PAMANTASAN NG LUNGSOD NG PASIG
SECOND SEMESTER, SCHOOL YEAR 2024-2025

COLLEGE OF COMPUTER STUDIES

COURSE TITLE: Information Assurance and Security I

COURSE DESCRIPTION: This course introduces the fundamental principles of information assurance and security. It covers essential concepts, including security policies, risk management, cryptography, network security, and ethical/legal considerations in securing information systems. Students will explore tools and techniques to protect digital assets and mitigate cyber threats.

COURSE CREDITS: 3 units (2 – unit lecture and 1 – unit laboratory)

PRE-REQUISITE/S:

CONTACT HOURS: Refers to the number of hours a week

INSTRUCTOR/S: Juanito P. Alvarez Jr., Norman E. Espiritu and Ramil N. Madriaga

COURSE LEARNING OUTCOMES: Upon successful completion of this course, students will be able to:

1. Identify Fundamental Security Concepts Explain the principles of confidentiality, integrity, and availability (CIA). Distinguish between various types of threats, vulnerabilities, and attacks on information systems and conduct Risk Assessments and Develop Security Policies
2. Analyze potential risks and evaluate their impact on organizational assets. Design and implement effective security policies, standards, and procedures based on industry frameworks. Apply Cryptographic Techniques
3. Utilize encryption algorithms to secure data in transit and at rest. Implement digital signatures and hashing techniques for data integrity and authentication. Implement Network Security Measures.
4. Configure firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS). Develop strategies to secure wireless and wired networks against cyber threats. Enhance Application Security.
5. Identify and mitigate common application-level vulnerabilities such as SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF). Integrate secure coding practices in software development processes. Plan and Respond to Security Incidents.
6. Develop and execute incident response plans to minimize damage from cybersecurity breaches. Create disaster recovery and business continuity plans to ensure operational resilience. Understand Legal and Ethical Issues.
7. Explain the implications of cybersecurity laws, regulations, and compliance requirements. Evaluate ethical dilemmas and privacy issues in the context of information security. Recognize Emerging Trends and Technologies in Security

8. Explore the role of artificial intelligence, Internet of Things (IoT), and cloud computing in modern security landscapes. Assess current and future challenges in cybersecurity.

EVIDENCE OF LEARNING

1. Knowledge-Based Evidence:
    - Students can clearly articulate the principles of confidentiality, integrity, and availability (CIA), along with real-world examples of how they are applied.
    - Ability to identify different types of threats, vulnerabilities, and attacks in various scenarios.
    - Accurately define key security concepts and differentiate between them.
2. Skill-Based Evidence
    - Students analyze case studies or incidents and map the security lapses to failures in the CIA principles or specific vulnerabilities.
    - Implement encryption techniques or access controls to ensure confidentiality in a lab setting.
    - Use tools like checksum or hash generators to validate data integrity.
    - Create a disaster recovery plan to address availability concerns.
    - Perform mock assessments of a system to identify potential threats and suggest mitigations..
3. Assessments and Assignments
    - Questions testing comprehension of CIA principles, threat types, and security measures.
    - Develop a simple security policy to address specific organizational risks.
    - Simulate a phishing attack scenario and design strategies to prevent it.
    - Hands-on activities demonstrating the application of cryptographic tools or network security configurations..
4. Collaborative and Communication Evidence
    - Participation in class discussions on real-world cybersecurity breaches and their implications on confidentiality, integrity, and availability.
    - Delivering presentations explaining key security concepts and applying them to hypothetical or real-world scenarios.
5. Reflection and Critical Thinking
    - Writing reflective journals or logs explaining their understanding of security principles and their relevance in mitigating cyber risks.
    - Evaluating the effectiveness of security measures in given scenarios and suggesting improvements.

Date of Submission: Week 18

Articulate the Final Project of the Subject. The final project is equivalent to the Final Examination if deemed necessary. In support of Academic Program and Subject Matter expertise, it is the teacher-in charge who decides on the final assessment. Should the teacher decide on a Final Project, the project can be a product/output-oriented or process/performance-oriented.

