	Universitas Negeri Surabaya Faculty of Engineering, Bachelor of Information Systems Study Program	Document Code

SEMESTER LEARNING PLAN

Courses	CODE	Course Family	Credit Weight			SEMESTER	Compilation Date
Information Systems Security	5720102017		T=2	P=0	ECTS=3.18	4	July 17, 2024

AUTHORIZATION	SP Developer	Course Cluster Coordinator	Study Program Coordinator
	.....	.....	I Kadek Dwi Nuryana, S.T., M.Kom.

Learning model	**Project Based Learning**

Program Learning Outcomes (PLO)

PLO study program that is charged to the course

Program Objectives (PO)

PO - 1	Students are expected to understand the practical aspects of being an effective information security manager
PO - 2	Students know and are able to understand the use of complex security functions, such as digital forensics, incident response, and security architecture
PO - 3	Students know the concept and how to balance costs and risks appropriately

PLO-PO Matrix

P.O
PO-1
PO-2
PO-3

PO Matrix at the end of each learning stage (Sub-PO)

P.O	Week															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
PO-1																
PO-2																
PO-3																

Short Course Description	In this course, things that must be considered and carried out in implementing information system security are discussed. A number of other relevant aspects were also discussed, such as information system risk management and information system control evaluation.

References

Main :

1. Camplbell, Tony. 2016. Practical Information Security Management: A Complete Guide to Planning and Implementation,Burns Beach,Australia
2. Kemenkominfo, 2015, INDEKS KAMI. JAKARTA

Supporters:

Supporting lecturer	Rahadian Bisma, S.Kom., M.Kom.

Week-	Final abilities of each learning stage (Sub-PO)	Evaluation		Help Learning, Learning methods, Student Assignments, [Estimated time]		Learning materials [References]	Assessment Weight (%)
		Indicator	Criteria & Form	Offline (*offline*)	Online (*online*)		
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)

1	Evolution of the Profession	1. history of the information security profession 2. Risks and Consequences	**Form of Assessment** : Participatory Activities	Approach: Scientific Model: Cooperative Method: Discussion, Presentation 2 X 50	Approach: Scientific Model: Cooperative Method: Discussion, Presentation 2 X 50	**Material:** Evolution of the Profession **Reference:** *Ministry of Communication and Information, 2015, OUR INDEX. JAKARTA*	4%
2	Information System Security Threats and Vulnerabilities	1. Threat 2. Vulnerability 3. The sophistication and capabilities of cybercriminals are now greater than ever, with technically superior threat actors researching and developing malicious malware frameworks that allow them or their Customers to break into their victims‘ systems, maintain access, cover their tracks, evade countermeasures and sucking up gigabytes of classified information to sell on the black market. This chapter discusses the various threats and vulnerabilities that affect us every day, including man-made ones and natural threats that are often overlooked when considering information security.	**Form of Assessment** : Participatory Activities	Approach: Scientific Model: Cooperative Method: Discussion, Presentation 2 X 50	Approach: Scientific Model: Cooperative Method: Discussion, Presentation 2 X 50	**Material:** Information System Security Threats and Vulnerabilities **Reference:** *Ministry of Communication and Information, 2015, OUR INDEX. JAKARTA*	7%

3	Security Manager	1. The role of the information security manager 2. career development 3. how to become an information security manager 4. Dive into the role of an information security manager and see what they have to do day to day. We also focus on how information security managers can manage the skills and competencies of their teams using recognized skills frameworks and how professionalism within the security sector can be used to elevate all of our roles as security officers from the traditional IT sphere into a profession. All his own. We'll also look at some common myths and misconceptions associated with professional training courses and academic courses and how they relate to your career development plans, concluding this chapter with a quick look at what an information security management system is.	**Form of Assessment** : Participatory Activities	Approach: Scientific Model: Cooperative Method: Discussion, Presentation 2 X 50	Approach: Scientific Model: Cooperative Method: Discussion, Presentation 2 X 50	**Material: Library** Security Manager : *Ministry of Communication and Information, 2015, OUR INDEX. JAKARTA*	4%

