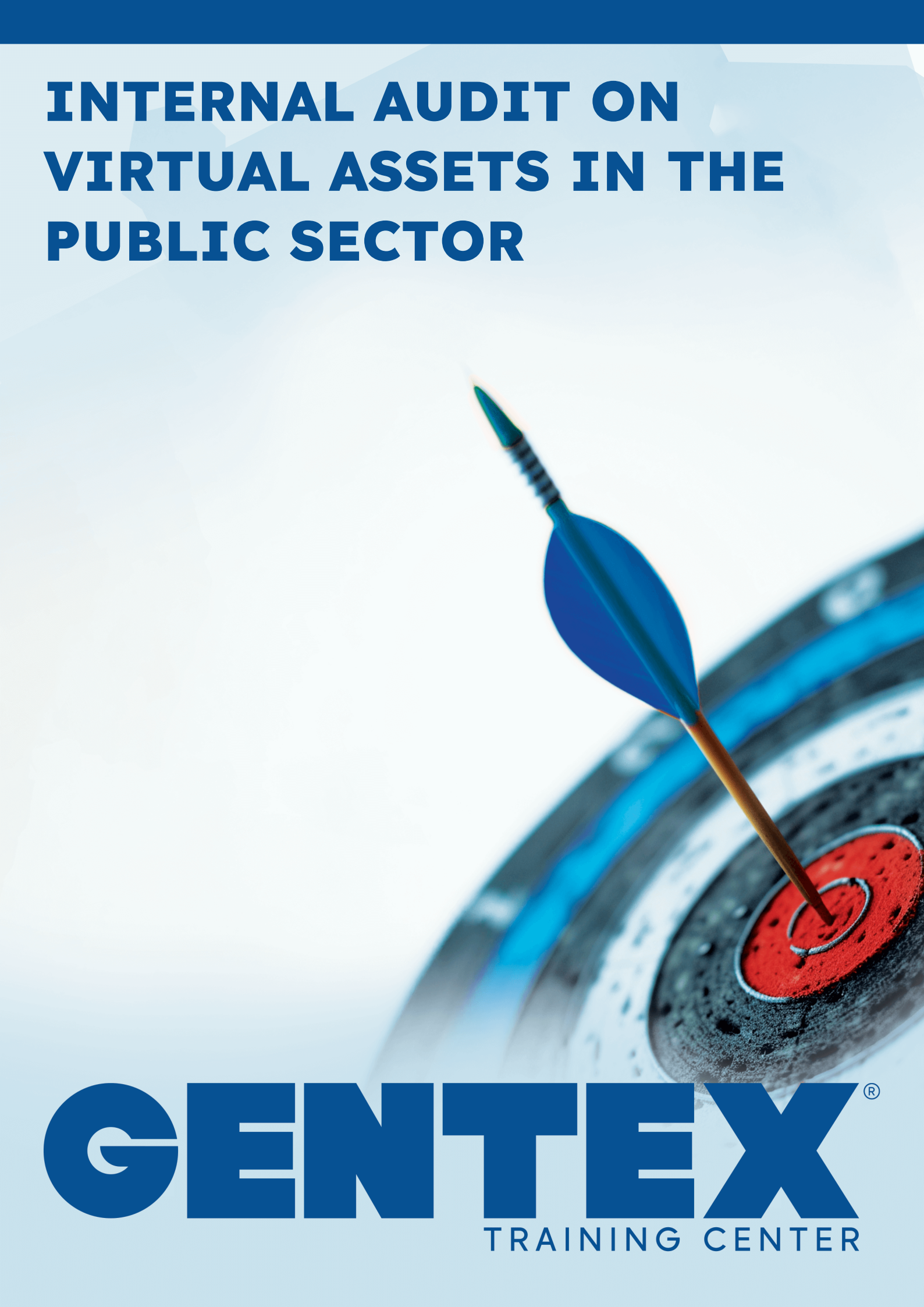
INTERNAL AUDIT ON VIRTUAL ASSETS IN THE PUBLIC SECTOR



