Pokhara University
Faculty of Science and Technology

Course Code: CMP 641 (3 Credits)	Full marks: 100
Course Title: Blockchain Technology (3-0-0)	Pass marks: 60
Nature of the course: Theory	Total Lectures: 45 hrs
Level: Master	Program: MSc CS

1. Course Description

This course provides an in-depth introduction to Blockchain Technology, its foundational concepts, and real-world applications. Students will explore the underlying cryptographic principles, consensus algorithms, smart contracts, and blockchain protocols like Ethereum and Hyperledger. The course emphasizes knowledge enabling students to design, develop, and deploy decentralized applications (DApps). It also includes coverage of Web3 ecosystems, Non-Fungible Tokens (NFTs), Decentralized Finance (DeFi), and emerging governance models such as DAOs. Emphasis is placed on security, scalability, and legal frameworks, providing a holistic understanding of blockchain's impact across industries including finance, supply chain, healthcare, and governance.

2. General Objectives

The course is designed with the following general objectives:

- To familiarize the students with the fundamental principles of blockchain technology, its architectures, consensus mechanisms, and the evolving Web3 ecosystem including NFTs, DeFi, and DAOs.
- To enable the students to design and implement smart contracts and decentralized applications (DApps) using platforms such as Ethereum and Solidity.
- To equip the students with the ability to evaluate real-world blockchain applications, address scalability, security, and privacy challenges, and consider regulatory and ethical implications of blockchain adoption.

3. Methods of Instruction

Lectures with interactive discussion, Instructor-led demonstrations, Group assignments and project work, Guest lectures from industry experts, Case study analysis and Student presentations.

4. Contents in Detail

Specific Objectives	Contents
• Define blockchain/DLT, characteristics, types, benefits, challenges, applications.	**Unit 1: Introduction to Blockchain (6 hrs)** 1.1 Defining Blockchain, Blockchain Evolution 1.2 Distributed Ledger Technology (DLT), Generic Blockchain elements, Blockchain Header 1.3 Blockchain Characteristics, Blockchain Structure 1.4. Blockchain Applications in Health, Insurance, Media, Asset Management, Supply Chain, Food Safety, Banking, Government 1.5 Types of Blockchain (Public, Consortium & Private) 1.6 Blockchain Benefits, Obstacles & Challenges, Current Landscape and Future Trends

• Explain essential cryptography: encryption, hashing, signatures, Merkle Trees. • Describe algorithms (RSA, ECC), ZKPs.	**Unit 2: Cryptography for Blockchain (5 hrs)** 2.1 Symmetric and Asymmetric Cryptography 2.2 Public and Private keys, DES, AES, RSA, ECC 2.3 Open SSL, Hash Function, Hash Pointer and Data Structure 2.4 Merkle Trees, Distributed Hash Table (DHTs), Digital Signature, Multisignature, Elliptic Curve Digital signature algorithm (ECDSA) 2.5 Zero Knowledge Proofs (ZKPs)
• Describe Bitcoin history, architecture, transactions, mining, security. • Differentiate Bitcoin/altcoins, understand ICOs, SPV.	**Unit 3: Cryptocurrency Fundamentals (5 hrs)** 3.1 Bitcoin Definition, Bitcoin History, Bitcoin Block, Genesis Block, Token and ICO, Bitcoin Exchanges 3.2 Bitcoin Payment, Bitcoin Transactions, Script Parsing and Processing, Simplified Payment Verification (SPV) 3.3 Bitcoin Architecture, Bitcoin P2P Network, Bitcoin Address, Bitcoin Storage & Uses, Bitcoin Security, Wallet 3.4 Altcoins, Cryptocurrency Ecosystem, Relationship between Altcoins & Bitcoin
• Analyze consensus mechanisms (PoW, PoS, BFT). • Compare approaches, explain forks, evaluate security/scalability trade-offs.	**Unit 4: Consensus Mechanisms (5 hrs)** 4.1 Distributed Consensus 4.2 Byzantine Generals Problem, Byzantine Agreement, Byzantine Fault Tolerance (BFT), Lamport-Shostak-Pease BFT Algorithm 4.3 Proof of Work, Proof of Stake, Proof of Authority, Proof of Burn, Proof of Elapsed Time, Proof-of-X approaches 4.4 Virtual Mining, Mining Difficulty, SegWit and Forks (Hard and Soft)
• Define smart contracts, history, implications (DAOs). • Describe design best practices, execution, failure modes, automation.	**Unit 5: Smart Contracts (5 hrs)** 5.1 Smart contract Definition, History of Smart Contract 5.2 Economic Concept of Contracts, Regulation and Legal Frameworks 5.3 DAO, Consensus Protocols and Inter-Contract Execution 5.4 Smart Contract Design, Smart Contract Best Practices, Smart Contract Failure and responses. 5.5 Solidity for Smart Contract Development
• Explore Ethereum: Ether, gas, structure, EVM, state, transactions. • Identify tools/languages for DApp development.	**Unit 6: Ethereum Ecosystem & dApp Development (6 hrs)** 6.1 Introduction, Ethereum Blockchain: Currency, Forks, Gas, Ethereum Structure 6.2 Consensus Mechanism, World State, Transactions 6.3 Elements of Ethereum Blockchain: Ethereum Virtual Machine 6.4 Ethereum Environment, Precompiled Contracts, Ether, Messages, Accounts, Block, Mining 6.5 Ethereum testnets & dApp Development: tools, languages, compilers
• Analyse Hyperledger Fabric	**Unit 7: Hyperledger Fabric and Permissioned Blockchain (7 hrs)**