LEARNING PLAN

Time Frame	Intended Learning Outcomes	Course Contents	Teaching and Learning Activities	Evidence of Learning/Output (Summative/Formative Assessment/Performance Assessment	Learning Resources
Week 1 (Jan 27- Feb 2)	✓ Students are oriented about the course requirements. ✓ Understand Fundamental Concepts	✓ Course Orientation ✓ Overview of the Subject and Requirement of the course. ✓ Comprehend the course's framework and its governing principles. ✓ Introduction to Information Assurance and Security •	✓ Discussion on expectations of the course, subject requirements including the scheduled dates of submission. ✓ . Provide a high-level introduction to information assurance and security, focusing on its importance in protecting assets and data.	✓ Lectures ✓ Demonstrations ✓ Presentations	✓ Course Outline ✓ PowerPoint presentation ✓ https://www.sentinelone.com/ cybersecurity-101/cybersecurity/what-is-information -assurance/ ✓ https://sharedassessments.org/ glossary/ information-assurance-and-security/ ✓ https://www.futureoftech.org/ cybersecurity/2-history-of-cybersecurity/ ✓ https://www.linkedin.com/ pulse/ evolution-cybersecurity-brief-history-future-outlook-win-upskill
Week 2-3 (Feb 3-16)	✓ Explain the purpose and significance of information assurance (IA) and its role in protecting data and systems. ✓ Assess hypothetical scenarios	**INFORMATION SECURITY SYSTEM** ✓ Overview of Information Assurance (IA) and Security	✓ Deliver structured presentations on key topics such as the CIA triad, cryptographic methods, risk management, and network	✓ Assignment ✓ Class Participation ✓ Laboratory Exercise	✓ https://www.secondstartechnologies.com/blog/2024/01/the-evolution-of-cybersecurity-staying-ahead-of-

	to identify potential risks, vulnerabilities, and applicable mitigation strategies. ✓ Evaluate case studies to determine which aspect of confidentiality, integrity, or availability was compromised. ✓ Create simple security policies (e.g., password management or acceptable use policies) to address specific risks. ✓ Analyze various types of threats and attacks to determine their impact on information systems and suggest appropriate defenses. ✓ Integrate knowledge of security principles and terminology to recommend best practices for securing systems and data.	✓ Goals of IA: Confidentiality, Integrity, Availability ✓ Types of Threats and Attacks ✓ Basic Security Terminology	security ✓ Explain the CIA triad with simple, relatable examples (e.g., confidentiality as a password, integrity as unaltered data, availability as a functional website). ✓ Present hypothetical situations (e.g., a leaked database or server downtime) and have students determine which CIA goal is impacted. ✓ Discuss common threats (e.g., phishing, malware, DoS attacks) and show a video or simulation of a phishing attempt. ✓ Create a list of threats and ask students to classify them as human, natural, or technical. ✓ Introduce key terms such as vulnerability, exploit, attack, mitigation, and firewall with examples. ✓ Introduce frameworks like ISO 27001 or NIST and explain their role in guiding security policies.	✓ Quizzes	emerging-threats ✓ https://destcert.com/resources/five-pillars-information-security/ ✓ https://www.6clicks.com/resources/answers/what-are-the-5-components-of-information-security-management ✓ https://www.geeksforgeeks.org/information-assurance-vs-information-security/
Week 4-5 (Feb 17-March 2)	✓ Understand Risk Assessment and Analysis. ✓ Develop and Interpret Security Policies and Standards	**RISK MANAGEMENT AND SECURITY FRAMEWORKS** ✓ Risk Assessment and	✓ Lecture and demonstration on Risk Assessment Fundamentals ✓ Lecture on Policy Design	✓ Assignment ✓ Class Participation ✓ Laboratory Exercise ✓ Quizzes	✓ Wadhwa, P. (2024, November 6). Information Assurance vs Cybersecurity:

	✓ Describe the structure, purpose, and application of security frameworks such as ISO 27001 and NIST ✓ Grasp Cryptography Fundamentals ✓ Differentiate between symmetric and asymmetric encryption techniques, including their use cases, strengths, and weaknesses ✓ Conduct Risk Assessments ✓ Create security policies and standards tailored to organizational needs and aligned with security frameworks	Analysis ✓ Risk Management and Security Policies ✓ Developing Security Policies and Standards ✓ Security Frameworks (ISO 27001, NIST)	✓ Introduction to Frameworks Lecture ✓ Introduce cryptographic concepts such as encryption, decryption, keys, and ciphers. ✓ Visual Demonstrations ✓ Explain the differences between symmetric and asymmetric encryption, highlighting their use cases, advantages, and limitations		Differences & Similarities. Sprinto. https://sprinto.com/blog/information-assurance-vs- ✓ Morris, E. (2023, May 3). Balancing the CIA triad: addressing trade-offs and conflicting priorities. TechSpective. https://techspective.net/2023/05/03/balancing-the-cia-triad-addressing-trade-offs-and-conflicting-priorities/ ✓ Exabeam. (2025, January 6). What is Information Security (InfoSEC)? Goals, types and applications | Exabeam. https://www.exabeam.com/explainers/information-security/information-security-goals-types-and-applications/ ✓ Box News. (2021, May 15). The information security lifecycle. Box Blogs. https://blog.box.com/information-security-

					lifecycle
Week 6 – 7 (March 3-16)	✓ Utilize Cryptographic Methods ✓ Analyze and Apply Security Frameworks ✓ Compare Cryptographic Techniques ✓ Understand the Role of Hashing and Digital Signatures ✓ Identify the core principles and operational differences between DES, AES, and RSA encryption algorithms ✓ Explain how cryptography is applied in areas such as secure email, e-commerce, blockchain, digital certificates, and VPNs. ✓ Understand Network Security Fundamentals ✓ Define fundamental network security concepts, such as authentication, access control, encryption, and secure protocols (e.g., HTTPS, SSH). ✓ Perform hashing operations to verify data integrity using tools or programming libraries ✓ Encrypt and decrypt data using DES, AES, and RSA algorithms in real-world scenarios. ✓ Demonstrate the implementation of cryptographic practices in various software tools and systems.	**CRYPTOGRAPHY** ✓ Network Security ✓ Basics of Network Security ✓ Cryptography Fundamentals ✓ Symmetric vs. Asymmetric Cryptography ✓ Hashing and Digital Signatures ✓ Encryption Algorithms: DES, AES, RSA ✓ Applications of Cryptography	✓ Lecture on Hashing and Digital Signatures. Show examples of hash generation using online tools or software ✓ Assign students to generate hashes for files or text and verify their integrity using a tool ✓ Provide a scenario where students identify how digital signatures prevent tampering in document transmission ✓ Lecture with Algorithm Comparison ✓ Discuss the key goals of network security ✓ Introduce basic network security measures, such as firewalls, IDS/IPS, and VPNs ✓ Lecture on Network Security Fundamentals	✓ Assignment ✓ Class Participation ✓ Laboratory Exercise ✓ Quizzes	✓ FOTRA | Terranova Security. (2024, November 29). 9 examples of social engineering attacks. Terranova Security. https://www.terranovasecurity.com/blog/examples-of-social-engineering-attacks ✓ Verizon. (2023). 2023 Data Breach Investigations Report (DBIR). Retrieved from https://www.verizon.com/business/resources/reports/dbir/ ✓ Kaspersky. (2024). What is Social Engineering? Retrieved from https://www.kaspersky.com/resource-center/definitions/what-is-social-engineering ✓ Federal Trade Commission (FTC). (2023). How to Recognize and Avoid Phishing Scams. Retrieved from https://www.consumer.ftc.gov/articles/how-

