# UNIVERSITY OF KERALA

## Four Year Undergraduate Programme (FYUGP) — B.Com

## FORENSIC ACCOUNTING AND FRAUD DETECTION

| | |
|---|---|
| **Discipline** | COMMERCE |
| **Course Code** | UK5SECCOM301 |
| **Course Title** | Forensic Accounting and Fraud Detection |
| **Type of Course** | Skill Enhancement Course (SEC) |
| **Semester** | V |
| **Academic Level** | 300 – 399 |
| **Course Details** | 3 Credits \| Lecture: 2 hrs/week \| Tutorial: – \| Practical: 2 hrs/week \| Total: 4 hrs/week (60 Hours) |
| **Pre-requisites** | Basic knowledge of accounting and the legal environment of business. |
| **Course Summary** | This course enables learners to understand forensic accounting and to apply fraud-detection techniques in practice. It develops the ability to apply digital-forensics and data-analytics tools, analyse fraud schemes, devise evidence-gathering strategies, and evaluate internal-control and anti-fraud governance mechanisms. |

### Detailed Syllabus

| Unit | Content | Hrs |
|---|---|---|
| **Module I: Introduction to Forensic Accounting** | | **9** |
| 1 | **Forensic Accounting-** Evolution, Concept, Objectives & Scope of Forensic Accounting, Distinction between Forensic Accounting and Auditing. | 2 |
| 2 | **Forensic Accountant-** Qualifications, Qualities, Duties and Responsibilities, Ethical Obligations | 1 |
| 3 | **Application of Forensic Accounting: -**Relevance, Legal Framework and Application of Forensic Accounting | 2 |
| **Practicum**<br>Role-Play Activity: divide the class into groups of three – one Forensic Accountant, one Defence Attorney and one Judge/Observer. Provide a short case scenario (e.g., a company accountant who suddenly purchased a luxury car while inventory values dropped unexplainably before the annual audit). The Attorney cross-examines the Forensic Accountant on their legal duties, limitations and scope of investigation. The Judge/Observer evaluates the quality of the responses | | 4 |
| **Suggested Activities**<br>• Examine the modus operandi of a major documented accounting fraud in India (e.g., Satyam Computers scam 2009 or IL&FS scam 2018); prepare a brief structured report linking the fraud to (i) the failure of standard auditing procedures and (ii) the specific role forensic accounting could have played in early detection. | | |

| Unit | Content | Hrs |
|---|---|---|
| **Module II: Forensic Accounting Practice and Tools** | | **10** |
| 4 | Forensic Accounting Vs Traditional Accounting - Comparison on Objectives, Nature of Work, Skills required, Users and outcomes. | 2 |
| 5 | Process and Methodology of a Forensic Accounting: Process- Engagement and Risk Assessment, Planning, Evidence Collection, Analysis and Investigation, Reporting, Litigation and Resolution, prevention and governance. Methodologies & Techniques involved in Forensic Accounting | 2 |
| 6 | Digital Forensics: Process of digital forensic, areas of digital forensics relevant to Forensic Accounting, Data Analytics: types of data analytics, and Benford's Law | 1 |
| **Practicum**<br>Benford's Law Activity: divide the class into two halves. One half collects 25 real numbers (e.g., populations of towns from Wikipedia, prices of 25 items on an e-commerce website). The other half invents 25 fictional transaction amounts from memory. Papers are exchanged; each student counts how often digit 1 or digit 2 appears as the leading digit. Based on Benford's Law (digit 1 expected ~30% of the time), students flag whether their received dataset is organic or fabricated. Discuss the result and what this implies for a fraud investigator | | 5 |
| **Suggested Activities**<br>● Prepare a structured comparison chart contrasting Forensic Accounting and Traditional Accounting on: purpose, methodology, use of evidence, legal standing, type of output (report vs. audit opinion) and professional standards applicable. | | |
| **Module III: Foundations and Types of Frauds** | | **14** |
| 7 | Fraud:- Meaning, Legal Definition, Features of fraud, and Psychology of Fraud, importance of fraud psychology in forensic accounting. | 3 |
| 8 | Types of Financial Fraud:- Corporate, Financial Statement, and Banking Frauds. Cyber Frauds, Capital Market Frauds, and Tax Evasion, Insurance, Healthcare, and Consumer Frauds | 3 |
| **Practicum**<br>Reverse-Engineer the Fraud Scheme: assign a specific fraud type to each student pair (e.g., Tax Fraud, Cyber Fraud, Banking – Letter of Undertaking Fraud, or Financial Statement Fraud). Students act as "masterminds" and sketch a flowchart showing how a hypothetical person could exploit an organisational loophole to commit the assigned fraud. The neighbouring pair then acts as forensic investigators and identifies exactly where the trail of evidence was left behind | | 8 |
| **Suggested Activities**<br>● Review the published financial statements of a company involved in a documented fraud (e.g., Satyam Computers or Punjab National Bank); identify at least five specific financial red flags that were visible in the publicly available data prior to the fraud being reported. | | |
| **Module IV: Fraud Detection and Investigation** | | **15** |
| 9 | **Behavioural and Environmental Causes**: The Fraud Triangle & Fraud Diamond | 2 |
| 10 | **Fraud Indicators**: Identifying and Analysing Red Flags & Green Flags, financial flags, behavioural flags, Operational flags, Technology & Cyber flags, | 2 |
| 11 | **Fraud Detection Methods**, Evidence Gathering, and Investigation Procedures | 2 |

