	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 Jaringan	5720102141		T=2	P=0	ECTS=3.18	3	16 Desember 2025

OTORISASI	Pengembang RPS	Koordinator RMK	Koordinator Program Studi
	.....	.....	I KADEK DWI NURYANA

Model Pembelajaran	**Case Study**	
Capaian Pembelajaran (CP)	**CPL-PRODI yang dibebankan pada MK**	
	CPL-3	Mengembangkan pemikiran logis, kritis, sistematis, dan kreatif dalam melakukan pekerjaan yang spesifik di bidang keahliannya serta sesuai dengan standar kompetensi kerja bidang yang bersangkutan
	CPL-4	Mengembangkan diri secara berkelanjutan dan berkolaborasi.
	CPL-6	Mampu mengambil keputusan secara tepat baik mandiri maupun kelompok, bertanggung jawab dan sesuai etik dalam konteks penyelesaian masalah berdasarkan hasil analisis informasi dan data serta mengkomunikasikannya secara efektif
	CPL-8	Mampu membuat perencanaan infrastruktur TI, arsitektur jaringan, layanan fisik dan cloud, menganalisa konsep identifikasi, otentikasi, otorisasi akses dalam konteks melindungi orang dan perangkat
	CPL-10	Memiliki kemampuan merencanakan, menerapkan, memelihara dan meningkatkan sistem informasi organisasi untuk mencapai tujuan dan sasaran organisasi yang strategis baik jangka pendek maupun jangka panjang.
	Capaian Pembelajaran Mata Kuliah (CPMK)	
	CPMK - 1	Menerapkan prinsip-prinsip dasar kriptografi dalam mengamankan komunikasi jaringan (C3)
	CPMK - 2	Menganalisis kerentanan sistem jaringan dan mengidentifikasi potensi serangan siber (C4)
	CPMK - 3	Mengevaluasi efektivitas mekanisme keamanan jaringan yang telah diterapkan (C5)
	CPMK - 4	Menciptakan desain arsitektur keamanan jaringan yang komprehensif untuk organisasi (C6)
	CPMK - 5	Menerapkan teknik deteksi intrusi dan respon insiden keamanan (C3)
	CPMK - 6	Menganalisis pola serangan dan melakukan forensik jaringan (C4)
	CPMK - 7	Mengevaluasi kebijakan keamanan informasi dan kesesuaiannya dengan standar industri (C5)
	CPMK - 8	Menciptakan solusi keamanan terintegrasi untuk lingkungan cloud dan hybrid (C6)
	CPMK - 9	Menerapkan teknik pengamanan aplikasi web dan layanan jaringan (C3)
	CPMK - 10	Menganalisis dan mengevaluasi risiko keamanan dalam infrastruktur TI organisasi (C4/C5)
	Matrik CPL - CPMK	

CPMK	CPL-3	CPL-4	CPL-6	CPL-8	CPL-10
CPMK-1	✔			✔	
CPMK-2	✔			✔	
CPMK-3			✔		✔
CPMK-4				✔	✔
CPMK-5	✔		✔		
CPMK-6	✔		✔		
CPMK-7			✔		✔
CPMK-8				✔	✔
CPMK-9	✔			✔	
CPMK-10			✔		✔

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			✔													
CPMK-4				✔	✔											
CPMK-5																
CPMK-6						✔	✔	✔								
CPMK-7									✔	✔						✔
CPMK-8											✔				✔	
CPMK-9												✔		✔		
CPMK-10	✔															

Deskripsi Singkat MK	Mata kuliah Keamanan Jaringan membahas prinsip-prinsip dasar keamanan jaringan komputer, ancaman keamanan, teknik serangan, dan mekanisme pertahanan. Tujuan mata kuliah ini adalah memberikan pemahaman tentang konsep keamanan jaringan, teknik pengamanan infrastruktur jaringan, serta kemampuan dalam menganalisis dan mengimplementasikan solusi keamanan. Ruang lingkup mencakup kriptografi, autentikasi, firewall, intrusion detection systems, keamanan protokol jaringan, wireless security, dan manajemen risiko keamanan informasi.
Pustaka	**Utama :**
	Pendukung :
Dosen Pengampu	Dwi Fatrianto Suyatno, S.Kom., M.Kom. Rahadian Bisma, S.Kom., M.Kom.

