Certificate in Financial Fraud Risk Management

Module 1: Foundations of Financial Fraud

- Meaning, characteristics and consequences of financial fraud.
- Distinguishing fraud, error, negligence, misconduct and commercial loss.
- Internal, external and collusive fraud.
- Occupational fraud, asset misappropriation, corruption and financial-statement fraud.
- Customer, employee, intermediary and third-party fraud.
- Fraud triangle: pressure, opportunity and rationalisation.
- Management override and abuse of authority.
- Financial, operational, regulatory and reputational consequences.
- Fraud-risk management versus fraud investigation.
- Responsibilities and boundaries of financial-services professionals.
- Red flags as indicators requiring review—not proof of fraud.

Module 2: Fraud-Risk Governance and Organisational Culture

- Board and senior-management oversight.
- Fraud-risk policies and accountability.
- Roles of business teams, risk, compliance, internal audit and specialist investigators.
- Fraud-risk committees and escalation structures.
- Risk appetite and tolerance for control weaknesses.
- Codes of conduct and employee declarations.
- Conflicts of interest and related-party relationships.
- Incentives, sales pressure and misconduct risk.
- Management override and exceptions to policy.
- Whistleblowing and protection against retaliation.
- Fraud-awareness training and communication.
- Management reporting and oversight of remediation.

Module 3: Fraud-Risk Assessment

- Identifying fraud risks across products, processes and customer journeys.

- Process mapping and identification of vulnerable activities.
- Inherent risk, control effectiveness and residual risk.
- Likelihood, impact and risk prioritisation.
- Fraud scenarios and scheme-based assessment.
- Customer, employee, product, channel and geographic risk factors.
- Collusion and circumvention of controls.
- Fraud-risk registers and risk-control matrices.
- Assessing new products, distribution arrangements and outsourcing.
- Using incidents, complaints and near misses to update assessments.
- Risk indicators, ownership and review frequency.
- Documenting assumptions and assessment limitations.

Module 4: Internal Controls and Fraud Prevention

- Preventive, detective and corrective controls.
- Segregation of duties and incompatible responsibilities.
- Maker–checker controls and approval hierarchies.
- Delegation of authority and transaction limits.
- Independent verification and callback procedures.
- Access controls and privileged-user oversight.
- Reconciliations and exception reporting.
- Vendor and beneficiary master-data controls.
- Physical and digital safeguarding of assets.
- Employee screening, role rotation and mandatory leave.
- Control design versus operating effectiveness.
- Compensating controls for smaller organisations.
- Testing controls and addressing recurring exceptions.

Module 5: Identity, Onboarding and Account-Related Fraud

- Identity theft, impersonation and synthetic identities.
- Forged, altered and inconsistent onboarding documents.
- Customer identification and beneficial-ownership verification.
- Remote onboarding and identity-verification vulnerabilities.
- Account takeover and unauthorised profile changes.
- Mule accounts and suspicious account networks.
- Dormant-account abuse.
- Misuse of powers of attorney and authorised signatory arrangements.

- Unusual changes to contact, address or bank details.
- Source-of-funds and customer-profile inconsistencies.
- Enhanced verification and escalation.
- Distinguishing fraud controls from broader KYC and AML obligations.

Module 6: Payment, Transaction and Treasury Fraud

- Unauthorised and deceptively induced payments.
- Business-email compromise and executive impersonation.
- Invoice substitution and beneficiary diversion.
- Card, internet-banking, mobile-banking and UPI-related fraud scenarios.
- QR-code manipulation, phishing links and deceptive payment requests.
- Unauthorised mandates and recurring-payment abuse.
- Duplicate payments and manipulated refunds.
- Cheque and payment-instrument fraud.
- Treasury dealing and settlement irregularities.
- Reconciliation breaks and suspense-account abuse.
- Independent verification of payment instructions.
- Immediate escalation, payment recall and recovery coordination.
- Limits of recovery and the importance of timely action.

Module 7: Lending and Credit Fraud

- Fraud risks across origination, appraisal, disbursement and monitoring.
- Misrepresentation of income, assets, liabilities and repayment capacity.
- Fabricated financial statements and supporting documents.
- Manipulated bank statements, invoices and transaction records.
- Multiple financing and undisclosed borrowing.
- Collateral overvaluation and defective security documentation.
- Diversion of funds and misuse of loan proceeds.
- Related-party transactions and circular fund flows.
- Borrower–employee–intermediary collusion.
- Digital-lending and loan-app impersonation risks.
- Early-warning signals and red-flag escalation.
- Distinguishing business distress, wilful misconduct and suspected fraud.
- Due process and authorised decision-making in fraud classification.