architecture/consensus. • Describe components, flow, channels, identity, tools for enterprise chain code.	7.1 Introduction, Hyperledger Architecture, Consensus Algorithm in Hyperledger, Hyperledger Node 7.2 Hyperledger Fabric: Fabric Architecture, Transaction Flow in Fabric, Components of Fabric 7.3 Ordering Services, Channels in Fabric, Fabric Peer and Certificate Authority 7.4 Fabric Membership and Identity management, Hyperledger Fabric Network 7.5 Hyperledger Composer, Hyperledger Explorer, Hyperledger Caliper, Chaincode, Peers
• Explore Web3 stack, Layer 2, NFTs, DeFi, and interoperability. • Assess legal, ethical, and sustainability issues in blockchain and decentralization.	**Unit 8: Web3, Emerging Technologies, and Socio-Ethical Aspects (6 hrs)** 8.1 Layer 2 solutions (Polygon, Optimism, zkRollups) 8.2 Introduction to Web3 stack: Wallets, IPFS, The Graph, NFTs, DeFi basics 8.3 Interoperability: Polkadot, Cosmos 8.4 Data privacy, GDPR, and blockchain 8.5 Environmental impact of mining 8.6 Regulatory landscape: Nepal and global overview, Ethical considerations of decentralization

5. Case Studies

- Blockchain in Supply Chain (e.g., IBM Food Trust)
- DeFi platforms (e.g., Uniswap, Compound)
- Blockchain for identity and e-governance (e.g., Estonia's e-Residency)
- Blockchain in E-Governance and Voting Systems

6. Evaluation system and Students' Responsibilities

Internal Evaluation	**Weight**	**Marks**	**External Evaluation**	**Marks**
Theory			Semester-End examination	40
Attendance & Class Participation	10%	6		
Assignments	10%	6		
Presentations/Quizzes	10%	6		
Internal Assessment	50%	30		
Case study Workshops	20%	12		
Total Internal		60		
Full Marks: 60 + 40 = 100				

Students' Responsibilities

Each student must secure at least 60% marks separately in internal assessment and practical evaluation with 80% attendance in the class in order to appear in the Semester End Examination. Failing to get such a score will be given NOT QUALIFIED (NQ) to appear for the Semester-End Examinations. Students are advised to attend all the classes, formal exam,

test, etc. and complete all the assignments within the specified time period. Students are required to complete all the requirements defined for the completion of the course.

7. References:

1. Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press.
2. Antonopoulos, A. M. (2017). Mastering Bitcoin: Programming the Open Blockchain (2nd ed.). O'Reilly Media.
3. Mougayar, W. (2016). The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. Wiley.
4. Singhal, B., Dhameja, G., & Panda, P. S. (2018). Beginning Blockchain: A Beginner's Guide to Building Blockchain Solutions. Apress.
5. Bashir, I. (2017). Mastering Blockchain: Master the Theoretical and Technical Foundations of Blockchain Technology and Explore Its Future (2nd ed.). Packt Publishing.
6. Antonopoulos, A. M., & Wood, G. (2018). Mastering Ethereum: Building Smart Contracts and DApps. O'Reilly Media.

Pokhara University
Faculty of Science and Technology

Course Code: CMP 642 (3 Credits)
Course Title: **Cryptography** (3-0-0)
Nature of the course: Theory/Tutorial/Practical
Level: Master

Full marks: 100
Pass marks: 60
Total Lectures: 45 hrs
Program: MCE/ MSc CS

1. Course Description

This course is designed to establish the theoretical foundations and practical implementations of modern cryptography with an emphasis on advanced concepts. It builds on introductory cryptography, delving deeper into symmetric and asymmetric cryptographic primitives, cryptographic hash functions, message authentication, number theory, and post-quantum cryptographic schemes. Moreover, the course aims to foster a comprehensive understanding of cryptographic security models and the ability to rigorously analyze protocols for confidentiality, integrity, and authenticity in real-world systems.