	✓ Develop comprehensive strategies that combine cryptographic principles with network security techniques to protect data and systems effectively.				recognize-and-avoid-phishing-scams
Week 8 (March 17-23)	✓ Explain the functions and differences between firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS). ✓ Identify the common threats to wireless networks, such as eavesdropping, rogue access points, and man-in-the-middle attacks. ✓ Explain how VPNs ensure secure communication over public networks by encrypting data and masking user identities. ✓ Configure and Deploy Firewalls, IDS, and IPS ✓ Secure Wireless Networks ✓ Deploy and Use Virtual Private Networks (VPNs) ✓ Evaluate Network Security Tools and Techniques	**NETWORK SECURITY SYSTEM AND DEVICES** ✓ Firewalls, IDS, and IPS ✓ Securing Wireless Networks ✓ Virtual Private Networks (VPNs)	✓ Lecture on Firewall, IDS, and IPS Basics ✓ Hands-On Lab ✓ Group Discussion ✓ Lecture on Wireless Network Threats and Security Measures ✓ Lecture on VPN Fundamentals ✓ Security Challenge or Hackathon	✓ Assignment ✓ Class Participation ✓ Laboratory Exercise ✓ Quizzes	✓ Britannica, T. Editors of Encyclopaedia. (n.d.). *History of cryptology*. Encyclopedia Britannica. Retrieved February 3, 2025, from https://www.britannica.com/topic/cryptology/History-of-cryptology ✓ GeeksforGeeks. (2025, January 6). RSA Algorithm in Cryptography. GeeksforGeeks. https://www.geeksforgeeks.org/rsa-algorithm-cryptography/ ✓ https://www.imperva.com/learn/data-security/information-security-infosec/
Week 9 (March 24-30, 2025) – MIDTERM EXAMINATION					
Week 10-11 (March 31-April 13)	✓ Understand the Fundamentals of Application Security	**APPLICATION SECURITY**	✓ Lecture on Web Application Security Principles, discuss	✓ Assignment ✓ Class Participation	✓ https://www.geeksforgeeks.org/network-

	✓ Understand the Secure Software Development Life Cycle (SDLC) ✓ Apply input validation, output encoding, and secure authentication mechanisms to protect web applications. ✓ Develop secure software by incorporating threat modeling, code reviews, and security testing into the development process. ✓ Perform vulnerability assessments to detect SQL Injection, XSS, and CSRF in a sample web application. ✓ Evaluate Application Security Practices	✓Securing Web Applications ✓Secure Software Development Life Cycle (SDLC) ✓Common Vulnerabilities: SQL Injection, XSS, CSRF	techniques such as input validation, secure authentication, and session management ✓ Lecture on Secure SDLC. Introduce the stages of the SDLC and explain how security can be integrated at each stage (e.g., threat modeling, code reviews, security testing). ✓ Facilitate a discussion on the trade-offs between security and development speed in real-world software projects. ✓ Lecture on Common Vulnerabilities ✓ Assign students to design, build, and secure a small web application, incorporating secure coding practices, addressing vulnerabilities, and using an SDLC approach.	✓ Laboratory Exercise ✓ Quizzes	security- best-practices/?utm ✓ https://amatas.com/blog/cybersecurity-challenges- in-2024-key-issues-and-solutions/ ✓ https://novotech.com/blogs/news/safeguarding-your-wi- fi-the-importance-of-wireless-network-security
Week 12-13 (April 14-27)	✓ Understand Incident Response (IR) ✓ Comprehend Disaster Recovery (DR) and Business Continuity ✓ Develop an Incident Response Plan ✓ Analyze an organization's current incident response and disaster recovery capabilities and identify gaps. ✓ Design a unified framework that	**Incident Counter-Measure** ✓ Incident Response and Disaster Recovery ✓ Incident Response Planning ✓ Disaster Recovery and Business Continuity Plans	✓ Introduce the principles of incident response (IR) and disaster recovery (DR). ✓ Explain their importance in maintaining organizational resilience. ✓ Ask students to identify potential threats that could lead to incidents or disasters and how they might respond. ✓ Guide students through the	✓ Assignment ✓ Class Participation ✓ Laboratory Exercise ✓ Quizzes	✓ **https://www.esecurityplanet.com/compliance/it-security-policies/#:~: text=The%20ultimate% 20goal%20of%20an%20IT%20security%20policy%20is%20to,risks%20are%20controlled%**

