	Universitas Negeri Surabaya Fakultas Teknik Program Studi S1 Sistem Informasi	Kode Dokumen

RENCANA PEMBELAJARAN SEMESTER

MATA KULIAH (MK)	KODE	Rumpun MK	BOBOT (sks)			SEMESTER	Tgl Penyusunan
Keamanan Sistem Informasi	5720103151		T=3	P=0	ECTS=4.77	4	8 Desember 2025

OTORISASI	Pengembang RPS	Koordinator RMK	Koordinator Program Studi
	Rahadian Bisma, S.Kom., M.Kom.	.....	I KADEK DWI NURYANA

Model Pembelajaran	**Case Study**	
Capaian Pembelajaran (CP)	**CPL-PRODI yang dibebankan pada MK**	
	CPL-13	Mampu memahami dan menjelaskan konsep dan pentingnya keamanan sistem informasi dalam mengelola data dan informasi serta mengidentifikasi hal - hal tentang kebocoran data
	CPL-15	Mampu memahami, menganalisis, menilai, dan mengevaluasi sistem informasi dalam mengelola data dan informasi bisnis serta merekomendasikan pengambilan keputusan dengan memperhatikan hukum kode etik dalam penggunaan informasi
	Capaian Pembelajaran Mata Kuliah (CPMK)	
	CPMK - 1	Mahasiswa diharapkan paham aspek praktis menjadi manajer keamanan informasi yang efektif
	CPMK - 2	Mahasiswa tau dan mampu memahami memanfaatkan fungsi keamanan yang kompleks, seperti forensik digital, respon insiden, dan arsitektur keamanan
	CPMK - 3	Mahasiswa mengetahui konsep dan cara menyeimbangkan antara biaya dan risiko yang tepat
	Matrik CPL - CPMK	

CPMK	CPL-13	CPL-15
CPMK-1	✔	✔
CPMK-2		✔
CPMK-3	✔	

Matrik CPMK pada Kemampuan akhir tiap tahapan belajar (Sub-CPMK)

CPMK	Minggu Ke															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
CPMK-1	✔	✔			✔		✔		✔		✔	✔		✔	✔	
CPMK-2			✔					✔					✔			
CPMK-3				✔		✔				✔						✔

Deskripsi Singkat MK	Mata kuliah ini membahas konsep, prinsip, dan praktik keamanan sistem informasi dengan pendekatan tata kelola (governance) untuk memastikan perlindungan aset informasi dalam suatu organisasi. Mahasiswa akan mempelajari kerangka kerja tata kelola keamanan informasi seperti ISO 27001, NIST, COBIT, dan ITIL, serta bagaimana mengintegrasikan kebijakan, prosedur, dan kontrol keamanan dalam strategi bisnis.	
Pustaka	**Utama :**	
	1. Rashid A., Chivers, Andrew Martin, The Cyber Security Body of Knowledge, 1.1.0, 2021	
	Pendukung :	
Dosen Pengampu	Rahadian Bisma, S.Kom., M.Kom. Cendra Devayana Putra, S.Kom., M.IM.	

Mg Ke-	Kemampuan akhir tiap tahapan belajar (Sub-CPMK)	Penilaian		Bantuk Pembelajaran, Metode Pembelajaran, Penugasan Mahasiswa, [Estimasi Waktu]		Materi Pembelajaran [Pustaka]	Bobot Penilaian (%)
		Indikator	Kriteria & Bentuk	Luring (*offline*)	Daring (*online*)		
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)