4	Information Security as a Business Function	1. Security in Organizational Structures 2. Work with Specialist Groups 3. Working with Standards and Regulations 4. Working with Risk Management 5. Working with Enterprise Architecture 6. Work with Facilities Management 7. looks at how information security managers can embed security as a function in the business, ensuring that we align all people, processes and technology to security outcomes that support the business and its strategic needs. We will look at the traditional organizational structures that we see every day in business, looking at how to layer security into these structures to ensure that we cover all aspects of risk, not just those related to cyber. This chapter takes a deeper look at risk management, business continuity management and enterprise architecture, explaining the role of security in each of these business functions. The chapter concludes with a brief explanation of how security can be integrated with facilities management		Approach: Scientific Model: Cooperative Method: Discussion, Presentation 2 X 50	Approach: Scientific Model: Cooperative Method: Discussion, Presentation 2 X 50	**Material:** Information Security as a Business Function **Reference:** *Ministry of Communication and Information, 2015, OUR INDEX. JAKARTA*	4%

5	Information Security Implementation	1. Integration with Risk Management 2. Risk Language 3. Use Existing Frameworks 4. Safe Development 5. Security Architecture Awareness 6. Security Requirements 7. Organization Interface 8. Information security implementation goes into more detail about how information security managers can integrate security team functions with functions provided by the rest of the organization, such as risk management, architecture and software development. Most importantly, this chapter looks at the concept of security requirements as opposed to security controls, showing you how to elicit security requirements at the project initiation stage to ensure that threats, vulnerabilities, and risks are addressed by design and not as an afterthought.	**Form of Assessment** : Participatory Activities	Approach: Scientific Model: Cooperative Method: Discussion, Presentation 2 X 50	Approach: Scientific Model: Cooperative Method: Discussion, Presentation 2 X 50	**Material:** Implementation of Information Security **Reference:** *Ministry of Communication and Information, 2015, OUR INDEX. JAKARTA*	4%
6	Information Security Implementation	1. Integration with Risk Management o Risk Language o Use Existing Frameworks 2. Secure Development Security Architecture Awareness Security Requirements 3. Organization Interface	**Form of Assessment** : Participatory Activities	Scientific Approach, Model, Cooperative, Method, Discussion, Presentation 2x50	Scientific Approach, Model, Cooperative, Method, Discussion, Presentation 2x50	**Material:** Implementation of Information Security **Reference:** *Ministry of Communication and Information, 2015, OUR INDEX. JAKARTA*	4%

7	Guidelines and Legislative Standards Framework	1. Why Do We Need Standards? 2. Legislation 3. Standard ISO / IEC 27000 standard 4. Business continuity 5. Risk Management Standards 6. COBIT 7. As a foundation of everything we do in security, especially when operating in the role of information security manager, we need to justify what we impose on the business from a risk reduction standpoint. In a world where threats and vulnerabilities impact what we do every day, there are now many standards, frameworks, guidelines and national laws that drive what we must do to meet specific industry or legal requirements. Chapter 6 discusses the various international standards and guidelines that affect our organization, assessing their value to you as an information security manager as well as their value to the industry at large.	**Form of Assessment** : Participatory Activities	Approach: Scientific Model: Cooperative Method: Discussion, Presentation 6 X 50	Approach: Scientific Model: Cooperative Method: Discussion, Presentation 6 X 50	**Material:** Standard Guidelines and Legislation Framework **Reference:** *Ministry of Communication and Information, 2015, OUR INDEX. JAKARTA*	4%
8	UTS/USS		**Form of Assessment** : Project Results Assessment / Product Assessment	UTS 2 X 50	UTS 2 X 50	**Material:** UTS **Library:**	20%
9	Guidelines and Legislative Standards Framework	1. Why Do We Need Standards? 2. Invitational legislation 3. Standard ISO / IEC 27000 standard 4. Business continuity 5. Risk Management Standards 6. COBIT	**Form of Assessment** : Participatory Activities	Scientific Approach , Model, Cooperative, Method, Discussion, Presentation 2x50	Scientific Approach , Model, Cooperative, Method, Discussion, Presentation 2x50	**Material:** Information Protection **Bibliography:** *Campbell, Tony. 2016. Practical Information Security Management: A Complete Guide to Planning and Implementation, Burns Beach, Australia*	4%