| Unit | Content | Hrs |
|---|---|---|
| 12 | **Asset Recovery and Interrogation Techniques:** Evidence obtaining, analysis, arrangement of evidence, and Techniques of interrogation. | 2 |
| | **Practicum**<br>Red Flag Silent Auction: write five behavioural anomalies on the board (e.g., "Employee never takes a vacation," "A vendor address matches an employee's home address," "Frequent round-number journal entries posted at midnight"). Each student team selects one red flag, devises a 3-step investigation strategy and prepares specific interview questions for the suspect. Teams present their action plan; the class votes on which strategy would most securely establish evidence. **OR**<br>Fraud Triangle Analysis: for a selected real or hypothetical fraud case, identify specific factors under each vertex of the Fraud Triangle (Pressure, Opportunity, Rationalisation) and each component of the Fraud Diamond (adding Capability); prepare a structured Fraud Risk Assessment Report. | 7 |
| | **Suggested Activities**<br>● Design a forensic accounting investigation plan for a company that was a victim of financial fraud (e.g., Kingfisher Airlines, DHFL or YES Bank); outline the evidence-gathering steps, documents to be reviewed, persons to be interviewed and the format of the investigation report. | |
| | **Module V: Fraud Prevention and Management [CCA Only]** | **12** |
| 13 | **Fraud Prevention: Internal Controls**- Types, and Importance, Fraud Risk Assessment- Steps, and Prevention Measures | 2 |
| 14 | **Policy & Legal Implications of Fraud:** Policy implications- Importance, Legal Consequences- Types: criminal consequences, civil, regulatory, and employment consequences and Expert Witness Testimony- Role, characteristics and importance. | 2 |
| 15 | **Corporate Governance and Fraud Prevention:** Role, Whistleblower Mechanisms, and Ethics- role of ethics and ethical principles in forensic accounting. | 2 |
| | **Practicum**<br>Whistleblower Policy Draft-Off: present a mock organisational culture (e.g., a highly competitive startup where mistakes are severely punished and management discourages dissent). Teams design a one-page Whistleblower and Anti-Fraud Policy covering: (i) how an employee can safely report fraud, (ii) who reviews the report and how confidentiality is protected, and (iii) what prevents management from retaliating against the reporter. Teams swap policies and critique whether they would feel safe reporting fraud under the peer-drafted policy. | 6 |
| | **Suggested Activities**<br>● Identify the internal control failures that allowed a selected capital market fraud (e.g., Harshad Mehta Scam or Ketan Parekh Scam) to remain undetected for an extended period; prepare a Fraud Prevention Recommendation Report covering the specific internal controls, governance mechanisms and regulatory measures that should have been in place. | |
| | **Total Instructional Hours** | **60** |

## References

### Text Books


- Crumbley, D. L., Heitger, L. E., & Smith, G. S. Forensic and Investigative Accounting. CCH Incorporated, Chicago.
- Kranacher, M., Riley, R., & Wells, J. T. Forensic Accounting and Fraud Examination. John Wiley & Sons, New Jersey.
- Rufus, R. J., Miller, L. S., & Hahn, W. D. Forensic Accounting. Pearson Education, New Jersey.

