	Universitas Negeri Surabaya **Faculty of Economics and Business** **Digital Business Undergraduate Study Program**	**Document Code**

SEMESTER LEARNING PLAN

Courses	**CODE**	**Course Family**	**Credit Weight**			**SEMESTER**	**Compilation Date**
Data Security Management	6120903026	Study Program Elective Courses	**T=0**	**P=0**	**ECTS=0**	4	July 17, 2024

AUTHORIZATION	**SP Developer**	**Course Cluster Coordinator**	**Study Program Coordinator**
	Renny Sari Dewi S.Kom., M.Kom	Ika Diyah Candra Arifah S.E., M.Com, CMA	Hujjatullah Fazlurrahman, S.E., MBA.

Learning model	**Case Studies**

Program Learning Outcomes (PLO)

PLO study program which is charged to the course

PLO-3	Develop logical, critical, systematic and creative thinking in carrying out specific work in their field of expertise and in accordance with work competency standards in the field concerned
PLO-5	Able to master the theory of digital business thoroughly
PLO-6	Able to adapt to the context of digital business problems faced well
PLO-7	Able to develop digital business ideas creatively and innovatively
PLO-8	Able to develop knowledge in the field of digital business appropriately
PLO-9	Able to develop digital business based on entrepreneurial leadership in a sustainable manner
PLO-10	Able to implement digital business theory in managing organizations ethically and effectively
PLO-11	Able to apply information and communication technology in business management appropriately

Program Objectives (PO)

PO - 1	Students are able to explain concepts, policies and the relationship between data security and IT use [C2, P2]
PO - 2	Students are able to provide case studies and explanations about international frameworks or standards related to consumer data protection [C3, A2]
PO - 3	Students are able to practice data attack techniques through information technology media [C3, P3, A2]
PO - 4	Students are able to respond wisely after data attacks ethically [C3, P2, A3]

PLO-PO Matrix

P.O	PLO-3	PLO-5	PLO-6	PLO-7	PLO-8	PLO-9	PLO-10	PLO-11
PO-1	✔	✔						
PO-2	✔	✔	✔					
PO-3				✔	✔			
PO-4						✔	✔	✔

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									✔	✔	✔	✔				
PO-4													✔	✔	✔	✔

Short Course Description	As science and technology develop increasingly rapidly, students' affection and psychomotor skills need to be given insight into global issues, frameworks, and national/international standards aimed at data security. This course is designed so that students are able to learn the legal basis for using information technology wisely and ethically. However, in this lecture there is also practice of data attack techniques so that you can comprehensively understand data security management. This course is delivered in the form of discussion, case-based learning, and role playing. After taking the data security management course, students are expected to explore the role of data hackers so that lessons can be learned to be more careful in sharing data within an organization. (As science and technology develop more rapidly, affective and psychomotor students need to be given insight regarding global issues, frameworks, and national/international standards to secure data. This course is designed so that students can learn the legal basis for the wise and ethical use of information technology. However, in this lecture, there is also the practice of data attack techniques to understand data security management comprehensively course, students are expected to explore the role of data hackers so that the lessons learned can be used to be more careful in sharing data within the organization.)
References	**Main :** 1. Chopra, A, and Chaudhary, M. Implementing an Information Security Management System, Security Management Based on ISO 27001 Guidelines. 2020 2. ISO/IEC 27001:2013 Information Security Management 3. Framework COBIT 2019 **Supporters:** 1. Modul Praktikum Data Security Management
Supporting lecturer	Ika Diyah Candra Arifah, S.E., M.Com. Renny Sari Dewi, S. Kom., M. Kom., MCE., MOS.

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	Students are able to understand the concept of data/information security management	1.1.1. Students are able to explain the concept of data/information security management 2.1.2. Students understand the relationship between data security management and risk management 3.1.3. Students are able to differentiate between data security and data protection	**Criteria:** Holistic rubric **Form of Assessment** : Participatory Activities	Discovery learning, discussion 3 X 50	Discovery learning, discussion 3 X 50	**Material:** Risk Management Concepts **References:** *Chopra, A, and Chaudhary, M. Implementing an Information Security Management System, Security Management Based on ISO 27001 Guidelines. 2020*	4%
2	Students are able to explain policies/regulations related to consumer data protection	1.2.1. Students are able to explain the law and ethics in data security management 2.2.2. Students get to know Law 27 of 2022 concerning personal data protection (UU PDP)	**Criteria:** 5 **Form of Assessment** : Participatory Activities	Discovery learning, discussion 3 X 50	Discovery learning, discussion 3 X 50	**Material:** Law and ethics of data securities management. **Reference:** *Chopra, A, and Chaudhary, M. Implementing an Information Security Management System, Security Management Based on ISO 27001 Guidelines. 2020*	5%