1	Evolusi profesi	1. sejarah profesi keamanan informasi 2. Risiko dan Konsekuensi	**Kriteria:** 1. Skor max 10. 2. Jika 4 aspek: 8 3. Jika 3 aspek: 6 4. Jika 2 aspek: 4 5. Jika 1 aspek: 2 **Bentuk Penilaian** : Praktik / Unjuk Kerja	Pendekatan: Saintifik Model: Kooperatif Metode: Diskusi, Presentasi 2 X 50	Pendekatan: Saintifik Model: Kooperatif Metode: Diskusi, Presentasi 2 X 50	**Materi:** Evolusi profesi **Pustaka:** *Rashid A., Chivers, Andrew Martin, The Cyber Security Body of Knowledge, 1.1.0, 2021*	4%
2	Ancaman dan Kerentanan Keamanan Sistem informasi	1. Ancaman 2. Kerentanan 3. Kecanggihan dan kemampuan penjahat dunia maya sekarang lebih besar daripada sebelumnya, dengan pelaku ancaman teknis yang unggul yang meneliti dan mengembangkan kerangka kerja malware berbahaya yang memungkinkan mereka atau Pelanggan mereka untuk masuk ke sistem korban mereka, menjaga akses, menutupi jejak mereka, menghindari tindakan balasan dan menyedot gigabyte informasi rahasia untuk dijual di pasar gelap. Bab ini membahas berbagai ancaman dan kerentanan yang mempengaruhi kita setiap hari, termasuk yang buatan manusia dan ancaman alami yang sering diabaikan saat mempertimbangkan keamanan informasi.	**Kriteria:** 1. Skor max 10. 2. Jika 4 aspek: 8 3. Jika 3 aspek: 6 4. Jika 2 aspek: 4 5. Jika 1 aspek: 2 **Bentuk Penilaian** : Aktifitas Partisipasif	Pendekatan: Saintifik Model: Kooperatif Metode: Diskusi, Presentasi 2 X 50	Pendekatan: Saintifik Model: Kooperatif Metode: Diskusi, Presentasi 2 X 50	**Materi:** Ancaman dan Kerentanan Keamanan Sistem informasi **Pustaka:** *Rashid A., Chivers, Andrew Martin, The Cyber Security Body of Knowledge, 1.1.0, 2021*	7%

3	Manajer Keamanan	1. Role dari manajer kemanan informasi 2. pengembangan karier 3. cara menjadi manajer keamanan informasi 4. Menyelami peran manajer keamanan informasi dan melihat apa yang harus mereka lakukan Dari hari ke hari. Kami juga berfokus pada bagaimana manajer keamanan informasi dapat mengelola keterampilan dan kompetensi tim mereka dengan menggunakan kerangka kerja keterampilan yang diakui dan bagaimana profesionalisme dalam sektor keamanan dapat digunakan untuk mengangkat semua peran kami sebagai petugas keamanan dari lingkup TI tradisional menjadi sebuah profesi. Semua miliknya sendiri. Kami juga akan melihat beberapa mitos umum dan kesalahpahaman yang terkait dengan kursus pelatihan profesional dan kursus akademis dan kaitannya dengan rencana pengembangan karir Anda, menutup bab ini dengan melihat sekilas apa itu sistem manajemen keamanan informasi.	**Kriteria:** 1. Skor max 10. 2. Jika 4 aspek: 8 3. Jika 3 aspek: 6 4. Jika 2 aspek: 4 5. Jika 1 aspek: 2 **Bentuk Penilaian** : Aktifitas Partisipasif	Pendekatan: Saintifik Model: KooperatifMetode: Diskusi, Presentasi 2 X 50	Pendekatan: Saintifik Model: KooperatifMetode: Diskusi, Presentasi 2 X 50	**Materi:** Manajer Keamanan **Pustaka:** *Rashid A., Chivers, Andrew Martin, The Cyber Security Body of Knowledge, 1.1.0, 2021*	4%