2. General Objectives:

The course is designed with the following general

- To make the students competent in symmetric and asymmetric cryptographic primitives, provable security principles, and cryptographic hardness assumptions.
- To enable the students to implement cryptographic schemes (e.g., RSA, El Gamal, HMAC) and apply cryptography in securing protocols such as SSL/TLS and IPsec.
- To familiarize the students with formal models of cryptographic constructions and post-quantum cryptographic candidates like lattice-based and hash-based schemes.

3. Methods of Instruction

- Lectures with slides and blackboard explanations
- Interactive tutorial discussions and problem-solving sessions
- Hands-on practical labs involving cryptographic programming
- Student-led presentations on advanced topics
- Assignments and project-based learning

4. Contents in detail

Specific Objectives	Contents
• Define computational security and secure encryption schemes, including CPA and CCA security. • Differentiate concrete and asymptotic security. • Prove security via reductionist arguments.	**Unit 1: Private-Key Encryption (7 hrs)** 1.1 Computational Security: Concrete and Asymptotic Approach 1.2 Computationally Secure Encryption 1.3 Constructing Secure Encryption Schemes, Pseudorandom Generators 1.4 Proofs by Reduction 1.5 Stronger Security Notions: Chosen-Plaintext Attacks and CPA-Security 1.6 Constructing CPA-Secure Encryption Schemes 1.6.1 Pseudorandom Functions, CPA-Secure Encryption from Pseudorandom functions 1.7 Chosen-Ciphertext Attacks
• Formalize integrity vs. Secrecy.	**Unit 2: Message Authentication Codes (6 hrs)**

• Design CBC-MAC and analyze its security. • Implement authenticated encryption • Interpret message integrity and authenticity using MACs.	2.1 Message Integrity, Secrecy vs. Integrity, and Encryption vs. Message Authentication 2.2 Message Authentication Codes 2.3 Constructing Secure Message Authentication Codes: A Fixed-Length MAC, Domain Extension for MACs 2.4 CBC-MAC: The Basic Construction 2.5 Authenticated Encryption 2.5.1 Generic Constructions 2.5.2 Secure Communication Sessions
• Construct cryptographic hash functions. • Prove collision resistance of Merkle-Damgård. • Implement HMAC and Merkle trees. • Analyze the random oracle model.	**Unit 3: Hash Functions and Applications (6 hrs)** 3.1 Collision Resistance and Weaker Notions of Security 3.2 Domain Extension: The Merkle–Damgard Transform 3.3 Message Authentication using Hash Functions, Hash-and-MAC 3.4 Generic Attacks on Hash Functions: Birthday Attacks for Finding Collisions and Small-Space Birthday Attacks 3.5 The Random-Oracle Model 3.5.1 Soundness of Random-Oracle Methodology 3.6 Additional Applications of Hash Functions: Fingerprinting and Deduplication, Merkle Trees, Password Hashing and Key Derivation
• Apply modular arithmetic to RSA/DH. • Generate safe primes for cryptographic use.1 • Formalize hardness assumptions (Factoring, DLOG)	**Unit 4: Number Theory and Cryptographic Hardness Assumptions (6 hrs)** 4.1 Preliminaries and Basic Group Theory: Primes and Divisibility, Modular Arithmetic, Groups, The Group Z_N* 4.2 Primes, Factoring, and RSA: Generating Random Primes, The Factoring Assumption, and The RSA Assumption 4.3 Cryptographic Assumptions in Cyclic Groups: Cyclic Groups and Generators 4.4 The Discrete-Logarithm/Diffie–Hellman Assumptions 4.5 Elliptic Curve Arithmetic
• Interpret secure constructions of public-key encryption schemes. • Contrast CPA/CCA-security in hybrid encryption. • Implement El Gamal and RSA • Analyze KEM/DEM paradigms.	**Unit 5: Public-Key Encryption (6 hrs)** 5.1 Public-Key Encryption: Security against Chosen-Plaintext Attacks, and Security against Chosen-Ciphertext Attacks 5.2 Hybrid Encryption and the KEM/DEM Paradigm: CPA-Security and CCA-Security 5.3 CDH/DDH-Based Encryption 5.3.1 El Gamal Encryption 5.3.2 DDH-Based Key Encapsulation 5.4 RSA Encryption 5. 5 Elliptic Curve Cryptography

• Interpret security protocols and standards on the internet. • Configure TLS/SSL for secure channels. • Deploy PGP/SMIME for email security.	**Unit 6: Network and Internet security (6 hrs)** 6.1 Web Security Issues 6.2 Secure Sockets Layer (SSL) Security 6.3 Transport Layer Security (TLS) 6.4. HTTPS 6.5 Secure Shell (SSH) 6.6. Electronic mail security: Pretty Good Privacy (PGP) and S/MIME 6.7 IP Security Overview: Applications and Benefits of IPsec
• Interpret quantum-resilient cryptographic primitives (lattice based, code based, multivariate based and hash based) • Compare lattice-based (NTRU, LWE) and hash-based signatures. • Implement NTRU and McEliece • Analyze various Multivariate scheme	**Unit 7: Post-Quantum Cryptography (8 hrs)** 7.1 Overview of post-quantum Cryptography 7.2 Lattice-based Cryptography 7.2.1 NTRU 7.2.2 Lattices and the Security of NTRU 7.2.3 Learning with Errors 7.3 Code-based Cryptography: The McEliece Cryptosystem 7.4. Multivariate Cryptography: Hidden Field Equations, The Oil and Vinegar Signature Scheme 7.5 Hash-based Signature Schemes: Lamport Signature Scheme and an overview of Winternitz Signature Scheme

5. List of Tutorials

The following tutorial activities of 16 hours per group of maximum 24 students should be conducted to cover all the required contents of this course.

