

INFORMATION SYSTEMS SECURITY PROFESSIONALISM

Credits: 4

Year: II

Part: II

Course Objectives

This course aims to develop a deep understanding of the roles, responsibilities, and ethical foundations of an information security professional. It explores global standards, governance, legal implications, and career paths within the field of information security, preparing students for professional excellence, leadership, and compliance in cybersecurity.

Learning Outcomes	Chapter Contents	Credit Hours	Teaching Methods
<ul style="list-style-type: none"> ▪ Understand the evolving role of information security professionals in both public and private sectors. ▪ Describe the expectations placed on professionals regarding ethics, behavior, and responsibility. ▪ Identify and compare key industry certifications such as CISSP, CISM, and CEH. ▪ Explore the significance of professional conduct and codes of ethics 	<p>1 Introduction to Information Security Professionalism</p> <p>1.1 Cybersecurity as a profession 1.2 Roles and responsibilities 1.3 Codes of Ethics (ISACA, ISC², etc.) 1.4 Professional certifications (CISSP, CISM, CEH) 1.5 Professional behavior and governance</p>	10	<ul style="list-style-type: none"> ▪ Lecture presentations with multimedia content ▪ Case discussion on ethical dilemmas and career progression ▪ Seminar on industry certifications and career paths ▪ Role-play on professional code of conduct ▪ Group presentations on InfoSec roles

<p>in daily security practice.</p>			
<ul style="list-style-type: none"> ▪ Analyze and interpret national and international cybersecurity laws and policies. ▪ Explain the legal responsibilities of professionals in managing data and reporting incidents. ▪ Assess how ethical dilemmas are handled within the field of cybersecurity. ▪ Demonstrate an understanding of responsible disclosure and its impact on public trust. 	<p>2 Legal, Ethical and Regulatory Frameworks</p> <p>2.1 Cybercrime laws (Nepal, GDPR, HIPAA, etc.)</p> <p>2.2 Intellectual property, liability</p> <p>2.3 Privacy laws and compliance</p> <p>2.4 Responsible disclosure and ethical dilemmas</p>	<p>10</p>	<ul style="list-style-type: none"> ▪ Interactive lectures with real-world legal cases ▪ Case study analysis on local and international laws ▪ Panel discussion on ethical dilemmas in InfoSec ▪ Group presentation on responsible disclosure ▪ Guest lecture by a cybersecurity lawyer or policy expert
<ul style="list-style-type: none"> ▪ Apply globally recognized security frameworks (e.g., ISO 27001, NIST) to real-world governance issues. ▪ Identify the purpose and application of governance models like 	<p>3 Professional Standards and Governance</p> <p>3.1 ISO 27001, NIST Cybersecurity Framework</p> <p>3.2 COBIT, CIS benchmarks</p> <p>3.3 Security governance models</p> <p>3.4 Compliance roles and responsibilities</p> <p>3.5 Control objectives and performance evaluation</p>	<p>10</p>	<ul style="list-style-type: none"> ▪ Lectures on global frameworks and standard comparisons ▪ Workshop: Mapping COBIT/NIST/ISO to audit functions ▪ Group activity on writing sample compliance policies ▪ Case studies on governance gaps

<p>COBIT and CIS.</p> <ul style="list-style-type: none"> ▪ Align organizational roles with appropriate controls and compliance objectives. ▪ Distinguish between operational, strategic, and compliance responsibilities in IS governance. 			<ul style="list-style-type: none"> ▪ Evaluation of real audit and control structures
<ul style="list-style-type: none"> ▪ Understand and apply key components of risk assessment and mitigation strategies. ▪ Use ISO and NIST frameworks to assess risks and prioritize control efforts. ▪ Design documentation for compliance audits and stakeholder reporting. ▪ Communicate audit and risk findings professionally through structured formats. 	<p>4 Risk Management and Compliance Practices</p> <p>4.1 Risk frameworks (NIST RMF, ISO 27005)</p> <p>4.2 Risk assessment and mitigation planning</p> <p>4.3 Compliance audit planning</p> <p>4.4 Documentation and professional reporting</p>	<p>10</p>	<ul style="list-style-type: none"> ▪ Lecture sessions on risk and compliance fundamentals ▪ Group-based risk assessment simulation using ISO 27005 ▪ Hands-on activity: Writing audit documentation ▪ Presentation: Designing an enterprise compliance checklist ▪ Peer review of mock audit reports
<ul style="list-style-type: none"> ▪ Lead initiatives to build security-focused culture 	<p>5 Leadership, Communication, and Career Development</p> <p>5.1 Managing security teams</p> <p>5.2 Building a security culture</p>		<ul style="list-style-type: none"> ▪ Leadership simulation exercises

<p>and awareness in an organization.</p> <ul style="list-style-type: none"> ▪ Manage teams, communication flows, and escalation paths during security events. ▪ Develop personal strategies for professional growth and certification alignment. ▪ Understand the value of CPD (Continuing Professional Development) in long-term career success. 	<p>5.3 Incident response leadership 5.4 Career strategy and CPD planning</p>	<p>10</p>	<p>(incident handling)</p> <ul style="list-style-type: none"> ▪ Team communication drills and analysis ▪ Personal CPD roadmap creation workshop ▪ Group presentations on InfoSec career paths ▪ Guest talk by industry leaders or HR professionals
<ul style="list-style-type: none"> ▪ Explore how emerging technologies affect the professional landscape of cybersecurity. ▪ Critically examine ethical challenges arising from AI and cloud technologies. ▪ Study real-world examples of professional misconduct and identify preventive measures. 	<p>6 Professional Trends and Future Outlook</p> <p>6.1 AI in cybersecurity 6.2 Cloud governance trends 6.3 Professional misconduct and ethics case studies 6.4 Gender and diversity in cybersecurity professions</p>	<p>10</p>	<ul style="list-style-type: none"> ▪ Debate: Ethics and AI use in cybersecurity ▪ Seminar: Diversity, equity, and inclusion in InfoSec ▪ Case study review: Real-world professional misconduct ▪ Group project on cybersecurity trends and innovations ▪ Open discussion: Governance in future technologies

<ul style="list-style-type: none"> ▪ Promote inclusive practices and diverse representation in the cybersecurity workforce. 			
--	--	--	--

Practical Activities

1. Create a cybersecurity career roadmap and CPD strategy
2. Conduct a professional misconduct analysis using real case studies
3. Draft a governance policy framework for an enterprise
4. Simulate a professional audit and prepare documentation using ISO/NIST standards

Evaluation Schemes

a. Internal Evaluation

Type	Weightage
Minor tests	70%
Assignments	30%

b. Final Exam

The questions will cover all chapters of the syllabus. The evaluation scheme will be as indicated in the table:

Chapter	Hours	Mark distribution*
1	10	10
2	10	10
3	10	10
4	10	10
5	10	10
6	10	10
Total	60	60

*There may be minor deviation in marks distribution.

References

- ISACA. (2023). *CISM/CISA Review Manual*
- ISC². (2024). *CISSP Official Study Guide*
- Whitman & Mattord. (2022). *Principles of Information Security*
- Bayuk, J. L. (2010). *Cybersecurity Policy Guidebook*
- Nepal Cyber Law and IT Policy documents
- ISO 27001, NIST RMF, COBIT documentation