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	Mahasiswa dapat mengidentifikasi kebutuhan kriptografi dalam komunikasi jaringan, memilih metode kriptografi yang sesuai, dan menerapkannya dalam skenario keamanan dasar.	1.Mahasiswa mampu menjelaskan konsep enkripsi dan dekripsi dalam kriptografi 2.Mahasiswa dapat menerapkan algoritma kriptografi simetris dan asimetris pada data komunikasi 3.Mahasiswa mampu menganalisis kebutuhan kriptografi dalam berbagai skenario komunikasi jaringan	**Bentuk Penilaian** : Aktifitas Partisipasif, Tes			**Materi:** Konsep dasar kriptografi dan steganografi, Jenis-jenis algoritma kriptografi (simetris dan asimetris), Aplikasi kriptografi dalam keamanan jaringan, Tools dan software untuk implementasi kriptografi **Pustaka:** *Handbook Perkuliahan*	0%
2	Mahasiswa dapat mengimplementasikan teknik kriptografi untuk melindungi data dalam transmisi jaringan.	1.Mampu menjelaskan konsep enkripsi dan dekripsi 2.Dapat mengaplikasikan algoritma kriptografi simetris dan asimetris 3.Mampu mengimplementasikan kriptografi dalam skenario komunikasi jaringan	**Bentuk Penilaian** : Aktifitas Partisipasif, Praktik / Unjuk Kerja	Ceramah interaktif, demonstrasi, diskusi kelompok, dan praktikum langsung.	Implementasi algoritma kriptografi menggunakan tools online, Analisis studi kasus keamanan komunikasi	**Materi:** Konsep dasar kriptografi, Jenis-jenis algoritma kriptografi (simetris dan asimetris), Aplikasi kriptografi dalam keamanan jaringan, Studi kasus implementasi kriptografi **Pustaka:** *Handbook Perkuliahan*	0%
3	Mahasiswa dapat mengidentifikasi, mengklasifikasikan, dan menganalisis kerentanan jaringan serta merumuskan potensi ancaman siber yang mungkin terjadi	1.Kemampuan mengidentifikasi jenis-jenis kerentanan jaringan 2.Kemampuan menganalisis dampak kerentanan terhadap sistem 3.Kemampuan mengklasifikasikan jenis serangan siber berdasarkan kerentanan yang ditemukan 4.Kemampuan merumuskan skenario serangan berdasarkan analisis kerentanan	**Bentuk Penilaian** : Aktifitas Partisipasif, Praktik / Unjuk Kerja, Tes	Studi kasus, diskusi kelompok, simulasi praktikum, dan presentasi analisis.		**Materi:** Konsep dasar kerentanan sistem jaringan, Teknik identifikasi dan klasifikasi kerentanan, Jenis-jenis serangan siber dan karakteristiknya, Analisis dampak kerentanan terhadap keamanan jaringan, Tools untuk analisis kerentanan jaringan **Pustaka:** *Handbook Perkuliahan*	0%