**Standard Reference Books**

- Manning, G. A. Financial Investigation and Forensic Accounting. CRC Press (Taylor & Francis Group), Boca Raton.
- Silverstone, H., & Sheetz, M. Forensic Accounting and Fraud Investigation for Non-Experts. John Wiley & Sons, New Jersey.

**Journals, Reports and Web Resources**

- American Accounting Association – Journal of Forensic Accounting Research – https://aaahq.org
- Accounting Today – Forensic Accounting Section – https://www.accountingtoday.com/tag/forensic-accounting
- ICAI – Forensic Accounting and Investigation Standards – https://www.icai.org

## Course Outcomes (COs)

| No. | Upon completion of the course the graduate will be able to: | Cognitive Level | PSO Addressed |
|---|---|---|---|
| CO1 | Explain the legal and regulatory frameworks governing financial fraud and the scope and methodology of forensic accounting. | U | PSO-1 |
| CO2 | Apply digital-forensics techniques and data-analytics tools, including Benford's Law, to the forensic investigation of financial datasets. | Ap | PSO-7 |
| CO3 | Analyse corporate, banking, cyber and capital-market fraud schemes to identify the mechanisms and vulnerabilities exploited. | An | PSO-11 |
| CO4 | Devise an evidence-gathering and interrogation strategy based on identified financial and behavioural red flags. | C | PSO-9, 11 |
| CO5 | Evaluate internal-control frameworks, whistleblower policies and anti-fraud governance mechanisms for mitigating fraud risk. | E | PSO-11, 12 |
| R – Remember U – Understand Ap – Apply An – Analyse E – Evaluate C – Create | | | |

Note: 1 or 2 COs per module.

| CO – PO/PSO, Cognitive Level and Knowledge Category | | | | | | | |
|---|---|---|---|---|---|---|---|
| CO No. | CO | PO / PSO | Cognitive Level | Knowledge | Module | L / T | P |
| CO1 | Explain the legal and regulatory frameworks governing financial fraud and the scope and methodology of forensic accounting. | PSO-1 | U | F, C | M I | L | P |
| CO2 | Apply digital-forensics techniques and data-analytics tools, including Benford's Law, to the forensic investigation of financial datasets. | PSO-7 | Ap | P | M II | L | P |
| CO3 | Analyse corporate, banking, cyber and capital-market fraud schemes to identify the mechanisms and vulnerabilities exploited. | PSO-11 | An | C, P | M III | L | P |
| CO4 | Devise an evidence-gathering and interrogation strategy based on | PSO-9, 11 | C | P, M | M IV | L | P |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | identified financial and behavioural red flags. | | | | | | |
| **CO5** | Evaluate internal-control frameworks, whistleblower policies and anti-fraud governance mechanisms for mitigating fraud risk. | PSO-11, 12 | E | C, P | M V | L | P |
| Cognitive Levels: R – Remember U – Understand Ap – Apply An – Analyse E – Evaluate C – Create \| Knowledge: F – Factual C – Conceptual P – Procedural M – Metacognitive | | | | | | | |

## Mapping of COs with PSOs

| CO \ PSO | PSO 1 | PSO 2 | PSO 3 | PSO 4 | PSO 5 | PSO 6 | PSO 7 | PSO 8 | PSO 9 | PSO 10 | PSO 11 | PSO 12 | PSO 13 | PSO 14 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CO1** | 3 | – | – | – | – | – | – | – | – | – | – | – | – | – |
| **CO2** | – | – | – | – | – | – | 3 | – | – | – | – | – | – | – |
| **CO3** | – | – | – | – | – | – | – | – | – | – | 3 | – | – | – |
| **CO4** | – | – | – | – | – | – | – | – | 2 | – | 2 | – | – | – |
| **CO5** | – | – | – | – | – | – | – | – | – | – | 3 | 2 | – | – |
| Correlation: (–) No correlation 1 – Mild 2 – Moderate 3 – Strong | | | | | | | | | | | | | | |