4	Keamanan Informasi sebagai Fungsi Bisnis	1. Keamanan dalam Struktur Organisasi 2. Bekerja dengan Kelompok Spesialis 3. Bekerja dengan Standar dan Peraturan 4. Bekerja dengan Manajemen Risiko 5. Bekerja dengan Arsitektur Enterprise 6. Bekerja dengan Manajemen Fasilitas 7. melihat bagaimana manajer keamanan informasi dapat menanamkan keamanan sebagai fungsi dalam bisnis, memastikan bahwa kita menyelaraskan semua orang, proses, dan teknologi ke hasil keamanan yang mendukung bisnis dan kebutuhan strategisnya. Kita akan melihat struktur organisasi tradisional yang kita lihat setiap hari dalam bisnis, melihat bagaimana memberi lapisan keamanan ke dalam struktur ini untuk memastikan bahwa kita mencakup semua aspek risiko, tidak hanya yang terkait dengan cyber. Bab ini membahas manajemen risiko, manajemen kontinuitas bisnis dan arsitektur enterprise yang lebih dalam, yang menjelaskan peran keamanan dalam masing-masing fungsi bisnis ini. Bab ini ditutup dengan penjelasan singkat tentang bagaimana keamanan dapat diintegrasikan dengan manajemen fasilitas	**Kriteria:** 1. Skor max 10. 2. Jika 4 aspek: 8 3. Jika 3 aspek: 6 4. Jika 2 aspek: 4 5. Jika 1 aspek: 2 **Bentuk Penilaian** : Praktik / Unjuk Kerja	Pendekatan:Saintifik Model: KooperatifMetode:Diskusi, Presentasi 2 X 50	Pendekatan:Saintifik Model: KooperatifMetode:Diskusi, Presentasi 2 X 50	**Materi:** Keamanan Informasi sebagai Fungsi Bisnis **Pustaka:** *Rashid A., Chivers, Andrew Martin, The Cyber Security Body of Knowledge, 1.1.0, 2021*	2%

5	Implementasi Keamanan Informasi	1. Integrasi dengan Manajemen Risiko 2. Bahasa Resiko 3. Gunakan Kerangka yang Ada 4. Pengembangan Aman 5. Kesadaran Arsitektur Keamanan 6. Persyaratan Keamanan 7. Antarmuka Organisasi 8. Implementasi keamanan informasi masuk ke rincian lebih lanjut tentang bagaimana manajer keamanan informasiDapat mengintegrasikan fungsi tim keamanan dengan fungsi yang disediakan oleh organisasi lainnya, seperti manajemen risiko, arsitektur dan pengembangan perangkat lunak. Yang terpenting, bab ini terlihatPada konsep persyaratan keamanan yang bertentangan dengan kontrol keamanan, menunjukkan kepada Anda bagaimana untuk mendapatkan persyaratan keamanan di tahap inisiasi proyek untuk memastikan bahwa ancaman, kerentanan, dan risiko ditangani oleh desain dan bukan sebagai renungan.	**Kriteria:** 1. Skor max 10. 2. Jika 4 aspek: 8 3. Jika 3 aspek: 6 4. Jika 2 aspek: 4 5. Jika 1 aspek: 2 **Bentuk Penilaian** : Aktifitas Partisipasif	Pendekatan:Saintifik Model: KooperatifMetode:Diskusi, Presentasi 2 X 50	Pendekatan:Saintifik Model: KooperatifMetode:Diskusi, Presentasi 2 X 50	**Materi:** Implementasi Keamanan Informasi **Pustaka:** *Rashid A., Chivers, Andrew Martin, The Cyber Security Body of Knowledge, 1.1.0, 2021*	4%
6	Implementasi Keamanan Informasi	1. Integrasi dengan Manajemen Risiko o Bahasa Resiko o Gunakan Kerangka yang Ada 2. Pengembangan Aman Kesadaran Arsitektur Keamanan Persyaratan Keamanan 3. Antarmuka Organisasi	**Kriteria:** 1. Skor max 10. 2. Jika 4 aspek: 8 3. Jika 3 aspek: 6 4. Jika 2 aspek: 4 5. Jika 1 aspek: 2 **Bentuk Penilaian** : Aktifitas Partisipasif	Pendekatan Saintifik, Model, Kooperatif, Metode, Diskusi, Presentasi 2x50	Pendekatan Saintifik, Model, Kooperatif, Metode, Diskusi, Presentasi 2x50	**Materi:** Implementasi Keamanan Informasi **Pustaka:** *Rashid A., Chivers, Andrew Martin, The Cyber Security Body of Knowledge, 1.1.0, 2021*	4%