4	Mahasiswa dapat mengidentifikasi, mengklasifikasikan, dan menganalisis kerentanan jaringan serta memprediksi dampak serangan siber yang mungkin terjadi	1.Kemampuan mengidentifikasi jenis-jenis kerentanan jaringan 2.Kemampuan menganalisis skenario serangan berdasarkan kerentanan 3.Kemampuan mengevaluasi tingkat risiko dari kerentanan yang teridentifikasi	**Bentuk Penilaian** : Aktifitas Partisipasif, Penilaian Hasil Project / Penilaian Produk	Studi kasus, diskusi kelompok, demonstrasi tools analisis kerentanan, dan simulasi serangan.	Analisis Case Study, Mahasiswa menganalisis studi kasus serangan siber nyata, mengidentifikasi kerentanan yang dieksploitasi, dan membuat laporan analisis dampak serta rekomendasi mitigasi	**Materi:** Konsep kerentanan jaringan, Teknik identifikasi kerentanan, Klasifikasi serangan siber, Analisis dampak kerentanan, Tools vulnerability assessment **Pustaka:** *Handbook Perkuliahan*	0%
5	Mahasiswa dapat mengidentifikasi, mengklasifikasikan, dan menganalisis kerentanan jaringan serta memprediksi dampak serangan siber yang mungkin terjadi	1.Kemampuan mengidentifikasi jenis-jenis kerentanan jaringan 2.Kemampuan menganalisis skenario serangan berdasarkan kerentanan 3.Kemampuan mengevaluasi tingkat risiko dari kerentanan yang teridentifikasi	**Bentuk Penilaian** : Aktifitas Partisipasif, Penilaian Hasil Project / Penilaian Produk	Studi kasus, diskusi kelompok, demonstrasi tools analisis kerentanan, dan simulasi serangan.	Analisis Case Study, Mahasiswa menganalisis studi kasus serangan siber nyata, mengidentifikasi kerentanan yang dieksploitasi, dan membuat laporan analisis dampak serta rekomendasi mitigasi	**Materi:** Konsep kerentanan jaringan, Teknik identifikasi kerentanan, Klasifikasi serangan siber, Analisis dampak kerentanan, Tools vulnerability assessment **Pustaka:** *Handbook Perkuliahan*	0%
6	Mahasiswa dapat menilai dan memberikan rekomendasi kritis terhadap implementasi mekanisme keamanan jaringan berdasarkan prinsip-prinsip evaluasi dan standar industri.	1.Kemampuan menganalisis efektivitas mekanisme keamanan yang diterapkan 2.Kemampuan mengidentifikasi celah keamanan dan memberikan solusi perbaikan 3.Kemampuan menyusun laporan evaluasi dengan rekomendasi berbasis bukti	**Bentuk Penilaian** : Aktifitas Partisipasif, Penilaian Hasil Project / Penilaian Produk	Studi kasus, diskusi kelompok, presentasi, dan simulasi evaluasi keamanan.		**Materi:** Prinsip evaluasi keamanan jaringan, Teknik analisis efektivitas firewall, IDS/IPS, dan enkripsi, Studi kasus implementasi keamanan jaringan dunia nyata, Metodologi penilaian risiko dan rekomendasi perbaikan **Pustaka:** *Handbook Perkuliahan*	0%
7	Mahasiswa dapat menilai dan memberikan rekomendasi kritis terhadap implementasi mekanisme keamanan jaringan berdasarkan prinsip-prinsip evaluasi dan standar industri.	1.Kemampuan menganalisis efektivitas mekanisme keamanan yang diterapkan 2.Kemampuan mengidentifikasi celah keamanan dan memberikan solusi perbaikan 3.Kemampuan menyusun laporan evaluasi dengan rekomendasi berbasis bukti	**Bentuk Penilaian** : Aktifitas Partisipasif, Penilaian Hasil Project / Penilaian Produk	Studi kasus, diskusi kelompok, presentasi, dan simulasi evaluasi keamanan.		**Materi:** Prinsip evaluasi keamanan jaringan, Teknik analisis efektivitas firewall, IDS/IPS, dan enkripsi, Studi kasus implementasi keamanan jaringan dunia nyata, Metodologi penilaian risiko dan rekomendasi perbaikan **Pustaka:** *Handbook Perkuliahan*	0%
8	Mahasiswa dapat menilai dan memberikan rekomendasi kritis terhadap implementasi mekanisme keamanan jaringan berdasarkan prinsip-prinsip evaluasi dan standar industri.	1.Kemampuan menganalisis efektivitas mekanisme keamanan yang diterapkan 2.Kemampuan mengidentifikasi celah keamanan dan memberikan solusi perbaikan 3.Kemampuan menyusun laporan evaluasi dengan rekomendasi berbasis bukti	**Bentuk Penilaian** : Aktifitas Partisipasif, Penilaian Hasil Project / Penilaian Produk, Penilaian Praktikum, Tes	Studi kasus, diskusi kelompok, presentasi, dan simulasi evaluasi keamanan.		**Materi:** Prinsip evaluasi keamanan jaringan, Teknik analisis efektivitas firewall, IDS/IPS, dan enkripsi, Studi kasus implementasi keamanan jaringan dunia nyata, Metodologi penilaian risiko dan rekomendasi perbaikan **Pustaka:** *Handbook Perkuliahan*	0%