S.N.	Tutorials
1	Symmetric encryption security proofs (reduction-based)
2	Constructing PRFs and their applications
3	CPA vs CCA: construction and examples
4	MAC construction and collision resistance exercises
5	CBC-MAC case study
6	HMAC implementation and security analysis
7	Birthday problem and hash collisions
8	Hash-based MAC implementation
9	Group theory refresher for cryptography
10	RSA key generation and vulnerabilities
11	ElGamal implementation and hybrid encryption
12	Exploring TLS handshake protocol
13	Secure email protocols simulation
14	Lattice-based cryptography: NTRU exercises
15	Code-based cryptosystem example: McEliece
16	Construct a toy example of Oil and Vinegar Signature
17	Lamport Signature Scheme exercises

6. Practical Work: Implementation in SageMath, Python or any Other languages

S.N.	Practical Works
1	Implement a stream cipher using a PRG
2	Simulate a block cipher and apply ECB/CBC modes
3	Design and test a CPA-secure encryption using a PRF
4	Implement CBC-MAC and analyze its behavior
5	RSA encryption/decryption tool with key generation
6	ElGamal encryption and decryption module
7	SSL/TLS protocol implementation in Python/Java
8	Secure email simulation using PGP
9	Implement NTRU encryption/decryption in Python/Sage
10	Implement McEliece Cryptosystem in Python/Sage
11	Implement Multivariate bases schemes in Python/Sage

7. Evaluation System and Students' Responsibilities

Internal Evaluation
In addition to the formal end-semester exam(s), the internal (formative) evaluation of a student may consist of quizzes, assignments, lab reports, projects, class participation and presentation etc. The tabular presentation of the internal evaluation is as follows. The components may differ according to the nature of the subjects.

Internal Evaluation	Weight	Marks	External Evaluation	Marks
Theory			Semester-End examination	40
Attendance & Class Participation	10%	6		
Assignments	10%	6		
Presentations/Quizzes	20%	12		
Internal Assessment	40%	24		
Group Workshops	20%	12		
Total Internal		60		
Full Marks: 60 + 40 = 100				

Students' Requirements:
Each student must secure at least 60% marks separately in internal assessment and practical evaluation with 80% attendance in the class in order to appear in the Semester End Examination. Failing to get such a score will be given NOT QUALIFIED (NQ) to appear for the Semester-End Examinations. Students are advised to attend all the classes, formal exam, test, etc. and complete all the assignments within the specified time period. Students are required to complete all the requirements defined for the completion of the course.

8. Prescribed Books and References

- Cryptography Theory and Practice, Douglas R. Stinson, Maura B. Paterson, CRC Press.
- Introduction to Modern Cryptography, Jonathan Katz, Yehuda Lindell McGraw Hill.
- A Graduate Course in Applied Cryptography, Dan Boneh and Victor Shoup, Stanford University.

Pokhara University
Faculty of Science and Technology

Course Code: CMP 643 (3 Credits)	Full marks: 100
Course Title: Data Mining (3-0-0)	Pass marks: 60
Nature of the course: Theory	Total Lectures: 45 hrs
Level: Master	Program: MCE

1. Course Description

This course offers a rigorous exploration of data mining principles, emphasizing mathematical foundations and practical applications. It delves into details of regression analysis, classification, association analysis, cluster analysis, anomaly detection, and Bayesian structure learning. The course also emphasizes case studies in selected topics to provide and exposure to the research-level questions of Data Mining.

2. General Objectives

The course is designed with the following general objectives:

- To develop students' knowledge of core data mining concepts, techniques, and their practical relevance to real-world problems.
- To equip the students with hands-on experience in using data mining tools and programming languages for data analysis.
- To acquaint the students with advanced topics and current research trends in the field of data mining.