Module 8: Investment, Wealth and Family Office Fraud

- Investment misrepresentation and fabricated performance.
- Ponzi and pyramid schemes.
- Unauthorised pooling of investor money.
- Impersonation of regulated entities and investment professionals.
- Fictitious holdings, false statements and custody discrepancies.
- Misappropriation of client or family assets.
- Manipulated valuations and overstated investment performance.
- Undisclosed commissions and related-party arrangements.
- Subscription, redemption and distribution-related fraud.
- Private-market investment and co-investment red flags.
- Misuse of family mandates and payment authority.
- Verification of ownership, custody and cash movements.
- Distinguishing mis-selling, conflicts and suspected fraud.

Module 9: Insurance and Claims Fraud

- Misrepresentation at policy issuance.
- Policyholder, intermediary, employee and service-provider fraud.
- Fabricated or inflated claims.
- Duplicate claims and altered documentation.
- Beneficiary and identity manipulation.
- Premium diversion and unauthorised collection.
- Claims involving collusive service providers.
- Policy surrender and payout-related irregularities.
- Data inconsistencies and suspicious claims patterns.
- Verification, customer communication and escalation.
- Avoiding unjustified denial or assumptions of wrongdoing.

Module 10: Financial-Statement and Accounting Fraud

- Revenue recognition manipulation.
- Fictitious sales and premature revenue booking.
- Concealment or understatement of liabilities.
- Expense deferral and inappropriate capitalisation.
- Inventory and asset overstatement.
- Provisioning and estimate manipulation.
- Related-party transactions and undisclosed arrangements.

- Cash-flow inconsistencies and unusual journal entries.
- Period-end adjustments and management override.
- Ratio, trend and cash-conversion analysis.
- Auditor qualifications and inconsistencies in disclosures.
- Distinguishing aggressive accounting from suspected fraud.
- Limits of financial analysis and need for corroboration.

Module 11: Employee, Procurement and Third-Party Fraud

- Payroll, reimbursement and employee-benefit fraud.
- Ghost employees and fictitious vendors.
- Duplicate invoicing and false billing.
- Procurement collusion and bid manipulation.
- Kickbacks, bribery and improper inducements.
- Undisclosed employee–vendor relationships.
- Conflicts in outsourcing and service-provider selection.
- Commission and referral-payment abuse.
- Customer information theft and unauthorised disclosure.
- Vendor onboarding and bank-detail verification.
- Third-party due diligence and ongoing monitoring.
- Investigation referrals and corrective controls.

Module 12: Cyber-Enabled Fraud and Social Engineering

- Relationship between cyber incidents and financial fraud.
- Phishing, spear phishing, smishing and vishing.
- Credential theft and session compromise.
- Remote-access scams and malicious applications.
- SIM-swap and authentication-related risks.
- Executive, vendor and customer impersonation.
- Deepfake voice, video and fabricated communications.
- AI-generated documents and synthetic identities.
- Social engineering of employees and customers.
- Coordination between fraud, cybersecurity and operations teams.
- Preserving relevant information without compromising systems.
- Customer awareness and secure verification practices.

Module 13: Fraud Detection and Data Analytics

- Data sources used in fraud monitoring.
- Data quality, completeness and reconciliation.
- Rules-based alerts and risk scoring.
- Duplicate, unusual-value and outlier detection.
- Trend, frequency and time-pattern analysis.
- Unusual journal entries and approval overrides.
- Shared bank accounts, addresses and contact details.
- Relationship mapping and network indicators.
- Spreadsheet-based fraud-analysis techniques.
- Introductory use and limitations of Benford's Law.
- False positives, false negatives and alert prioritisation.
- Corroborating analytical findings.
- AI-assisted detection, explainability and human review.
- Model drift, bias and confidentiality risks.