9	Mahasiswa dapat merancang arsitektur keamanan jaringan yang meliputi perimeter security, segmentasi jaringan, kontrol akses, monitoring, dan respons insiden sesuai konteks organisasi.	1. Kemampuan mengidentifikasi kebutuhan keamanan organisasi 2. Keterampilan dalam merancang arsitektur jaringan dengan layered security 3. Kemampuan mengintegrasikan tools dan teknologi keamanan yang relevan 4. Kreativitas dalam menyusun strategi respons dan pemulihan insiden 5. Kemampuan dokumentasi dan presentasi desain yang jelas dan terstruktur	**Bentuk Penilaian** : Penilaian Hasil Project / Penilaian Produk	Project-based learning, diskusi kelompok, studi kasus, dan presentasi.		**Materi:** Konsep arsitektur keamanan jaringan, Prinsip desain defense-in-depth, Teknologi keamanan jaringan (firewall, IDS/IPS, VPN, dll.), Segmentasi jaringan dan micro-segmentation, Strategi monitoring dan incident response planning **Pustaka:** *Handbook Perkuliahan*	0%
10	Mahasiswa dapat merancang arsitektur keamanan jaringan yang meliputi perimeter security, segmentasi jaringan, kontrol akses, monitoring, dan respons insiden sesuai konteks organisasi.	1. Kemampuan mengidentifikasi kebutuhan keamanan organisasi 2. Keterampilan dalam merancang arsitektur jaringan dengan layered security 3. Kemampuan mengintegrasikan tools dan teknologi keamanan yang relevan 4. Kreativitas dalam menyusun strategi respons dan pemulihan insiden 5. Kemampuan dokumentasi dan presentasi desain yang jelas dan terstruktur	**Bentuk Penilaian** : Penilaian Hasil Project / Penilaian Produk	Project-based learning, diskusi kelompok, studi kasus, dan presentasi.		**Materi:** Konsep arsitektur keamanan jaringan, Prinsip desain defense-in-depth, Teknologi keamanan jaringan (firewall, IDS/IPS, VPN, dll.), Segmentasi jaringan dan micro-segmentation, Strategi monitoring dan incident response planning **Pustaka:** *Handbook Perkuliahan*	0%
11	Mahasiswa dapat menganalisis log serangan, mengidentifikasi teknik yang digunakan penyerang, melakukan akuisisi data forensik, serta menyusun laporan investigasi insiden keamanan jaringan.	1. Kemampuan menganalisis pola serangan dari log jaringan 2. Ketepatan dalam mengidentifikasi teknik dan alat serangan 3. Kemampuan melakukan akuisisi dan preservasi data forensik 4. Kelengkapan dan kejelasan laporan investigasi insiden	**Bentuk Penilaian** : Penilaian Praktikum, Penilaian Hasil Project / Penilaian Produk	Studi kasus, simulasi serangan, demonstrasi tools forensik, diskusi kelompok, dan praktikum mandiri.	Analisis kasus forensik jaringan dengan menyediakan file pcap dan log serangan untuk dianalisis, mahasiswa diminta membuat laporan investigasi lengkap yang diupload melalui LMS	**Materi:** Jenis-jenis pola serangan jaringan, Teknik analisis log dan traffic jaringan, Prinsip-prinsip forensik digital, Tools forensik jaringan (Wireshark, Autopsy, FTK), Prosedur investigasi insiden keamanan **Pustaka:** *Handbook Perkuliahan*	0%
12	Mahasiswa dapat menganalisis, menilai, dan merekomendasikan perbaikan pada kebijakan keamanan informasi berdasarkan standar industri seperti ISO 27001, NIST, atau COBIT.	1. Kemampuan mengidentifikasi kelemahan dalam kebijakan keamanan informasi 2. Kemampuan membandingkan kebijakan dengan standar industri yang relevan 3. Kemampuan memberikan rekomendasi perbaikan berdasarkan evaluasi	**Bentuk Penilaian** : Penilaian Hasil Project / Penilaian Produk, Penilaian Praktikum	Studi kasus, diskusi kelompok, presentasi, dan simulasi evaluasi kebijakan.	Analisis Kebijakan Keamanan Informasi, Mahasiswa diminta untuk mengevaluasi sebuah contoh kebijakan keamanan informasi terhadap standar industri tertentu (misalnya ISO 27001) dan menyusun laporan rekomendasi perbaikan.	**Materi:** Prinsip-prinsip evaluasi kebijakan keamanan informasi, Standar industri keamanan informasi (ISO 27001, NIST Framework, COBIT), Teknik identifikasi gap dan ketidaksesuaian, Penyusunan rekomendasi perbaikan kebijakan **Pustaka:** *Handbook Perkuliahan*	0%
13	Mahasiswa dapat menciptakan solusi keamanan yang efektif dan inovatif untuk lingkungan cloud dan hybrid, mengintegrasikan berbagai teknologi dan pendekatan keamanan.	1. Kemampuan merancang arsitektur keamanan terintegrasi untuk cloud dan hybrid 2. Kreativitas dalam memilih dan mengombinasikan tools keamanan 3. Kesesuaian solusi dengan kebutuhan bisnis dan regulasi 4. Kemampuan mengimplementasikan proof of concept atau simulasi	**Bentuk Penilaian** : Penilaian Hasil Project / Penilaian Produk, Penilaian Praktikum, Praktik / Unjuk Kerja	Project-based learning, studi kasus, diskusi kelompok, dan demonstrasi praktis.		**Materi:** Prinsip keamanan cloud dan hybrid, Teknologi keamanan terintegrasi (seperti CASB, CSPM, CWPP), Desain arsitektur keamanan, Implementasi dan testing solusi **Pustaka:** *Handbook Perkuliahan*	0%