3. Methods of Instruction

Lectures for theoretical foundation.
Tutorial Sessions for interactive learning.
Case Studies of seminal papers on specified topics

4. Contents in Detail

Specific Objectives	Contents
• Describe the overall pipeline of the KDD process and the interesting problems of data mining • Apply various data transformation methods depending on the context of real-world problems	**Unit 1: Introduction to Data Mining (3 hrs)** 1.1. Defining Data Mining: The Knowledge Discovery from Database Process 1.2. Types of patterns that can be mined: class/concept description, frequent patterns and associations, classification and regression; cluster analysis; outlier analysis 1.3. Structured and unstructured data 1.4. The types of variables: numeric – continuous and discrete; categorical – nominal and ordinal 1.5. Data transformation 1.5.1 Smoothing: moving average for time series 1.5.2 Aggregation 1.5.3 Rescaling: z-score and unit scaling 1.5.4 Discretization – frequency based

	1.5.5 Binarization
• Describe the basic mathematical constructs and derivations related to regression analysis • Gauge the applicability of different regression methods for different for real-world problems • Interpret the results of regression modelling	**Unit 2: Regression Analysis (10 hrs)** 2.1 Generalized Linear Models (GLM) 2.1.1 Exponential family distributions and link functions 2.1.2 Logistic and Poisson regression models 2.1.3 Maximum likelihood estimation and inference 2.2 Kernel Regression 2.2.1 The Nadaraya-Watson estimator 2.2.2 Kernel functions 2.3 The bias-variance trade-off and regularization 2.3.1 L1, L2, and elastic net for GLM 2.3.2 Bandwidth selection as regulation for Kernel regression 2.4 Time series regression: brief introduction to challenges posed by autocorrelation and non-stationarity 2.5 Predictor importance and partial-dependence analysis for regression models Case study: Trade-offs between model-based and non-parametric approaches to data modelling in the context of regression analysis
• Describe the basic algorithms to classification analysis • Select the appropriate type of classification model and build the model for real-world problems • Interpret the results of classification modelling	**Unit 3: Classification Analysis (8 hrs)** 3.1 Decision Trees: CART algorithm 3.2 Naïve Bayes classifiers 3.3 Support Vector Machines for classification 3.4 Evaluation metrics: confusion matrix, ROC curves, cross-validation 3.5 Predictor importance and partial dependence analysis for classification models Case study: effect of correlation between predictor variables on the ranking of predictor variable importance in classifiers
• Describe the basic approaches to association analysis • Apply the apriori algorithm for real-world problems	**Unit 4: Association Analysis (4 hrs)** 4.1 Market basket analysis 4.2 Apriori algorithm 4.3 Overview of FP-Growth algorithm 4.4 Evaluation metrics: support, confidence, lift Case Study: visualization methods for association rule mining
• Describe the basic	**Unit 5: Cluster Analysis (8 hrs)**

mathematical constructs and derivations related to cluster analysis. • Select the appropriate type of clustering model and build the model for real-world problems.	5.1 Distance measures 5.2 Partitioning methods: k-means, k-medoids 5.3 Hierarchical clustering 5.4 Density-based methods: DBSCAN 5.5 Prototype-based methods: mixture models 5.6 Cluster validation and evaluation Case study: the challenge of deciding the optimal number of clusters in real-world clustering problems
• Describe the basic mathematical constructs and derivations related to anomaly and outlier detection. • Detect anomalies and outliers in real-world problems.	**Unit 6: Anomaly Detection and Outlier Analysis (4 hrs)** 6.1 Statistical approaches to anomaly detection 6.1.1 Univariate outliers based on normal distribution; multivariate outliers based on the chi-squared statistic 6.2 Proximity based outliers 6.2.1 Distance-based and density-based methods Case study: one-class classifiers for anomaly detection
• Describe the basic mathematical constructs and derivations related to Bayesian networks • Build and interpret Bayesian networks for real-world problems	**Unit 7: Bayesian Structure Learning (8 hrs)** 7.1 Introduction to Bayesian Networks 7.1.1 Conceptual foundations: directed acyclic graphs and conditional dependencies 7.1.2 Probabilistic interpretation: joint probability distribution and conditional independence 7.2 Learning approaches 7.2.1 constraint-based, score-based, hybrid methods for learning structures from data 7.2.2 model evaluation 7.3 Parameter learning and inference 7.3.1 Overview of MLE and Bayesian approaches 7.3.2 Computing marginal and conditional probabilities Case study: Causal analysis using Bayesian networks

5. Evaluation system and Students' Responsibilities

Internal Evaluation

The internal evaluation of a student may consist of assignments, attendance, internal assessment and group workshop. The internal evaluation scheme for this course is as follows:

Internal Evaluation	Weight	Marks	External Evaluation	Marks
Theory			Semester-End examination	40
Attendance & Class Participation	10%	6		
Assignments	10%	6		
Presentations/Quizzes	10%	6		
Internal Assessment	50%	30		
Practical and Case Studies	20%	12		
Total Internal		60		
Full Marks: 60 + 40 = 100				

6. Student Responsibilities:

Each student must secure at least 60% marks separately in internal assessment and practical evaluation with 80% attendance in the class in order to appear in the Semester End Examination. Failing to get such a score will be given NOT QUALIFIED (NQ) to appear for the Semester-End Examinations. Students are advised to attend all the classes, formal exam, test, etc. and complete all the assignments within the specified time period. Students are required to complete all the requirements defined for the completion of the course.