7	Kerangka Standar Pedoman dan Perundang-undangan	1. Mengapa Kita Membutuhkan Standar? 2. Perundang-undangan 3. Standar Standar ISO / IEC 27000 4. Keberlangsungan bisnis 5. Standar Manajemen Risiko 6. COBIT 7. Sebagai dasar dari segala hal yang kita lakukan dalam keamanan, terutama saat beroperasi dalam peran manajer keamanan informasi, kita perlu membenarkan apa yang kita memaksakan bisnis dari sudut pandang pengurangan risiko. Di dunia di mana ancaman dan kerentanan mempengaruhi apa yang kita lakukan setiap hari, sekarang ada banyak standar, kerangka kerja, pedoman dan undang-undang nasional yang mendorong apa yang harus kita lakukan untuk memenuhi persyaratan industri atau hukum tertentu. Bab 6 membahas berbagai standar dan pedoman internasional yang mempengaruhi organisasi kita, menilai nilai mereka kepada Anda sebagai manajer keamanan informasi dan juga nilai mereka untuk industri secara umum.	**Kriteria:** 1. Skor max 10. 2. Jika 4 aspek: 8 3. Jika 3 aspek: 6 4. Jika 2 aspek: 4 5. Jika 1 aspek: 2 **Bentuk Penilaian** : Aktifitas Partisipasif	Pendekatan:Saintifik Model: KooperatifMetode:Diskusi, Presentasi 6 X 50	Pendekatan:Saintifik Model: KooperatifMetode:Diskusi, Presentasi 6 X 50	**Materi:** Kerangka Standar Pedoman dan Perundang-undangan **Pustaka:** *Rashid A., Chivers, Andrew Martin, The Cyber Security Body of Knowledge, 1.1.0, 2021*	4%
8	Ujian Tengah Semester	UTS	**Kriteria:** UTS **Bentuk Penilaian** : Penilaian Hasil Project / Penilaian Produk, Tes	UTS 2 X 50	UTS 2 X 50	**Materi:** Ujian Tengah Semester **Pustaka:** *Rashid A., Chivers, Andrew Martin, The Cyber Security Body of Knowledge, 1.1.0, 2021*	20%
9	Kerangka Standar Pedoman dan Perundangundangan	1. Mengapa Kita Membutuhkan Standar? 2. Perundang undangan 3. Standar Standar ISO / IEC 27000 4. Keberlangsungan bisnis 5. Standar Manajemen Risiko 6. COBIT	**Kriteria:** 1. Skor max 10. 2. Jika 4 aspek: 8 3. Jika 3 aspek: 6 4. Jika 2 aspek: 4 5. Jika 1 aspek: 2 **Bentuk Penilaian** : Aktifitas Partisipasif	Pendekatan Saintifik, Model, Kooperatif, Metode, Diskusi, Presentasi 2x50	Pendekatan Saintifik, Model, Kooperatif, Metode, Diskusi, Presentasi 2x50	**Materi:** Kerangka Standar Pedoman dan Perundangundangan **Pustaka:** *Rashid A., Chivers, Andrew Martin, The Cyber Security Body of Knowledge, 1.1.0, 2021*	4%
10	Kerangka Standar Pedoman dan Perundangundangan	1. Mengapa Kita Membutuhkan Standar? 2. Perundangundangan 3. Standar Standar ISO / IEC 27000 4. Keberlangsungan bisnis 5. Standar Manajemen Risiko 6. COBIT	**Kriteria:** 1. Skor max 10. 2. Jika 4 aspek: 8 3. Jika 3 aspek: 6 4. Jika 2 aspek: 4 5. Jika 1 aspek: 2 **Bentuk Penilaian** : Tes	Pendekatan Saintifik, Model, Kooperatif, Metode, Diskusi, Presentasi 2x50	Pendekatan Saintifik, Model, Kooperatif, Metode, Diskusi, Presentasi 2x50	**Materi:** Kerangka Standar Pedoman dan Perundangundangan **Pustaka:** *Rashid A., Chivers, Andrew Martin, The Cyber Security Body of Knowledge, 1.1.0, 2021*	4%