GENTEX®
TRAINING CENTER

LEARN BOLD. **LEAD BEYOND**
GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com

Introduction

Internal Audit on Virtual Assets in the Public Sector Training Course prepares public sector auditors to examine crypto-asset activity responsibly and defensibly. Participants work through virtual asset fundamentals, the public sector use cases and mandates, custody and wallet controls, exchange and counterparty risk, AML, CTF and sanctions screening, valuation and accounting treatment, cybersecurity and key management, and reporting to audit committees and legislatures as one connected discipline. The programme links the risk a public body takes when it touches virtual assets with the controls and evidence that keep it accountable. As a result, learners gain a practical, current audit method. Furthermore, the course strengthens technology literacy, risk judgement, and accountability reporting.

Internal Audit on Virtual Assets in the Public Sector Course Objectives

- Explain virtual asset types, blockchain basics, and their public sector relevance.
- Apply the IIA International Standards to virtual asset audits.
- Identify public sector use cases, mandates, and policy frameworks.
- Audit custody, wallet, and private key management controls.
- Audit exchange, broker, and counterparty arrangements.
- Apply AML, CTF, and sanctions screening to virtual asset flows.
- Apply valuation, accounting, and disclosure treatment.
- Audit cybersecurity, key management, and access controls.
- Apply fraud, seizure, and forfeiture risk assessment.
- Apply findings development, reporting, and accountability practice.

Course Methodology

- Interactive sessions built on virtual asset audit and control cases.

GENTEX® TRAINING CENTER

- Workshops on wallet controls, screening, and valuation review.
- Group exercises on transaction analysis, custody testing, and risk assessment.
- Hands-on practice with audit programmes, wallet schematics, and checklists.
- Simulation of a virtual asset custody audit and a seizure review.
- Facilitator coaching and peer review on personal virtual asset audit plans.

Who Should Take This Course

- Internal auditors in ministries, agencies, and public bodies.
- Public sector IT, security, and digital transformation staff.
- Finance officers handling virtual asset holdings or transactions.
- Compliance and AML officers in public entities.
- Regulators and supervisors covering virtual asset activity.
- Consultants advising on virtual asset governance and audit.

Internal Audit on Virtual Assets in the Public Sector Course Outlines

Day 1: Virtual Asset Fundamentals and Public Sector Context

- Virtual asset types: cryptocurrencies, stablecoins, and tokens.
- Blockchain basics: wallets, addresses, and transactions.
- Public sector use cases and mandates.
- Policy and regulatory frameworks for virtual assets.
- Risk taxonomy: market, credit, custody, and conduct risk.

- Governance and accountability for public virtual assets.
- Case discussion: a public body holding assets it could not control.

Day 2: Custody, Wallets, and Key Management

- Custody models: self-custody, third-party, and hybrid.
- Hot, warm, and cold wallet architecture.
- Private key generation, storage, and backup controls.
- Access control, multi-signature, and approval workflows.
- Segregation of duties for wallet operations.
- Physical and environmental controls for key material.
- Workshop: auditing a wallet and key management architecture.

Day 3: Transaction, Exchange, and Counterparty Risk

- Exchange, broker, and OTC counterparty arrangements.
- Counterparty due diligence and licensing checks.
- Transaction verification, reconciliation, and blockchain analysis.
- On-chain analytics tools and tracing techniques.
- Valuation, pricing sources, and fair value review.
- Accounting treatment and disclosure obligations.
- Exercise: testing a virtual asset transaction and its valuation.

Day 4: AML, Sanctions, Cybersecurity, and Seizure

- AML, CTF, and travel rule requirements for virtual assets.
- Wallet and address screening against sanctions lists.
- Red flags in virtual asset transactions and mixing.

