

**JYOTI NIVAS COLLEGE AUTONOMOUS  
SYLLABUS FOR 2019 BATCH AND THEREAFTER**

**Programme: M.Voc. (Banking and Finance)**

**Semester: IV**

**CYBER CRIME AND SECURITY IN BANKS AND**

**FINANCIAL INSTITUTIONS**

**Course Code: 19MVB404**

**No. of Hours: 60**

**COURSE OBJECTIVES:**

- To make students understand the importance of cyber security in banks and financial institutions.
- To familiarize students about the various kinds of cyber crime with reference to banks and financial institutions.
- To make students understand the basics of cyber forensics, investigation and cyber security.

**LEARNING OUTCOMES:**

- To enable students recognize cyber crimes in banks and financial institutions.
- To be able to report cyber crimes in the banking sector.
- To know how to deal with cyber crime problems occurring in banks and financial institutions

**UNIT I: CYBER SECURITY IN BANKS**

**12 HRS**

Introduction to Cyber Security, Implementing Hardware Based security, software based firewalls, Security Standards And best practices. Assessing threat levels, penetration Testing security controls. Preventive, Detective and Corrective Controls

**UNIT II: CYBER CRIME AND CYBER LAW IN INDIA**

**12 HRS**

Introduction to Cyber Crime, Channels of Cyber Crime-Stalking,

Cyber Squatting, Cyber Extortion, Cyber Cheating. Cyber Warfare, Cyber Terrorism, Phishing and Hacking, Software Piracy, Computer Security-Internet Crime, Internet Fraud, User Failure & causes, Bank Failure-Computer Hackers. Cyber Crime Investigation. Regulatory Compliances, Electronic Transaction and Taxation issues

**UNIT III: CYBER FRAUD AND FRAUD MANAGEMENT**

**12 HRS**

Fraud Protection Prevention Controls, Detection Controls, Mitigation Controls, Encryption/Decryption. Incidence of Cyber Crimes, Reporting, Investigation, Crime Management, Evidence Collection And Chain of Custody, Cyber Crime Risk Management- Cyber Forensics. Cyber Forensics Investigation, Digital Evidence Collection, Evidence Preservation, E-Mail Investigation, E-Mail Tracking, IP Tracking, Encryption and Decryption, Password Cracking, Recovering deleted evidence

#### **UNIT IV: ACCOUNTING FRAUDS, FORGERY AND COUNTERFEITING; 12 HRS**

Vulnerability in banks. Bank failure and its impact on the system. Case Studies.

#### **UNIT V: IT SECURITY IN BANKING 12HRS**

Introduction to Data Security, Data Security, Database Security Network. Security Controls and Management, Operating System Security Management, Models. Cryptography, Encryption, Public Key infrastructure (PKI), Key Management, Global initiatives And development.

#### **PRACTICAL COMPONENTS:**

- Write a report on cyber security on banks.
- Present a case study on accounting frauds that have been exposed in the recent past and examine where the system has failed to detect the fraud.
- Explain the procedure for reporting a cyber crime to the Cyber Crime Police Station, Bangalore.

#### **BOOKS FOR REFERENCE:**

1. Verma Amita, Cyber Crimes and Law, Central Law Publications, Allahabad, 2009.
2. Dasgupta M. Cyber Crimes In India – A Comparative Study, Eastern Law House, Kolkata, 2009.
3. Barkha and Mohan Rama U, Cyber Law and Crimes – IT Act 2000 And Computer Crime Analysis, Asia Law House, Hyderabad 2009.
4. Eoghan Casey, Digital Evidence & Computer Crime, Forensic Digital Science, Computer and the Internet, Academic Press Textbook
5. Cyber Crimes and Fraud Management, Macmillan, 2012
6. Scott Charney, The Internet, Law Enforcement and Security, Internet Policy Institute, 2001
7. Kaptan SS & Choubey NS, E-Indian Banking in Electronic Era, Sarup and Sons.
8. IIBP, Banking Technology, Indian Institute of Bankers Publication
9. Vasudeva, E-Banking, Commonwealth Publishers, New Delhi.