	integrates incident response, disaster recovery, and business continuity for seamless execution during crises. ✓ Ensure compliance with relevant legal, regulatory, and industry standards.	✓ Case Studies in Incident Response	process of creating an IRP, including preparation, detection, analysis, containment, eradication, and recovery. ✓ Have students create an incident response plan for a hypothetical organization, detailing roles, communication workflows, and escalation procedures. ✓ Explain the purpose of disaster recovery plans (DRPs) and business continuity plans (BCPs). ✓ Assign groups to develop a DRP and BCP for a specific scenario (e.g., server crash, natural disaster, or prolonged power outage). ✓ Present students with high-profile incidents (e.g., Equifax data breach, WannaCry ransomware attack). ✓ Divide students into teams (incident response team, stakeholders, attackers) to simulate and respond to an incident based on a real-world case study.		**20and%20managed** ✓ **https://aptien.com/en/kb/articles/what-are-risk-assessment-scales** ✓ **https://www.isms.online/iso-27001/risk-assessment/** ✓ Intervalle Technologies. (2024, July 11). Cybersecurity and data privacy: the best practices. https://intervalle-technologies.com/blog/cybersecurity-and-data-privacy-best-practices/#:~:text=Network%20security%20is%20the%20practice%20of%20securing,and%20availability%20of%20data%20transmitted%20over%20networks. ✓ Thoma. (2021, April 19). 5 Applications of Digital Signatures. https://levelup.gitconnected.com/5-applications-of-digital-signatures-4e785d22d439

Week 14-15 (April 28-May 11)	✓ Understand Cybersecurity Laws and Regulations. ✓ Identify and explain key global and regional cybersecurity laws and regulations, such as GDPR, HIPAA, CCPA, and others. ✓ Explain the concept of digital privacy and its significance in the modern era. ✓ Analyze scenarios to determine whether they comply with relevant cybersecurity laws and regulations. ✓ Evaluate Ethical Dilemmas in Information Security ✓ Evaluate the ethical and legal implications of organizational cybersecurity policies and practices. ✓ Integrate Legal, Ethical, and Privacy Considerations	**INFORMATION SECURITY LAWS AND LEGAL ASPECT** ✓Legal, Ethical, and Social Aspects ✓Cybersecurity Laws and Regulations ✓Ethical Considerations in Information Security ✓Privacy Issues in the Digital Age	✓ Lecture on Cybersecurity Legal Frameworks ✓ Provide an overview of key cybersecurity laws and regulations, such as the GDPR, HIPAA, CCPA, and local laws relevant to the students' region. ✓ Assign students to research cybersecurity laws applicable in their country or region and present their findings. ✓ Cover ethical principles such as confidentiality, integrity, and accountability in the context of cybersecurity ✓ Discuss the ethical dilemmas security professionals might face (e.g., privacy vs. surveillance). ✓ Explain the concept of digital privacy, highlighting threats such as data tracking, social media privacy concerns, and surveillance. ✓ Assign students to analyze privacy policies of popular online platforms and critique their user-friendliness and transparency.	✓ Assignment ✓ Class Participation ✓ Laboratory Exercise ✓ Quizzes	✓ **https://www.mycvcreator.com/blog/the-role-of-privacy-policies-in-building-user-trust** ✓ **https://www.varonis.com/blog/risk-management-framework#the-6-risk-management-framework-rmf-steps** ✓ https://www.ibm.com/think/topics/cryptography ✓ SentinelOne. (2024, October 16). What is Information Assurance? Benefits & Challenges. https://www.sentinelone.com/cybersecurity-101/cybersecurity/what-is-information-assurance/ ✓ Exabeam. (2024, July 3). The 12 elements of an Information Security Policy | Exabeam. https://www.exabeam.com/explainers/information-security/the-12-elements-of-an-