## Mapping of COs with POs

| CO \ PO | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 | PO8 |
|---|---|---|---|---|---|---|---|---|
| **CO1** | 2 | – | – | – | – | – | – | 3 |
| **CO2** | 2 | – | – | – | – | – | 3 | – |
| **CO3** | 2 | 2 | – | – | – | – | – | – |
| **CO4** | 2 | 3 | – | – | – | – | – | – |
| **CO5** | – | – | – | – | 2 | – | – | 3 |
| Correlation: (–) No correlation 1 – Mild 2 – Moderate 3 – Strong | | | | | | | | |

## Assessment Rubrics

Assessment tools: Quiz / Assignment / Discussion / Seminar / Case Study / Activity / Internal Examination / Project / End Semester Examination

| | Internal Exam | Assignment | Project / Viva | End Semester Exam |
|---|---|---|---|---|
| **CO1** | ✓ | ✓ | | ✓ |
| **CO2** | ✓ | | ✓ | ✓ |
| **CO3** | ✓ | ✓ | ✓ | ✓ |
| **CO4** | ✓ | | ✓ | |

| | Internal Exam | Assignment | Project / Viva | End Semester Exam |
|---|---|---|---|---|
| CO5 | ✓ | | ✓ | |

## Assessment Pattern

| Component | Basis / Assessment Tools | Marks |
|---|---|---|
| **THEORY COMPONENT — 2 Credits (Total: 40 Marks) \| CCA : ESE = 30 : 70** | | |
| **CCA – Theory – All Modules (I–V)** | | **12** |
| Formative Assessment – Theory (FA) | Three components of 2 marks each (2 + 2 + 2 = 6 marks): • Practicum assignment on Fraud Triangle Analysis and red flag identification (2 marks) • Case-study analysis on a real-world corporate or banking fraud scenario (2 marks) • Quiz on Benford's Law, types of fraud and forensic accounting tools (2 marks) | 6 |
| Summative Assessment – Theory (SA) | Internal examination conducted after a defined instructional period; the score is converted to marks equal to FA. | 6 |
| **ESE – Theory (Modules I–IV only)** | | **28** |
| **Written Examination** | 60 minutes – covering Modules I, II, III and IV only | 28 |
| **Sub-total – Theory** | | **40** |
| **PRACTICAL COMPONENT — 1 Credit (Total: 20 Marks) \| CCA : ESE = 40 : 60** | | |
| **CCA – Practical – All Modules (I–V)** | | **8** |
| Formative Assessment – Practical (FA) | Continuous assessment of practicum exercises across all modules; recorded in the practicum portfolio. | 4 |
| Summative Assessment – Practical (SA) | Practical viva or structured demonstration. FA and SA carry equal weightage. | 4 |
| **ESE – Practical** | | **12** |
| **Practical Examination** | Practical examination / project presentation – 30 minutes. | **12** |
| **Sub-total – Practical** | | **20** |
| **Grand Total** | | **60** |

**Notes:**

- Total marks: 60 (3-credit SEC course: 2 theory credits + 1 practical credit). Theory – 40 marks (CCA : ESE = 30 : 70); Practical – 20 marks (CCA : ESE = 40 : 60).
- Theory FA (6 marks) and Theory SA (6 marks) carry equal weightage within Theory CCA (12 marks).
- Theory ESE: 90-minute written examination covering Modules I–IV only (28 marks). Module V assessed through Theory CCA only.

- Practical FA (4 marks) and Practical SA (4 marks) carry equal weightage within Practical CCA (8 marks).
- Practical ESE (12 marks): a 30-minute practical examination or project presentation.