Module 14: Transaction Monitoring and Early-Warning Systems

- Designing indicators around specific fraud scenarios.
- Behavioural changes and deviations from expected activity.
- Velocity, value, frequency and beneficiary patterns.
- Linking customer, account and transaction information.
- Early-warning signals and escalation thresholds.
- Alert triage, investigation referral and case ownership.
- Managing alert backlogs and ageing.
- Documenting closure decisions.
- Monitoring repeat incidents and control circumvention.
- Reviewing detection rules and thresholds.
- Measuring alert quality and operational effectiveness.
- Distinguishing fraud monitoring from AML monitoring while coordinating relevant information.

Module 15: Legal, Regulatory and Compliance Considerations

- Indian legal and regulatory architecture relevant to financial fraud.
- Roles of RBI, SEBI, IRDAI, FIU-IND and relevant enforcement authorities.
- Applicable criminal-law concepts concerning cheating, forgery and misappropriation.
- Electronic records and cyber-related offences.
- Fraud-related obligations applicable to different regulated entities.

- AML interfaces and suspicious-transaction reporting.
- Fraud reporting versus customer complaints and operational incident reporting.
- Confidentiality, privacy and lawful information sharing.
- Natural justice and fair treatment.
- Regulatory, contractual and internal reporting timelines.
- Staff accountability and authorised disciplinary processes.
- Cross-border incidents and jurisdictional limitations.
- Seeking qualified legal advice and specialist assistance.

Module 16: Fraud Incident Response and Escalation

- Receiving and recording allegations.
- Initial assessment and severity classification.
- Immediate containment within authorised powers.
- Protecting customers, assets and critical operations.
- Escalation to fraud, compliance, legal, cybersecurity and management teams.
- Preserving records and avoiding premature deletion or alteration.
- Restricting information to those with a legitimate need to know.
- Customer and stakeholder communication.
- Coordination with banks, insurers and service providers.
- Recovery, restitution and loss-mitigation considerations.
- Avoiding interference with formal investigations.
- Maintaining incident logs and decision records.

Module 17: Investigation Fundamentals and Evidence Preservation

- Purpose, scope and limitations of a fraud investigation.
- Distinguishing allegations, indicators, evidence and conclusions.
- Preparing factual chronologies.
- Identifying relevant documents, transactions and communications.
- Evidence integrity, provenance and chain-of-custody concepts.
- Original records, copies and controlled access.
- Basic fact-gathering and interview-awareness principles.
- Objective documentation and avoidance of leading conclusions.
- Corroboration and alternative explanations.
- Handling privileged, confidential and personal information.
- When to engage forensic accountants, digital-forensics specialists or counsel.
- Investigation reporting and professional boundaries.

Module 18: Whistleblowing, Complaints and Stakeholder Protection

- Whistleblowing channels and reporting accessibility.
- Anonymous and confidential disclosures.
- Complaint triage and conflict-free case allocation.
- Protection against retaliation.
- Handling malicious, mistaken or unsubstantiated allegations fairly.
- Confidentiality and limits on disclosure.
- Customer vulnerability and susceptibility to scams.
- Communicating with affected customers.
- Complaint records and recurring-pattern analysis.
- Employee fairness and reputational protection.
- Independent oversight of sensitive allegations.
- Closure communication within legal and confidentiality boundaries.

Module 19: Fraud-Loss Management, Remediation and Reporting

- Actual loss, potential exposure and recovery.
- Direct and indirect costs of fraud.
- Case registers and loss-event databases.
- Recovery tracking and insurance coordination.
- Root-cause analysis.
- Corrective-action plans and accountable owners.
- Control redesign and remediation testing.
- Repeat findings and overdue actions.
- Key risk indicators and management dashboards.
- Reporting to boards and committees.
- Learning from near misses and external incidents.
- Evaluating the effectiveness of the fraud-risk program.

Module 20: Ethics and Professional Judgement

- Integrity, objectivity and professional scepticism.
- Avoiding assumptions based on status, relationships or reputation.
- Conflicts of interest in handling allegations.
- Pressure to conceal, minimise or exaggerate incidents.
- Fair treatment and presumption against premature conclusions.
- Confidentiality and responsible information use.
- Avoiding unauthorised access and excessive data collection.

- Limitations of analytical tools and AI-generated outputs.
- Maintaining accurate, defensible records.
- Recognising limits of competence.
- Escalating concerns despite commercial pressure.
- Accountability for decisions and recommendations.