7. References

- Tan, P.N., Steinbach, M. and Kumar, V., 2006. Introduction to data mining. Pearson Education, Inc.
- Han, J., and Kamber, M., 2006. Concepts and techniques. Morgan Kaufmann
- Scutari, M., and Denis, J., 2022. Bayesian Networks with Examples in R. CRC Press.
- Greene, W. H. Econometric Analysis. Fifth Edition. Pearson Johnson, R.A. and Wichern, D.W., 2014.
- Johnson, R.A. and Wichern, D.W., 2014. Applied multivariate statistical analysis. PHI Learning Pvt Ltd.

Pokhara University
Faculty of Science and Technology

Course Code: CMP 644 (3 Credits)	Full marks: 100
Course Title: Information System Audit (3-0-0)	Pass marks: 60
Nature of the course: Theory	Total Lectures: 45 hrs
Level: Master	Program: MCE/ MSc CS

1. Course Description

The Information System Audit course for graduate students provides an in-depth understanding of auditing principles, methodologies, and best practices for assessing the security, integrity, and compliance of information systems. The course covers risk assessment, control frameworks, IT governance, regulatory compliance, and emerging threats in cybersecurity. Students will gain hands-on experience in auditing IT infrastructure, applications, and processes through case studies and practical exercises. This course covers different concepts of Information Systems Auditing including basics, hardware and software security issues, information systems audit and conducting IS audit, risk-based systems audit, business continuity and disaster, auditing in the ICT environment, and security testing.

2. General Objectives

The course is designed with the following general objectives:

- To develop students' knowledge of information systems auditing principles, processes, methodologies, and risk-based auditing approaches in ICT environments.
- To acquaint the students with Governance, Risk, and Compliance (GRC), as well as the importance of business continuity and disaster recovery in audit planning.
- To equip the students with practical understanding of security testing tools, vulnerability assessment, penetration testing, and insights into emerging trends in information systems auditing.

3. Methods of Instruction

Lecture, Discussion, Readings, Case Studies and Group Workshops

4. Contents in Detail.

Specific Objectives	Contents
Describe Information System Audit and IT Audit Frameworks with emphasis on widely known standards such as ISO 27001, NIST, COBIT, CIS, MITRE and C2M2	**Unit 1: Overview of Systems Audit (8 Hrs.)** 1.1 Information Systems Audit and Information Systems Auditor 1.2 Legal Requirements of an Information Systems Audit 1.3 Systems Environment and Information Systems Audit 1.4 Information Systems Assets and Classification of Controls 1.5 Information Systems Audit Coverage 1.6 Government and Regulatory Frameworks 1.7 IT Audit Framework, ISO 27001, NIST Cyber Security Framework, COBIT, CIS, MITRE, C2M2
Compare Hardware and Software Security Issues	**Unit 2: Hardware and Software Security Issues (8 Hrs.)**

during Information System Audit	2.1 Hardware Security Objective 2.2 Peripheral Devices and Storage Media 2.3 Authentication Devices 2.4 Hardware Acquisition, Hardware Maintenance and Management of Obsolescence 2.5 Disposal of Equipment; Problem Management; Change Management 2.6 Network and Communication Issues. 2.7 Overview of Types of Software; Elements of Software Security 2.8 Control Issues during Installation and Maintenance 2.9 Licensing Issues, ICT Procurement Practices
Describe Information System Audit Requirements in terms of Information System Control, Logs and Evidence Collection	**Unit 3: Information Systems Audit Requirements (8 Hrs.)** 3.1 Information Systems Control Objectives; Information Systems Audit Objectives; 3.2 System Effectiveness and Efficiency 3.3 Information Systems Abuse 3.4 Asset Safeguarding Objective and Process 3.5 Evidence Collection and Evaluation 3.6 Logs and Audit Trails as Evidence 3.7 IT Audit Standard and Regulatory Requirements
Summarize Information System Auditing	**Unit 4: Conducting an Information Systems Audit (10 Hrs.)** 4.1 Audit Program and Audit Plan 4.2 Audit Procedures and Approaches 4.3 System Understanding and Review 4.4 Compliance Reviews and Tests 4.5 Substantive Reviews and Tests 4.6 Audit Tools and Techniques 4.7 Sampling Techniques 4.8 Audit Questionnaire; Audit Documentation; Audit Report 4.9 Auditing Approaches; Sample Audit Work-Planning Memo 4.10 Sample Audit Work Process Flow 4.11 Conducting a Risk-Based Information Systems Audit 4.12 Risk Assessment and Risk Management Strategy.
Describe Business continuity and Disaster Recovery Plan during Information System Audit	**Unit 5: Business Continuity and Disaster Recovery Plan (6 Hrs.)** 5.1 Business Continuity and Disaster Recovery Process 5.2 Business Impact Analysis; Incident Response Plan 5.3 Disaster Recovery Plan 5.4 Types of Disaster Recovery Plans 5.5 Emergency Preparedness Audit Checklist 5.6 Business Continuity Strategies 5.7 Business Resumption Plan Audit Checklist 5.8 Recovery Procedures Testing Checklist; Plan Maintenance Checklist.