11	Perlindungan Informasi	1. Klasifikasi Informasi 2. Tingkat Dampak Bisnis 3. Melaksanakan Klasifikasi Informasi 4. Implementasi Strategis 5. Identifikasi, Otentikasi, dan Otorisasi 6. Model Kontrol Akses 7. Sistem Wewenang 8. Delegasi Hak Istimewa 9. Informasi adalah sumber kehidupan bisnis modern, tidak peduli apakah mereka melakukan perdagangan asuransi perjalanan, rahasia pemerintah, bangunan, dan konstruksi atau informasi pendidikan lanjutan berada di jantung usaha membuat bisnis ini berjalan. Bab 7 melihat bagaimana kita dapat membangun sistem untuk membantu melindungi informasi penting yang sangat penting dalam organisasi kita, dengan mempertimbangkan kepekaan data dan sistem kontrol akses yang dapat kita gunakan untuk memastikan bahwa hanya mereka yang perlu mengakses mendapatkannya.	**Kriteria:** 1. Skor max 10. 2. Jika 4 aspek: 8 3. Jika 3 aspek: 6 4. Jika 2 aspek: 4 5. Jika 1 aspek: 2 **Bentuk Penilaian** : Aktifitas Partisipasif	Pendekatan:Saintifik Model: KooperatifMetode:Diskusi, Presentasi 2 X 50	Pendekatan:Saintifik Model: KooperatifMetode:Diskusi, Presentasi	**Materi:** Perlindungan Informasi **Pustaka:** *Rashid A., Chivers, Andrew Martin, The Cyber Security Body of Knowledge, 1.1.0, 2021*	7%
12	Perlindungan Orang	1. Kerentanan Manusia 2. Teknik Sosial 3. Membangun Budaya Keamanan 4. Staf lalai 5. Aturan Berselancar dan Menguping 6. Perilaku Kode 7. Employment Contracts 8. Siklus Hidup Keamanan Personalia 9. Pengerahan 10. Pilihan 11. Kinerja dan Suksesi 12. Transisi	**Kriteria:** 1. Skor max 10. 2. Jika 4 aspek: 8 3. Jika 3 aspek: 6 4. Jika 2 aspek: 4 5. Jika 1 aspek: 2 **Bentuk Penilaian** : Aktifitas Partisipasif	Pendekatan:Saintifik Model: KooperatifMetode:Diskusi, Presentasi 2 X 50	Pendekatan:Saintifik Model: KooperatifMetode:Diskusi, Presentasi 2 X 50	**Materi:** Perlindungan Orang **Pustaka:** *Rashid A., Chivers, Andrew Martin, The Cyber Security Body of Knowledge, 1.1.0, 2021*	4%

