|  |  |  |  |
| --- | --- | --- | --- |
| binadarmalogo.png | **RENCANA PEMBELAJARAN SEMESTER *(SEMESTER LESSON PLAN)*** | Nomor Dok | FRM/KUL/01/02 |
| Nomor Revisi | 02 |
| Tgl. Berlaku | 1 Januari 2018 |
| Klausa ISO | 7.5.1 & 7.5.5 |

|  |  |  |  |
| --- | --- | --- | --- |
| **Disusun oleh** *(Prepared by)* | **Diperiksa oleh** *(Checked by)* | **Disetujui oleh** *(Approved by)* | **Tanggal Validasi**  *(Valid date)* |
|  |  |  |  |
|  |  |  |

1. Fakultas *(Faculty)* : Ilmu Komputer
2. Program Studi *(Study Program)*  : Magister Teknik Informatika Jenjang *(Grade)* : S-2
3. Mata Kuliah *(Course)* : IT Risk Management & Disaster Recovery SKS *(Credit) : 3* Semester *(Semester)* :  *1*
4. Kode Mata Kuliah *(Code)* : MTIK-232 Sertifikasi *(Certification)* : Ya *(Yes)* Tidak *(No)*
5. Mata Kuliah Prasyarat *(Prerequisite)*  :  - ..............................................
6. Dosen Koordinator *(Coordinator)* : -

✓

1. Dosen Pengampuh *(Lecturer)* :  Tim *(Team)* Mandiri *(Personal)*
2. Capaian Pembelajaran Mata Kuliah (*Course* *Learning Outcomes*) :

|  |  |  |
| --- | --- | --- |
| Capaian Pembelajaran Lulusan Program Studi MTI (CPL) | Sikap  Pengetahuan  Keterampilan Umum  Keterampilan Khusus | 1. Bertakwa kepada Tuhan Yang Maha Esa dan mampu menunjukkan sikap religius 2. Menjunjung tinggi nilai kemanusiaan dalam menjalankan tugas berdasarkan agama, moral dan etika. 3. Dapat berperan sebagai warga negara yang bangga dan cinta tanah air, memiliki nasionalisme serta rasa tanggungjawab pada negara dan bangsa. 4. Dapat berkontribusi dalam peningkatan mutu kehidupan bermasyarakat, berbangsa, dan bernegara berdasarkan Pancasila. 5. Dapat bekerja sama dan memiliki kepekaan sosial serta kepedulian terhadap masyarakat dan lingkungan. 6. Dapat menghargai keanekaragaman budaya, pandangan, agama, dan kepercayaan, serta pendapat atau temuan orisinal orang lain. 7. Taat hukum dan disiplin dalam kehidupan bermasyarakat dan bernegara. 8. Menunjukkan sikap bertanggungjawab atas pekerjaan di bidang keahliannya secara mandiri. 9. Menginternalisasi nilai, norma, dan etika akademik. 10. Menginternalisasi semangat kemandirian, kejuangan, dan kewirausahaan 11. Memiliki kemampuan memecahkan permasalahan sains dan teknologi dalam bidang Ilmu Komputer/Informatika melalui pendekatan inter atau multidisipliner. 12. Mempunyai pengetahuan dan pemahaman sejumlah tema ilmu komputer, termasuk abstraksi, kompleksitas dan evolusi dari perubahan/pengembangan keilmuan dan prinsip-prinsip umum ilmu komputer seperti berbagi (*sharing*) sumber daya, keamanan (*security*) dan bekerja secara paralel (*concurrency*). 13. Memiliki pengetahuan sesuai dengan capaian pembelajaran program studi S2 Ilmu Komputer pada ***“Domain Spesific”*** atau ***“Research”*** sesuai dengan konsentrasi Program Studi yaitu *Enterprise IT Infrastructure, Enterprise Network Security,* dan *Enterprise Software Engineering.* 14. Mampu mengembangkan pemikiran logis, kritis, sistematis, dan kreatif melalui penelitian ilmiah, penciptaan desain atau karya seni dalam bidang ilmu pengetahuan dan teknologi yang memperhatikan dan menerapkan nilai humaniora sesuai dengan bidang keahliannya, menyusun konsepsi ilmiah dan hasil kajiannya berdasarkan kaidah, tata cara, dan etika ilmiah dalam bentuk tesis, dan memublikasikan tulisan dalam jurnal ilmiah terakreditasi tingkat nasional dan mendapatkan pengakuan internasional berbentuk presentasi ilmiah atau yang setara; 15. Mampu melakukan validasi akademik atau kajian sesuai bidang keahliannya dalam menyelesaikan masalah di masyarakat atau industri yang relevan melalui pengembangan pengetahuan dan keahliannya. 16. Mampu menyusun ide, hasil pemikiran, dan argumen saintifik secara bertanggung jawab dan berdasarkan etika akademik, serta mengkomunikasikannya melalui media kepada masyarakat akademik dan masyarakat luas. 17. Mampu mengidentifikasi bidang keilmuan yang menjadi obyek penelitiannya dan memposisikan ke dalam suatu peta penelitian yang dikembangkan melalui pendekatan interdisiplin atau multidisiplin. 18. Mampu mengambil keputusan dalam konteks menyelesaikan masalah pengembangan ilmu pengetahuan dan teknologi yang memperhatikan dan menerapkan nilai humaniora berdasarkan kajian analisis atau eksperimental terhadap informasi dan data. 19. Mampu mengelola, mengembangkan dan memelihara jaringan kerja dengan kolega, sejawat di dalam lembaga dan komunitas penelitian yang lebih luas. 20. Mampu meningkatkan kapasitas pembelajaran secara mandiri; dan 21. Mampu mendokumentasikan, menyimpan, mengamankan, dan menemukan kembali data hasil penelitian dalam rangka menjamin kesahihan dan mencegah plagiasi.   Mampu mendesain, menganalisis, dan mengimplementasikan *behaviour* sistem berbasis komputer yang berkualitas (terukur dan teruji) dengan mengaplikasikannya pada *domain* yang sesuai dengan konsentrasi Program Studi yaitu *Enterprise IT Infrastructure, Enterprise Network Security*, dan *Enterprise Software Engineering* berdasarkan kebutuhan dan keterbatasan sistem, serta mampu mengelolanya dengan tepat. |
| Capaian Pembelajaran Mata Kuliah (CPMK) | Mampu mendesain, menganalisis dan mengevaluasi prinsip-prinsip keamanan informasi dan risiko yang terlibat dan diperlukan dalam proses mitigasi bencana, meliputi kegiatan komputer forensik untuk manajemen risiko keamanan dan mengusulkan metode pemulihan dari serangan dan gangguan keamanan dan bencana secara cepat pada infrastruktur TI, demi kelangsungan bisnis dan organisasi. | |