10	Guidelines and Legislative Standards Framework	1. Why Do We Need Standards? 2. Legislation 3. Standard ISO / IEC 27000 standard 4. Business continuity 5. Risk Management Standards 6. COBIT	**Criteria:** 7 **Form of Assessment** : Participatory Activities	Scientific Approach , Model, Cooperative, Method, Discussion, Presentation 2x50	Scientific Approach , Model, Cooperative, Method, Discussion, Presentation 2x50	**Material:** Standard Guidelines and Legislation Framework **Reference:** *Ministry of Communication and Information, 2015, OUR INDEX. JAKARTA*	4%
11	Information Protection	1. Information Classification 2. Business Impact Level 3. Carrying out Information Classification 4. Strategic Implementation 5. Identification, Authentication and Authorization 6. Access Control Model 7. Authority System 8. Delegation of Privileges 9. Information is the lifeblood of modern businesses, no matter whether they trade travel insurance, government secrets, building, and construction or advanced education information is at the heart of making these businesses work. Chapter 7 looks at how we can build systems to help protect critical information within our organizations, taking into account the sensitivity of the data and the access control systems we can use to ensure that only those who need access get it.	**Form of Assessment** : Participatory Activities	Approach: Scientific Model: Cooperative Method: Discussion, Presentation 2 X 50	Approach: Scientific Model: Cooperative Method: Discussion, Presentation 2 X 50	**Material:** Information Protection **Bibliography:** *Campbell, Tony. 2016. Practical Information Security Management: A Complete Guide to Planning and Implementation, Burns Beach, Australia*	7%
12	Protection of People	1. Human Vulnerability 2. Social Engineering 3. Building a Security Culture 4. Negligent staff 5. Surfing and Eavesdropping Rules 6. Code Behavior 7. Employment Contracts 8. Personnel Security Life Cycle 9. Deployment 10. Choice 11. Performance and Succession 12. Transition	**Form of Assessment** : Participatory Activities	Approach: Scientific Model: Cooperative Method: Discussion, Presentation 2 X 50	Approach: Scientific Model: Cooperative Method: Discussion, Presentation 2 X 50	**Material:** People Protection **Reference:** *Campbell, Tony. 2016. Practical Information Security Management: A Complete Guide to Planning and Implementation, Burns Beach, Australia*	4%

13	Protection of Premises	1. What is Physical Security? 2. Physical Security in ISO/IEC 27001:2013 3. Start with a Risk Assessment 4. Threats and Vulnerabilities 5. Complete the Risk Assessment 6. Design Perimeter 7. Barriers, Walls, and Fences 8. Mailrooms and Loading Bays 9. Security 10. CCTV 11. Lighting 12. Offices, field locations, and data centers can all be weak points in operations where attacks can occur. In this meeting we look at the physical security measures we can take to defend and defend our facilities, including key considerations information security managers must have when working with experts on facilities management teams, business executives and law enforcement to help protect our physical security. Environment.		Approach: Scientific Model: Cooperative Method: Discussion, Presentation 4 X 50	Approach: Scientific Model: Cooperative Method: Discussion, Presentation 4 X 50	**Material:** Protection of Premises **Bibliography:** *Campbell, Tony. 2016. Practical Information Security Management: A Complete Guide to Planning and Implementation, Burns Beach, Australia*	4%
14	1. Protection of Premises 2. Protection of Systems	1. What is Physical Security? Physical Security in ISO / IEC 27001: 2013 2. Start with Risk Assessment, Threats and Vulnerabilities, Complete Risk Assessment, Design Perimeter, Barriers, Walls and Fences, Mailrooms and	**Form of Assessment** : Participatory Activities	Scientific Approach, Model, Cooperative, Method, Discussion, Presentation 2x50	Scientific Approach, Model, Cooperative, Method, Discussion, Presentation 2x50	**Material:** Protection of Premises **Bibliography:** *Campbell, Tony. 2016. Practical Information Security Management: A Complete Guide to Planning and Implementation, Burns Beach, Australia*	4%