13	Perlindungan Orang (2)	1. Apa itu Keamanan Fisik? 2. Keamanan Fisik di ISO / IEC 27001: 2013 3. Mulailah dengan Risk Assessment 4. Lengkapi Risk Assessment 5. Perimeter Desain 6. Hambatan, Dinding, dan Pagar 7. Mailrooms dan Loading Bays 8. Penjaga keamanan 9. CCTV 10. Penerangan 11. Kantor, lokasi lapangan, dan pusat data semuanya bisa menjadi titik lemah dalam operasi dimana serangan dapat terjadi. Di pertemuan ini kita melihat tindakan pengamanan fisik yang dapat kita ambil untuk membela dan mempertahankan fasilitas kita, termasuk pertimbangan utama yang harus dimiliki manajer keamanan informasi saat bekerja bersama para ahli di tim manajemen fasilitas, eksekutif bisnis dan penegakan hukum untuk membantu melindungi fisik kita. Lingkungan.	**Kriteria:** 1. Skor max 10. 2. Jika 4 aspek: 8 3. Jika 3 aspek: 6 4. Jika 2 aspek: 4 5. Jika 1 aspek: 2 **Bentuk Penilaian** : Praktik / Unjuk Kerja	Pendekatan:Saintifik Model: KooperatifMetode:Diskusi, Presentasi 4 X 50	Pendekatan:Saintifik Model: KooperatifMetode:Diskusi, Presentasi 4 X 50	**Materi:** Perlindungan Orang **Pustaka:** *Rashid A., Chivers, Andrew Martin, The Cyber Security Body of Knowledge, 1.1.0, 2021*	4%
14	1. Protection of Premises 2. Protection of Systems	1. Apa itu Keamanan Fisik? Keamana n Fisik di ISO / IEC 27001: 2013 2. Mulailah dengan Risk Assessment, Ancaman dan Kerentanan ,Lengkapi Risk Assessmen ,Perimeter Desain, Hambatan, Dinding dan Pagar ,Mailroom s dan	**Kriteria:** 1. Skor max 10. 2. Jika 4 aspek: 8 3. Jika 3 aspek: 6 4. Jika 2 aspek: 4 5. Jika 1 aspek: 2 **Bentuk Penilaian** : Aktifitas Partisipasif	Pendekatan Saintifik, Model, Kooperatif, Metode, Diskusi, Presentasi 2x50	Pendekatan Saintifik, Model, Kooperatif, Metode, Diskusi, Presentasi 2x50	**Materi:** Protection of Premises **Pustaka:** *Rashid A., Chivers, Andrew Martin, The Cyber Security Body of Knowledge, 1.1.0, 2021*	4%

15	Protection of Systems	1. Memperkenalkan Malware 2. Apa itu Malware? 3. Klasifikasi Perangkat Lunak Perusak 4. Serangan Konten Aktif 5. Vektor ancaman 6. Penanggulangan Teknis 7. Keamanan jaringan 8. Apakah Firewall itu? 9. Zona Demiliterisasi (DMZ) 10. Enkripsi Jaringan 11. Jaringan nirkabel 12. kontrol teknis yang perlu diketahui oleh manajer keamanan informasi di dalam arsitektur enterprise, memastikan dasar pengetahuan keamanan yang masuk akal dapat ditambahkan ke gudang keamanan. Ini akan membantu manajer keamanan informasi saat mereka melakukan percakapan dengan tim teknis, seperti insinyur jaringan, pakar sistem operasi Windows dan administrator basis data, memastikan manajer keamanan informasi dapat berbicara bahasa mereka sambil menerjemahkan risiko teknis ke dalam kontrol keamanan yang berarti.	**Kriteria:** 1. Skor max 10. 2. Jika 4 aspek: 8 3. Jika 3 aspek: 6 4. Jika 2 aspek: 4 5. Jika 1 aspek: 2 **Bentuk Penilaian** : Tes	Pendekatan:Saintifik Model: KooperatifMetode:Diskusi, Presentasi 2 X 50		**Materi:** Protection of Systems **Pustaka:** *Rashid A., Chivers, Andrew Martin, The Cyber Security Body of Knowledge, 1.1.0, 2021*	2%
16	Ujian Akhir Semester	UAS	**Kriteria:** UAS **Bentuk Penilaian** : Praktik / Unjuk Kerja	UAS	UAS	**Materi:** Ujian Akhir Semester **Pustaka:** *Rashid A., Chivers, Andrew Martin, The Cyber Security Body of Knowledge, 1.1.0, 2021*	22%