14	Mampu mengimplementasikan teknik pengamanan aplikasi web dan layanan jaringan dalam skenario nyata	1.Kemampuan mengidentifikasi kerentanan keamanan pada aplikasi web 2.Kemampuan mengimplementasikan mekanisme autentikasi dan otorisasi 3.Kemampuan mengkonfigurasi firewall dan sistem deteksi intrusi 4.Kemampuan menerapkan enkripsi data pada layanan jaringan	**Bentuk Penilaian** : Penilaian Praktikum, Praktik / Unjuk Kerja	Demonstrasi, praktikum, studi kasus, dan diskusi interaktif.		**Materi:** Web Application Firewall (WAF), Secure Socket Layer (SSL)/Transport Layer Security (TLS), Authentication dan Authorization mechanisms, Intrusion Detection/Prevention Systems, Vulnerability assessment tools **Pustaka:** *Handbook Perkuliahan*	0%
15	Mahasiswa dapat mengidentifikasi ancaman dan kerentanan dalam infrastruktur TI, menilai dampak dan kemungkinan terjadinya risiko, serta merancang rekomendasi mitigasi berdasarkan analisis risiko yang komprehensif.	1.Kemampuan mengidentifikasi ancaman dan kerentanan dalam infrastruktur TI organisasi 2.Kemampuan menilai tingkat risiko berdasarkan dampak dan kemungkinan terjadinya 3.Kemampuan merancang strategi mitigasi risiko yang efektif dan efisien 4.Kemampuan menyusun laporan evaluasi risiko dengan rekomendasi yang jelas dan terstruktur	**Bentuk Penilaian** : Penilaian Hasil Project / Penilaian Produk, Penilaian Praktikum	Studi kasus, diskusi kelompok, presentasi, dan simulasi analisis risiko menggunakan tools seperti risk assessment matrix..		**Materi:** Konsep dasar manajemen risiko keamanan informasi, Metodologi analisis risiko (kuantitatif dan kualitatif), Identifikasi ancaman dan kerentanan dalam infrastruktur TI, Penilaian dampak dan kemungkinan risiko, Strategi mitigasi dan kontrol keamanan, Penyusunan laporan evaluasi risiko **Pustaka:** *Handbook Perkuliahan*	0%
16	Mahasiswa dapat menganalisis, mengevaluasi, dan merekomendasikan perbaikan kebijakan keamanan informasi berdasarkan standar industri yang relevan.	1.Kemampuan mengidentifikasi elemen-elemen kebijakan keamanan informasi 2.Kemampuan membandingkan kebijakan dengan standar industri (seperti ISO 27001, NIST) 3.Kemampuan mengevaluasi kesenjangan dan ketidaksesuaian 4.Kemampuan memberikan rekomendasi perbaikan yang spesifik dan terukur	**Bentuk Penilaian** : Penilaian Hasil Project / Penilaian Produk, Penilaian Portofolio, Tes	Studi kasus, diskusi kelompok, presentasi, dan analisis dokumen.	Analisis dokumen kebijakan keamanan informasi dan pembuatan laporan evaluasi kesesuaian standar	**Materi:** Prinsip dan komponen kebijakan keamanan informasi, Standar industri keamanan informasi (ISO 27001, NIST Framework), Teknik evaluasi dan audit kebijakan, Studi kasus kebijakan keamanan pada organisasi nyata **Pustaka:** *Handbook Perkuliahan*	0%

Rekap Persentase Evaluasi : Case Study

No	Evaluasi	Persentase
		0%

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.