15	Protection of Systems	1. Introducing Malware 2. What is Malware? 3. Classification of Malware 4. Active Content Attacks 5. Threat vector 6. Technical Countermeasures 7. Network security 8. What is a Firewall? 9. Demilitarized Zone (DMZ) 10. Network Encryption 11. Wireless network 12. technical controls that information security managers need to know within an enterprise architecture, ensuring a reasonable base of security knowledge can be added to the security arsenal. This will help information security managers as they have conversations with technical teams, such as network engineers, Windows operating system experts and database administrators, ensuring information security managers can speak their language while translating technical risks into meaningful security controls.		Approach: Scientific Model: Cooperative Method: Discussion, Presentation 2 X 50	Approach: Scientific Model: Cooperative Method: Discussion, Presentation 2 X 50	**Material:** Protection of Systems **Reader:** *Campbell, Tony. 2016. Practical Information Security Management: A Complete Guide to Planning and Implementation, Burns Beach, Australia*	4%
16	UAS		**Form of Assessment** : Project Results Assessment / Product Assessment	UAS 2 X 50	UAS 2 X 50	**Material:** UAS **Literature:**	30%

Evaluation Percentage Recap: Project Based Learning

No	Evaluation	Percentage
1.	Participatory Activities	50%
2.	Project Results Assessment / Product Assessment	50%
		100%

Notes

1. **Learning Outcomes of Study Program Graduates (PLO - Study Program)** are the abilities possessed by each Study Program graduate which are the internalization of attitudes, mastery of knowledge and skills according to the level of their study program obtained through the learning process.
2. **The PLO imposed on courses** are several learning outcomes of study program graduates (CPL-Study Program) which are used for the formation/development of a course consisting of aspects of attitude, general skills, special skills and knowledge.

3. **Program Objectives (PO)** are abilities that are specifically described from the PLO assigned to a course, and are specific to the study material or learning materials for that course.
4. **Subject Sub-PO (Sub-PO)** is a capability that is specifically described from the PO that can be measured or observed and is the final ability that is planned at each learning stage, and is specific to the learning material of the course.
5. **Indicators for assessing** ability in the process and student learning outcomes are specific and measurable statements that identify the ability or performance of student learning outcomes accompanied by evidence.
6. **Assessment Criteria** are benchmarks used as a measure or measure of learning achievement in assessments based on predetermined indicators. Assessment criteria are guidelines for assessors so that assessments are consistent and unbiased. Criteria can be quantitative or qualitative.
7. **Forms of assessment:** test and non-test.
8. **Forms of learning:** Lecture, Response, Tutorial, Seminar or equivalent, Practicum, Studio Practice, Workshop Practice, Field Practice, Research, Community Service and/or other equivalent forms of learning.
9. **Learning Methods:** Small Group Discussion, Role-Play & Simulation, Discovery Learning, Self-Directed Learning, Cooperative Learning, Collaborative Learning, Contextual Learning, Project Based Learning, and other equivalent methods.
10. **Learning materials** are details or descriptions of study materials which can be presented in the form of several main points and sub-topics.
11. **The assessment weight** is the percentage of assessment of each sub-PO achievement whose size is proportional to the level of difficulty of achieving that sub-PO, and the total is 100%.
12. TM=Face to face, PT=Structured assignments, BM=Independent study.