
# Professional Postgraduate Program in Information Security Management (PPGP-ISM)

(Autonomous, full-time, 11 months, residential Program in association with **MIEL**)

The changing technology and business environment trends have necessitated for readiness in equipping one-self to face the newer challenges. Presently most of the organizations are using IT driven business solutions for their business activities. The critical business transactions and the financial transactions are part of the most of the common IT enabled business solution requirement. The dependence on IT infrastructure and the digital information is too critical. Frequent news stories indicate that important systems are being compromised with alarming frequency. Recent legislation in various countries, including the Data Protection Act, the Regulation of Investigatory Powers Act, and the BS7799 standard on Information Security Management (now ISO27001) are forcing companies to take information security more seriously. Information security requires a clear understanding of relevant technological issues and of the social/organisational issues, as well as the relationships between them. This programme covers these concerns by offering modules that cover security technologies, incident management and support, network quality of service as well as knowledge system architecture. This program aims to provide the holistic information security knowledge with practical approach.

## Distinctive Features:

- Structured and integrated laboratory sessions to assimilate learning and enhance thereupon with cutting edge technologies and tools
- Self-placed modules to increase creativity and encourage innovation
- Module based seminar sessions to improve information analysis and representation skills
- Case-study based teaching methodologies in collaboration with industry experts
- Hands-on experience on CA eTrust, Linux OS, Firewall, Check Points, PKI software
- Industry-Academia collaboration with TIBCO, SAP, SAS and CA
- Expert lectures, seminars and case studies by leading experts from industries
- Twelve weeks full time project to enhance the understanding of real-life scenarios in chosen area of technology

## Eligibility Criteria

- Graduates with a Bachelor's Degree in Engineering / Technology in any discipline or MCA, MCM and MCS (with minimum 50 percent marks or equivalent grades).
- Basic programming knowledge in C and C++.

## Curriculum

### Basic Courses:

**CS001 / CS002 / CS003 Life Skills Development – I / II / III (Each 20 Hours):** The Life Skills Development Program prepares students for communication and interaction in an organizational set-up. The focus would be on grammar, vocabulary, spoken English, remedial English, presentation skills, debates, group discussions, team building, time management, cross-cultural communication, creative and business writing. The ultimate objective of this course is to develop individuals with high intelligence and emotional quotients who are also competent speakers of English. At the end of the Life Skills Development Program the students would be well equipped with language skills, soft skills and life skills to enter the challenging corporate world.

### Foundation Courses:

**IS501 Information Security Introduction (20 Hours):** Overview of Standards & Metrics . Introduction to Information Security. World of Cyber Crimes . Information Assets & Operations. Common Security Misnomers. Sound Canons of Information Security. Overview of Security Solutions. Information Security Program .

**IS502 Physical and Environmental Security (25 Hours):** Relevance of Traditional Security even in modern days . Safekeeping of the Data & Records. Physical Access Control. Human Issues. Nasty petty devices and related menace. Environmental Controls.

**IS503 Window Architecture (25 Hours):** Windows Origin & Development. Windows Architecture. Networking in Windows. Building solutions using MS Back-office. The WIN32 API. Processing. Memory & I/O Management.

**IS504 UNIX Architecture (25 Hours):** Operating Systems Fundamentals. Kernel & Shell. Pipes, Filters and Redirection. File System. Rich Command Set. Shell Scripts & AWK Scripts.

### Core Courses:

**IS601 Cryptography Fundamentals (30 Hours):** Introduction & Overview of Cryptography. First Visit to Cryptology – Keys, Hashing, etc. Mathematical Foundation. Digital Encryption Standard (DES). Practical Implementation of Cryptography.

**IS602 Network Security (50 Hours):** Revisiting Network fundamentals. Network Protocols. Security Concerns of Computer Network. Network Security Design. Network Security Administration. High Availability Technologies .

**IS603 Access Control (40 Hours):** Defining Access Controls. Identification, Authentication & Authorisation. Access Control Methodologies . Centralised vis-a-vis Decentralised. Access Control Techniques. Discretionary, Mandatory, Role Based, Content based. Access Control Lists & Directories.