- Cybersecurity, phishing, and social engineering risks.
- Seizure, forfeiture, and asset recovery controls.
- Insurance, insurance limits, and loss reporting.
- Simulation: screening a transaction and reviewing a seizure.

Day 5: Reporting, Governance, and Accountability

- Structuring findings with criteria, cause, effect, and impact.
- Root cause analysis for custody and control failures.
- Reporting to audit committees, executives, and legislatures.
- Public transparency and disclosure practice.
- Recovery action, remediation, and follow-up.
- Regulatory change monitoring in virtual assets.
- Capstone: presenting a virtual asset audit report and recommendations.

Conclusion

By successfully completing Internal Audit on Virtual Assets in the Public Sector, participants will gain a practical command of virtual asset fundamentals, custody and key management controls, transaction and counterparty risk, AML, sanctions and cybersecurity requirements, valuation and accounting treatment, and accountability reporting. They will acquire skills in wallet control review, blockchain analysis, screening practice, and technology-aware findings that protect public assets. Gentex Training Center designs the programme to help professionals audit virtual assets in the public sector with confidence.

FAQs

GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com

Q1 What is the "Internal Audit on Virtual Assets in the Public Sector" course about?

It prepares public sector auditors to examine crypto-asset activity responsibly and defensibly. The course spans virtual asset fundamentals and context, custody, wallets and key management, transaction, exchange and counterparty risk, AML, sanctions, cybersecurity and seizure, and reporting, governance and accountability.

Q2 What are the key benefits of the "Internal Audit on Virtual Assets in the Public Sector" course?

You gain a practical, current audit method that links the risk a public body takes with virtual assets to the controls and evidence that keep it accountable. The course improves custody and key management testing, strengthens transaction and counterparty analysis, sharpens AML, sanctions and cybersecurity review, and gives you valuation and accountability reporting that supports public scrutiny.

Q3 What skills will I gain from the "Internal Audit on Virtual Assets in the Public Sector" course?

You will develop four core skills: virtual asset custody and key management control testing, transaction verification with blockchain analysis techniques, AML, sanctions and cybersecurity assessment for virtual asset flows, and virtual asset findings development with valuation review and accountability reporting.

GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com

Q4 What tools, methods, or standards are covered in the "Internal Audit on Virtual Assets in the Public Sector" course?

The course covers virtual asset types including cryptocurrencies, stablecoins and tokens, blockchain basics of wallets, addresses and transactions, public sector use cases and mandates, policy and regulatory frameworks, the risk taxonomy of market, credit, custody and conduct risk, governance and accountability for public virtual assets, custody models of self-custody, third-party and hybrid arrangements, hot, warm and cold wallet architecture, private key generation, storage and backup controls, access control, multi-signature and approval workflows, segregation of duties for wallet operations, physical and environmental controls for key material, exchange, broker and OTC counterparty arrangements, counterparty due diligence and licensing checks, transaction verification, reconciliation and blockchain analysis, on-chain analytics tools and tracing techniques, valuation, pricing sources and fair value review, accounting treatment and disclosure obligations, AML, CTF and travel rule requirements, wallet and address screening against sanctions lists, red flags in virtual asset transactions and mixing, cybersecurity, phishing and social engineering risks, seizure, forfeiture and asset recovery controls, insurance limits and loss reporting, findings structured with criteria, cause, effect and impact, root cause analysis for custody and control failures, reporting to audit committees, executives and legislatures, public transparency and disclosure practice, recovery action, remediation and follow-up, and regulatory change monitoring in virtual assets.

GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com

Q5 How is the "Internal Audit on Virtual Assets in the Public Sector" course applied in real-world practice?

Participants apply it to real work such as auditing a wallet and key management architecture, reviewing custody and multi-signature arrangements, testing a virtual asset transaction and its valuation, screening addresses against sanctions lists, reviewing seizure and forfeiture controls, and drafting technology-aware findings for an audit committee. The same methods support regulatory change monitoring and remediation follow-up.