3	Students are able to explain the ethical use of information technology along with case studies related to consumer data leaks	1.3.1. Students are able to summarize literature studies related to consumer data security management 2.3.2. Students are able to explain cases of data leakage 3.3.3. Students are able to provide solutions to data security problems	**Criteria:** 5 **Form of Assessment** : Practice / Performance	Discovery & Cooperative learning, case-based learning 3 X 50	Discovery & Cooperative learning, case-based learning 3 X 50	**Material:** Data/Information Security Management Concepts **Library:** *ISO/IEC 27001:2013 Information Security Management*	5%
4	Students are able to explain national/international frameworks or standards related to consumer data protection	4.1. Students are able to explain the ISO/IEC 27001 framework	**Criteria:** Holistic rubric **Form of Assessment** : Practice / Performance	Discovery & Cooperative learning, case-based learning 3 X 50	Discovery & Cooperative learning, case-based learning 3 X 50	**Material:** securities management framework **Reference:** *ISO/IEC 27001:2013 Information Security Management*	5%
5	Students can explain national/international frameworks or standards related to consumer data protection Students can explain national/international frameworks or standards related to consumer data protection	5.1 Students are able to analyze the implementation of ISO/IEC 27001	**Criteria:** Holistic rubric **Form of Assessment** : Practice / Performance	Discovery & Cooperative learning, case-based learning 3 X 50	Discovery & Cooperative learning, case-based learning	**Material:** ISO/IEC 27001 **Reference:** *ISO/IEC 27001:2013 Information Security Management*	5%
6	Students are able to explain national/international frameworks or standards related to consumer data protection	6.1 Students are able to explain the Control Objective for Information Technology (COBIT) framework	**Criteria:** Holistic rubric **Form of Assessment** : Participatory Activities, Portfolio Assessment	Discovery & Cooperative learning, case-based learning 3 X 50	Discovery & Cooperative learning, case-based learning	**Material:** COBIT 2019 **Library:** *COBIT 2019 Framework*	5%
7	Students can explain national/international frameworks or standards related to consumer data protection Students can explain national/international frameworks or standards related to consumer data protection	7.1 Students are able to analyze the application of the Control Objective for Information Technology (COBIT) framework	**Criteria:** Holistic rubric **Form of Assessment** : Participatory Activities, Practice/Performance	Discovery & Cooperative learning, case-based learning 3 X 50	Discovery & Cooperative learning, case-based learning 3 X 50	**Material:** COBIT 2019 **Library:** *COBIT 2019 Framework*	5%

8	Midterm exam	Students are able to answer correctly and thoroughly from the compilation of lecture material 1-7	**Criteria:** Holistic rubric **Form of Assessment** : Assessment of Project Results / Product Assessment, Practices / Performance	Written test 3 X 50	Written test 3 x 50	**Material:** Securities Management Concepts **References:** *Chopra, A, and Chaudhary, M. Implementing an Information Security Management System, Security Management Based on ISO 27001 Guidelines. 2020* **Material:** Discussion of case 1 **Reference:** *ISO/IEC 27001:2013 Information Security Management* **Material:** Discussion of case 2 **Reference:** *COBIT 2019 Framework*	15%
9	Students are able to practice techniques for attacking consumer data through software	1. 9.1 Students are able to understand the forms of attacks on software 2. 9.2 Students are able to map the advantages and disadvantages of software/social media attack tools	**Criteria:** Holistic rubric **Form of Assessment** : Participatory Activities, Practical Assessment	Computer practice, 3 X 50 software simulation	Computer practice, software simulation 3 x 50	**Material:** Introduction and general practicum instructions **Library:** *Data Security Management Practicum Module*	5%
10	Students are able to practice techniques for attacking consumer data through software	10.1 Students are able to practice attack tools using the SQL Injection method	**Criteria:** Holistic rubric **Form of Assessment** : Participatory Activities, Practice/Performance	Computer practice, 3 X 50 software simulation	Computer practice, software simulation 3 x 50	**Material:** SQL injection **Library:** *Data Security Management Practical Module*	5%
11	Students are able to practice techniques for attacking consumer data through software	11.1 Students are able to practice attack tools using Phishing or Sniffing methods	**Criteria:** Holistic rubric **Forms of Assessment** : Participatory Activities, Practical Assessment, Practical / Performance	Computer practice, 3 X 50 software simulation	Computer practice, software simulation 3 x 50	**Material:** Phishing **Library:** *Data Security Management Practical Module*	5%
12	Students are able to practice techniques for attacking consumer data through software	12.1 Students are able to practice attack tools using the Spoofing method	**Criteria:** Holistic rubric **Forms of Assessment** : Participatory Activities, Practical Assessment, Practical / Performance	Computer practice, 3 X 50 software simulation	Computer practice, software simulation 3 x 50	**Material:** Spoofing **Literature:** *Data Security Management Practical Module*	5%
13	Students are able to name software weaknesses that cause data leaks	13.1 Students are able to recognize forms of access rights (permissions) in terms of file sharing.	**Form of Assessment** : Participatory Activities, Practice/Performance	3 X 50			0%
14	Students are able to name software weaknesses that cause data leaks	14.1 Students are able to assess software weaknesses that are vulnerable to hacking/attacks	**Criteria:** Holistic rubric **Form of Assessment** : Participatory Activities	Lectures, discussions 3 X 50	Lectures, discussions 3 x 50	**Material:** File Sharing **Library:** *Data Security Management Practical Module*	5%

15	Students are able to respond to the use of information technology wisely, ethically and efficiently to prevent data leaks	1. 15.1 Students are able to make scientific studies regarding data leak prevention techniques wisely and ethically 2. 15.2 Students are able to show wise and ethical attitudes in social engineering practices which are detrimental to society	**Form of Assessment** : Practice/Performance, Test	Lectures, discussions 3 X 50	Lectures, discussions 3 x 50	**Material:** Data leak prevention methods **Reference:** *Data Security Management Practical Module*	5%
16	Students are able to respond to the use of information technology wisely, ethically and efficiently to prevent data leaks	16.1 Students are able to show wise and ethical attitudes in social engineering practices which are detrimental to society	**Form of Assessment** : Participatory Activities, Practice/Performance	Written test 3 X 50	Written test 3 x 50	**Material:** Social engineering **Library:** *Data Security Management Practical Module*	20%

Evaluation Percentage Recap: Case Study

No	Evaluation	Percentage
1.	Participatory Activities	37.34%
2.	Project Results Assessment / Product Assessment	7.5%
3.	Portfolio Assessment	2.5%
4.	Practical Assessment	5.84%
5.	Practice / Performance	43.34%
6.	Test	2.5%
		99.02%

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** abilities in the process and student learning outcomes are specific and measurable statements that identify the abilities 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.