**IS604 Internet Security (35 Hours):** Internet – Origin, Development & Current Status. Internet Security – Basic Concerns. Spectrum of Internet-based Services. Implementations of HTTP, Email, Chat, FTP, Telnet, etc. Security Concerns in Net-based Services . Security Solutions – Manual & Mechanized.

**IS605 Application Security (40 Hours):** Application Security Principles. Threats to applications. Threats Spectrum – Buffer Overruns, SQL Poisoning. Malicious Log Writing, Homograph, DOS attack, etc. Vulnerabilities – Race Conditions, Tempest, Weak ID. High privileges, Bandwidth flooding, Starvation attack, etc. Secure Design, Threat Modeling & Code Review.

**IS606 Applied Cryptography (30 Hours):** Digital Signatures & PKI. Implementation of Asymmetric Key – RSA, PGP, etc. Applied Cryptography in Web Applications. Advanced Cryptography – ECC, Quantum Crypto, etc. Security Concerns & Considerations.

**IS607 UNIX and Linux Security(30 Hours):** Open source Concerns for OS Installation. Minimizing System Services. Logging, Auditing and Automation. Access Control, Permissions and User Rights. Additional Security Configuration. Backups and Archives. The Security Infrastructure. Securing Network Services.

**IS608 Window Security (25 Hours):** Patching and Software Installation. Logging, Auditing and Automation. Warning Banners. Access Control, Permissions and User Rights. Additional Security Configuration. Backups and Archives. Security Policies and Templates. Service Packs, Patches and Backups. Securing Network Services.

**IS609 ISO 27001 and Other Security Models (30 Hours):** BS7799 as origin and ISO 27001 as its adoption by ISO. Details of ISO27001 and related models in 27000 series. Other classical models based on Clearance, Classification & Role-based Access.

**IS610 Security Certification (20 Hours):** What are Security Certifications. Professional Organizations and their membership, code of ethics, continuing skill update, furthering profession. Certification Examinations and their role in career of a professional and in expertise-building of a company . Major Exam's like CISSP, CISM, CBCP, CISA, CEH, CHFI, SSCP, LPT, ECSA, GSEC, GCIH, Security+, etc . Common Guidelines for professional certification exam's Specific areas of focus of each of these certifications Various technology-specific certifications from vendors.

## Advanced Courses:

**IS701 Web Application Security (40 Hours):** Web Communication. Web Security Protocols. Active Content & security concerns. Cracking Web Applications. Web Application Defenses.

**IS702 Firewall IDS/IPS and Honeynet (40 Hours):** Firewall as perimeter defense . Types, Merits & Applications of Firewalls. Firewall Policy & Configuration. Setting up, Maintenance & Security Review IDS & IPS. Honey-pots / Honey-nets.

**IS703 Wireless Communication and Telephony (40 Hours):** History of wireless communications. Overview of wireless technologies. Different types of telephony – Analog, Digital, Wireless, IP. Standards & Protocols. Security Concerns & counter measures. Steps in Securing A Wireless Network.

.

**IS704 Computer and Audit Assurance (40 Hours):** Origin & Progress of Computer Audit / Information Systems Audit. Objectives & Nature of IS Audit. IT Controls – A Closer Look. Administrative & Technical Controls. Assurance Function. IS Audit – Planning, Conducting & Reporting. Variants of CAAT, Control Self Assessment (CSA) etc.

**IS705: Cyber crime Investigation and Forensics (25 Hours)** Cybercrime Overview. Salient Features & Principles of Electronic Evidence. First Visit to Crime Spot – Planning and Tools. Search, Seizure, Packaging, Transport & Records. Precautions – Networked/ Standalone, Power On/ Off, etc. Imaging, Examination, Analysis & Disclosure of Evidence.

**IS706 Business Continuity and Disaster Recovery (40 Hours):** Business Reliance on IT. IT & Other Contingencies. Risk Analysis, Business Impact & Process Prioritisation. Developing BC Strategies & Emergency Response. Design & Implementing BCP. Senior Management Sanctions. Training, Implementation, Testing & Maintenance. Public Relation & Coordination with Public Authorities.