					information-security-policy/
Week 16-17 (May 12-25)	✓ Understand Emerging Trends in Security including artificial intelligence (AI), Internet of Things (IoT) security, and cloud security ✓ Comprehend the Role of Artificial Intelligence in Security how AI is applied in cybersecurity, such as in threat detection, behavior analysis, and automated response systems. ✓ Discuss the limitations and ethical concerns of using AI in security practices. ✓ Explain the security risks and vulnerabilities associated with IoT devices and networks. ✓ Understand the unique security challenges in cloud environments, including data breaches, shared responsibility, and misconfigurations. ✓ Analyze the effectiveness of AI-based solutions in enhancing security measures. ✓ Propose strategies to secure IoT systems against common threats like malware, DDoS attacks, and unauthorized access. ✓ Critically assess the impact of	**EMERGIMG TRENDS IN INFORMATION SECURITY** ✓Artificial Intelligence in Security ✓Internet of Things (IoT) Security ✓Cloud Security	✓ Lecture on Trends and Innovations, provide an overview of emerging trends in cybersecurity, such as AI applications, IoT, and cloud security challenges. ✓ Facilitate a brainstorming session where students identify potential future trends in cybersecurity and their possible implications. ✓ Explain how AI is used for threat detection, predictive analysis, and automated incident response. ✓ Discuss examples of AI tools like Darktrace, Cylance, or IBM Watson for cybersecurity. ✓ Discuss common security challenges in IoT environments, such as weak authentication, insecure communication, and lack of updates. ✓ Explain key cloud security concepts, including shared responsibility, encryption, and access control. ✓ Organize a hackathon where students build and secure a small IoT or cloud-based	✓ Assignment ✓ Class Participation ✓ Laboratory Exercise ✓ Quizzes	✓ https://www.sentinelone.com/cybersecurity-101/cybersecurity/what-is-information-assurance/ ✓ https://www.slideshare.net/slideshow/information-assurance-and-security-chapter-1-lesson-1-237603171/237603171 ✓ https://www.terranovasecurity.com/blog/examples-of-social-engineering-attacks ✓ SentinelOne. (2025, February 6). Information Security risk assessment: benefits & challenges. https://www.sentinelone.com/cybersecurity-101/cybersecurity/information-security-risk-assessment/

	emerging technologies such as AI, IoT, and cloud computing on the overall cybersecurity landscape. ✓ Develop a comprehensive security strategy that integrates emerging technologies while addressing associated risks.		system while addressing potential threats.		
Week 18 (May 26-31, 2025) – FINAL EXAMINATION					

READINGS AND REFERENCES

1. Abante, M. A. (2024). Information Assurance and Security (1st Edition)
2. Whitman, M. E., & Mattord, H. J. (2021). Principles of Information Security (7th Edition).
3. ISO/IEC 27005: Information Security Risk Management (ISO 27005)
4. Whitman, M. E., & Mattord, H. J. (2021). Principles of Information Security (7th Edition).
5. Stallings, W. (2020). Cryptography and Network Security (8th Edition).
6. Easttom, C. (2022). Computer Security Fundamentals (4th Edition).
7. Sharma, A., & Hegde, M. (2021). Artificial Intelligence and Cybersecurity.
8. Chou, D. C. (2020). Cloud Computing: Security and Governance Issues.

COURSE REQUIREMENTS

Quizzes, Active class participation, Reflection Papers, Assignments, Midterm Exam, and Final Project

GRADING SYSTEM

Criteria	**Midterm**	**Final Grading Period**
Class Standing	**60%**	**60%**
Quizzes	20%	20%
Attendance	5%	5%
Lab Activity	25%	25%
Recitation/Participation/Seat works/	10	10%
Major Examination (Midterm/Final Exam)	**40%**	**40%**

CLASSROOM POLICIES:

1. **Policy on Attendance and Tardiness**
2. **Policy on Missed Exams and Assignments**
3. **Class Participation**
4. **Submission of Requirements**
5. **Academic Dishonesty**

Prepared by:

Juanito P. Alvarez Jr.

Norman Espiritu

Norman E. Espiritu

Ramil N. Madriaga

Faculty

Noted by:

Department Chairperson

Approved by:

RIEGIE D. TAN
College Dean