Apply the concept of VAPT, Cloud Computing Audits and Emerging Concepts	**Unit 6: Security Testing and Cloud Computing Audit (5 Hrs.)** 6.1 Cybersecurity 6.2 Vulnerability Assessment and Penetration Testing (VAPT) 6.3 Secured Software Development Testing, 6.4 Open Web Application Security Project 6.5 Security Testing Tools 6.6 Cloud Audit Considerations 6.7 Emerging Concepts in Information System Audit

5. Group Workshops

The Group workshop should cover the following works:

SN	Group Workshops
1.	Information Security Gap Assessment through ISO 27001
2.	Cybersecurity Maturity Assessment through NIST Cybersecurity Framework
3.	Develop IS Audit Terms of Reference
4.	Develop the detailed Proposal for Conducting an Information System Audit
5.	Conduct Information System Audit and Reporting
6.	IT Governance Audit through Control Objectives for Related Technologies
7.	Conducting Risk Assessment

6. **Evaluation system and Students' Responsibilities**

Internal Evaluation

The internal evaluation of a student may consist of assignments, attendance, internal assessment and group workshop. The internal evaluation scheme for this course is as follows:

Internal Evaluation	Weight	Marks	External Evaluation	Marks
Theory			Semester-End examination	40
Attendance & Class Participation	10%	6		
Assignments	10%	6		
Presentations/Quizzes	20%	12		
Internal Assessment	40%	24		
Group Workshops	20%	12		
Total Internal		60		
Full Marks: 60 + 40 = 100				

Students' Responsibilities:

Each student must secure at least 60% marks separately in internal assessment and practical evaluation with 80% attendance in the class in order to appear in the Semester End Examination. Failing to get such a score will be given NOT QUALIFIED (NQ) to appear for

the Semester-End Examinations. Students are advised to attend all the classes, formal exam, test, etc. and complete all the assignments within the specified time period. Students are required to complete all the requirements defined for the completion of the course.

7. Prescribed Books and References

1. Hall, J. A. (2020). *Information Technology Auditing and Assurance* (5th ed.). Cengage Learning
2. Moeller, R. (2022). *IT Audit, Control, and Security* (3rd ed.). Wiley.
3. ISACA. (2024). *CISA Review Manual.* ISACA.
4. ISACA. (2022). *COBIT 2019 Framework: Governance and Management of Enterprise IT*. ISACA
5. Veena Hingarh and Arif Ahmed (2013), *Understanding and Conducting Information Systems Auditing*, Wiley
6. Jack J. Champlain (2003), *Auditing Information Systems*, 2nd Edition, Wiley
7. Richard Cascarino (2007), *Auditor's Guide to Information Systems Auditing*, Wiley
8. ISACA Journals
9. ISACA IT Audit Frameworks
10. NIST Special Publications
11. COBIT, CIS Frameworks, MITRE, C2M2

Pokhara University
Faculty of Science and Technology

Course Code: CMP 645 (3 Credits)
Course Title: Digital Ecosystem (3-0-0)
Nature of the course: Theory
Level: Master

Full marks: 100
Pass marks: 60
Total Lectures: 45 hrs
Program: MCE/ MSc CS

1. Course Description:

This course explores the comprehensive concept of digital ecosystems, covering their evolution, theoretical foundations, architecture, governance models, enabling technologies, sector-specific applications, and emerging trends. Students engage with real-world examples and practical assignments to understand and apply digital ecosystem strategies effectively.

2. General Objectives:

This course aims to equip students with an in-depth understanding of digital ecosystems, their components, management practices, and strategic implications, enabling students to apply ecosystem thinking effectively across business, governmental, and societal contexts.

3. Methods of Instruction:

The course employs interactive lectures, class discussions, group assignments, case studies, and presentations. Students will conduct research on various topics, prepare reports, and engage in practical design and analytical exercises.