**IS707 Security Operation Center (40 Hours):** Requirements and Best Practices for a Security Operations Center (SOC). Build and Implement the SOC Technology a. Deliver Event Correlation and Monitoring Technologies for SOC.

**IS611 Cyber Law (25 Hours):** Need of Distinct Cyber Legislation. Comparative Overview of various Nations. IT Act, 2000 – as enacted in 2000 & amended in 2006. Major types of civil & criminal offences. Punishment Stipulations. Judicial Process for Administration & Amendments Case Law.

**IS708 Enterprise Security Architecture (45 Hours):** Architecture from Business, Security, Law & Human angle. Guiding Beacons of ISO 27001, Common Criterion (CC), etc. Architectural Elements - Directories, Apps Integration, SSO Security Elements – Certificate, Policy, Domains, etc. Architectural Priorities of Scalability, Availability, etc. Management of Access, Privacy, Identification, etc. Security Audit & Compliance.

**IS709 Security Incident Management (40 Hours):** Security Events & Security Incidents. Nature, Symptoms & Impact of Security Incidents. Incident Handling Process. Internal Security Organization for Incidents. External Organizations like CERT etc.

**IS612 Security Profession (20 Hours):** Security as a Profession. Roles of Process Consulting. Technical Consulting. ISO and CISO. Specializations: IS Architect, IS Engineer & IS Manager.

**IS710 Industry Perspective Seminar (20 Hours):** Industry experts and faculty will be providing case studies to prepare students for a career choice in Information Security Management domain. Students need to provide their perspectives and defend their choices for evaluation.

## Project:

**IS801 Project (300 Hours):** Students take up an industry-sponsored project or in-house project as one of the requirements of this program. For industry-sponsored projects, the Career Management Cell facilitates interaction between students and the industry. The students can also take-up the in-house projects under the guidance of the faculty and/or Industry experts in their area of expertise. Students are encouraged to work on projects that will enhance their understanding in certain technology domains in real-life scenario. The project report has to be submitted to the Institute in the prescribed format, which will be examined by experts nominated by the Institute. The project is the culmination of the student's learning in the institute and is expected to be of the high standards demanded by the industry.

**Program Structure**

| Level | Subject Code | Subject Name | Hours |
|---|---|---|---|
| **Basic** | | | |
| | CS001 | Life Skills Development - I | 20 |
| | CS002 | Life Skills Development - II | 20 |
| | CS003 | Life Skills Development - III | 20 |
| **Foundation** | | | |
| | IS501 | Information Security Introduction | 20 |
| | IS502 | Physical and Environmental Security | 25 |
| | IS503 | Window Architecture | 25 |
| | IS504 | UNIX Architecture | 25 |
| **Core** | | | |
| | IS601 | Cryptography Fundamentals | 30 |
| | IS602 | Network Security | 50 |
| | IS603 | Access Control | 40 |
| | IS604 | Internet Security | 35 |
| | IS605 | Application Security | 40 |
| | IS606 | Applied Cryptography | 30 |
| | IS607 | UNIX and Linux Security | 30 |
| | IS608 | Window Security | 25 |
| | IS609 | ISO 27001 and Other Security Models | 30 |
| | IS610 | Security Certification | 20 |
| | IS611 | Cyber Law | 25 |
| | IS612 | Security Profession | 20 |
| Advanced | | | |
| | IS701 | Web Application Security | 40 |
| | IS702 | Firewall IDS/IPS and Honeynet | 40 |
| | IS703 | Wireless Communication and Telephony | 40 |
| | IS704 | Computer and Audit Assurance | 40 |
| | IS705 | Cybercrime Investigation and Forensics | 25 |
| | IS706 | Business Continuity and Disaster Recovery | 40 |
| | IS707 | Security Operation Center | 40 |
| | IS708 | Enterprise Security Architecture | 45 |
| | IS709 | Security Incident Management | 40 |
| | IS710 | Industry Perspective Seminar | 20 |
| Project | | | |
| | IS801 | Project | 300 |
| | | | **Total Hours: 1200** |