Rekap Persentase Evaluasi : Case Study

No	Evaluasi	Persentase
1.	Aktifitas Partisipasif	42%
2.	Penilaian Hasil Project / Penilaian Produk	10%
3.	Praktik / Unjuk Kerja	32%
4.	Tes	16%
		100%

Catatan

1. **Capaian Pembelajaran Lulusan Prodi (CPL - Prodi)** adalah kemampuan yang dimiliki oleh setiap lulusan prodi yang merupakan internalisasi dari sikap, penguasaan pengetahuan dan ketrampilan sesuai dengan jenjang prodinya yang diperoleh melalui proses pembelajaran.
2. **CPL yang dibebankan pada mata kuliah** adalah beberapa capaian pembelajaran lulusan program studi (CPL-Prodi) yang digunakan untuk pembentukan/pengembangan sebuah mata kuliah yang terdiri dari aspek sikap, ketrampulan umum, ketrampilan khusus dan pengetahuan.
3. **CP Mata kuliah (CPMK)** adalah kemampuan yang dijabarkan secara spesifik dari CPL yang dibebankan pada mata kuliah, dan bersifat spesifik terhadap bahan kajian atau materi pembelajaran mata kuliah tersebut.
4. **Sub-CPMK Mata kuliah (Sub-CPMK)** adalah kemampuan yang dijabarkan secara spesifik dari CPMK yang dapat diukur atau diamati dan merupakan kemampuan akhir yang direncanakan pada tiap tahap pembelajaran, dan bersifat spesifik terhadap materi pembelajaran mata kuliah tersebut.
5. **Indikator penilaian** kemampuan dalam proses maupun hasil belajar mahasiswa adalah pernyataan spesifik dan terukur yang mengidentifikasi kemampuan atau kinerja hasil belajar mahasiswa yang disertai bukti-bukti.
6. **Kreteria Penilaian** adalah patokan yang digunakan sebagai ukuran atau tolok ukur ketercapaian pembelajaran dalam penilaian berdasarkan indikator-indikator yang telah ditetapkan. Kreteria penilaian merupakan pedoman bagi penilai agar penilaian konsisten dan tidak bias. Kreteria dapat berupa kuantitatif ataupun kualitatif.
7. **Bentuk penilaian:** tes dan non-tes.
8. **Bentuk pembelajaran:** Kuliah, Responsi, Tutorial, Seminar atau yang setara, Praktikum, Praktik Studio, Praktik Bengkel, Praktik Lapangan, Penelitian, Pengabdian Kepada Masyarakat dan/atau bentuk pembelajaran lain yang setara.
9. **Metode Pembelajaran:** Small Group Discussion, Role-Play & Simulation, Discovery Learning, Self-Directed Learning, Cooperative Learning, Collaborative Learning, Contextual Learning, Project Based Learning, dan metode lainnya yg setara.
10. **Materi Pembelajaran** adalah rincian atau uraian dari bahan kajian yg dapat disajikan dalam bentuk beberapa pokok dan sub-pokok bahasan.
11. **Bobot penilaian** adalah prosentasi penilaian terhadap setiap pencapaian sub-CPMK yang besarnya proposional dengan tingkat kesulitan pencapaian sub-CPMK tsb., dan totalnya 100%.
12. TM=Tatap Muka, PT=Penugasan terstruktur, BM=Belajar mandiri.

RPS ini telah divalidasi pada tanggal 14 April 2025

Koordinator Program Studi S1 Sistem Informasi

I KADEK DWI NURYANA
NIDN 0014048107

UPM Program Studi S1 Sistem Informasi

NIDN 0008029505

File PDF ini digenerate pada tanggal 8 Desember 2025 Jam 20:48 menggunakan aplikasi RPS-OBE SiDia Unesa