4. Contents in Detail

Specific Objectives	Contents
Define digital ecosystems and identify their key characteristics	**Unit 1: Introduction to Digital Ecosystems (4 hrs)** 1.1 Definition and Key Characteristics 1.2 Evolution from Traditional Ecosystems to Digital Ecosystems 1.3 Components: Platform, Participants, Data, and Value 1.4 Real-world Examples (e.g., Amazon, Google, Alibaba, Smart Cities) 1.5 Overview of Nepal's digital journey (Digital Nepal Framework)
Apply theoretical concepts to analyze digital ecosystems	**Unit 2: Theoretical Foundations (5 hrs)** Introduction to Ecosystem Theory (Complex Systems Theory, Platform Theory, Network Effects Theory, Co-Evolution Theory, Innovation Ecosystem Theory)
Analyze open versus closed ecosystem architectures	**Unit 3: Architecture and Design of Digital Ecosystems (6 hrs)** 3.1 Layers: Physical, Application, Service, and Business Layers 3.2 Open vs Closed Ecosystems 3.3 API Economy and Interoperability 3.4 Data Flow and Integration in Ecosystems
Assess governance implications in managing digital ecosystems	**Unit 4: Governance and Management (5 hrs)** 4.1 Ecosystem Governance Models (Centralized Governance Model, Decentralized Governance

	Model, Hybrid Governance Model) 4.2 Platform Leadership and Orchestration 4.3 Trust, Security, and Privacy Issues
Evaluate how emerging technologies support ecosystem functionalities	**Unit 5: Technologies Enabling Digital Ecosystems (6 hrs)** 5.1 Internet of Things (IoT) and Edge Computing 5.2 Artificial Intelligence and Machine Learning (Application of AI in Digital Ecosystem) 5.3 Blockchain and Decentralization 5.4 Cloud Computing and Microservices
Identify strategic advantages of digital ecosystems in various sectors	**Unit 6: Digital Ecosystems in Different Sectors (6 hrs)** 6.1 E-commerce and Retail Ecosystems 6.2 Health and Smart City Ecosystems 6.3 Education Ecosystems (MOOCs, EdTech) 6.4 Tourism and Hospitality Ecosystems 6.5 Industrial and Manufacturing Ecosystems (Industry 4.0)
Apply ecosystem mapping and strategic positioning tools	**Unit 7: Business Models and Strategy (5 hrs)** 7.1 Platform Business Models (Transaction Platform Model, Advertising Platform Model, Data-Driven Platform Model, Product-as-a-Service) Platform Model, Social Platform Model) 7.2 Ecosystem Mapping and Strategic Positioning 7.3 Metrics for Ecosystem Health and Success 7.4 Case Studies of Failures and Successes (e.g., Nokia, Uber, Tesla, Panasonic, KODAK)
Evaluate the impact of emerging trends on future digital ecosystems	**Unit 8: Emerging Trends and Future Directions (4 hrs)** 8.1 Metaverse and Immersive Ecosystems 8.2 Ecosystemization of AI 8.3 Sustainable Digital Ecosystems (Green IT) 8.4 Digital Twin Ecosystems 8.5 Research Frontiers and Open Challenges

Practical Component / Assignments:

- **Case Study Analysis**: Choose a real-world domain digital ecosystem (e.g.: health, education, governance, fintech)
- **Ecosystem Design Project**: Design a digital ecosystem for a sector (e.g., agriculture, tourism, finance)
- **Research Paper / White Paper**: Investigate a current trend (e.g., DAOs in ecosystems, platform monopolies)
- **Group Presentation**: Emerging Technologies Shaping Future Ecosystems

5. **Evaluation system and Students' Responsibilities**

Internal Evaluation

The internal evaluation of a student may consist of assignments, attendance, internal assessment and group workshop. The internal evaluation scheme for this course is as follows:

Internal Evaluation	Weight	Marks	External Evaluation	Marks
Theory			Semester-End examination	40
Attendance & Class Participation	10%	6		
Assignments	10%	6		
Presentations/Quizzes	20%	12		
Internal Assessment	40%	24		
Group Workshops	20%	12		
Total Internal		60		
Full Marks: 60 + 40 = 100				

Student Responsibilities:
Each student must secure at least 60% marks separately in internal assessment and practical evaluation with 80% attendance in the class in order to appear in the Semester End Examination. Failing to get such a score will be given NOT QUALIFIED (NQ) to appear for the Semester-End Examinations. Students are advised to attend all the classes, formal exam, test, etc. and complete all the assignments within the specified time period. Students are required to complete all the requirements defined for the completion of the course.

6. Prescribed Books and References

Textbooks:

- Parker, G. G., Van Alstyne, M. W., &Choudary, S. P. (2016). Platform revolution: How networked markets are transforming the economy and how to make them work for you. W. W. Norton & Company.
- Cusumano, M. A., Gawer, A., &Yoffie, D. B. (2019). The business of platforms: Strategy in the age of digital competition, innovation, and power. Harper Business.
- Corallo, A., Passiante, G., &Prencipe, A. (2007). Digital business ecosystems. Edward Elgar Publishing.

Reference Books:

- Tiwana, A. (2013). Platform ecosystems: Aligning architecture, governance, and strategy. Morgan Kaufmann.
- Adner, R. (2012). The wide lens: What successful innovators see that others miss. Portfolio Penguin.
- Easley, D., & Kleinberg, J. (2010). Networks, crowds, and markets: Reasoning about a highly connected world. Cambridge University Press.