1. Deskripsi Mata Kuliah

|  |  |
| --- | --- |
| Deskripsi Singkat Mata Kuliah | Merupakan mata kuliah khusus pada konsentrasi Program Studi yaitu “*Enterprise IT Infrastructure”* yang memberikan gambaran dalam mendesain, menganalisis dan mengevaluasi prinsip-prinsip keamanan informasi dan risiko yang terlibat dan diperlukan dalam proses mitigasi bencana, meliputi kegiatan komputer forensik untuk manajemen risiko keamanan dan mengusulkan metode pemulihan dari serangan dan gangguan keamanan dan bencana secara cepat pada infrastruktur TI, demi kelangsungan bisnis dan organisasi. |

1. Bahan Kajian

|  |  |
| --- | --- |
| Bahan Kajian (Materi Pembelajaran) | 1. *Risk Management – Contingency Planning Within Information Security* 2. *Risk Management – Planning For Organizational Readiness* 3. *Technical aspect of Information Security* 4. *Network Risk – Intrusion* 5. *Network Risk Mitigation – Intrusion Detection* 6. *Incident Response Preparation, Organisation and Prevention* 7. *Incident Response Reaction, Recovery and Maintenance* 8. *Principles and Investigations of Computer Forensics for risk mitigation* 9. *Computer Forensics – Tools and Acquisitions* 10. *Computer Forensics – Analysis and validation* 11. *Disaster Recovery – Preparation, Operation and Maintenance* 12. *Business Continuity – Preparation, Operations and Maintenance* |

1. Implementasi Pembelajaran Mingguan *(Implementation Process of weekly learning time)*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Minggu** | **Sub CPMK**  **(Kemampuan akhir yang direncanakan)** | **Bahan Kajian/Materi Pembelajaran**  *(Study Material)* | **Bentuk dan Metode Pembelajaran**  *(Learning Method)* | **Sumber Belajar**  *(Learning Resource)* | **Penilaian** | | |
| **Indikator**  *(Indicator)* | **Kriteria & bentuk** | **Bobot** |
| 1 | Mampu menganalisa dan mengevaluasi manajemen risiko dalam perencanaan kontinjensi dan kesiapan organisasi dalam menghadapi gangguan keamanan dan bencana Bagian 1 (CPMK 1.1) | 1. *Risk Management in Contingency Planning Within Information Security* 2. *Risk Management in Planning For Organizational Readiness* | Kuliah dan Diskusi *(Discovery Learning, Small Group Discussion)* | 1. E-learning: [https://elearning.binadarma.ac.id](https://elearning.binadarma.ac.id/) 2. Buku Referensi [1] dan [2] | Ketepatan dalam menganalisa dan mengevaluasi manajemen risiko dalam perencanaan kontinjensi dan kesiapan organisasi dalam menghadapi gangguan keamanan dan bencana | **Kriteria :** Ketepatan dalam menganalisa dan mengevaluasi manajemen risiko dalam perencanaan kontinjensi dan kesiapan organisasi dalam menghadapi gangguan keamanan dan bencana  **Bentuk :**  Diskusi |  |
| 2 | Mampu menganalisa dan mengevaluasi manajemen risiko dalam perencanaan kontinjensi dan kesiapan organisasi dalam menghadapi gangguan keamanan dan bencana Bagian 2 (CPMK 1.2) | 1. *Risk Management in Contingency Planning Within Information Security* 2. *Risk Management in Planning For Organizational Readiness* | Kuliah, Tugas dan Diskusi *(Discovery Learning, Small Group Discussion)* | 1. E-learning: [https://elearning.binadarma.ac.id](https://elearning.binadarma.ac.id/) 2. Buku Referensi [1] dan [2] | Ketepatan dalam menganalisa dan mengevaluasi manajemen risiko dalam perencanaan kontinjensi dan kesiapan organisasi dalam menghadapi gangguan keamanan dan bencana Bagian 2 | **Kriteria :** Ketepatan dalam menganalisa dan mengevaluasi manajemen risiko dalam perencanaan kontinjensi dan kesiapan organisasi dalam menghadapi gangguan keamanan dan bencana Bagian 2  **Bentuk :**  Diskusi |  |
| 3 | Mampu menganalisis dan mengevaluasi konsep dan teknik pada gangguan (intrusi) keamanan aplikasi dan jaringan teknologi informasi (CPMK 1.3) | 1. *Technical aspect of Information Security* 2. *Network Risk in Intrusion* | Kuliah, Tugas dan Diskusi *(Discovery Learning, Small Group Discussion)* | 1. E-learning: [https://elearning.binadarma.ac.id](https://elearning.binadarma.ac.id/) 2. Buku Referensi [1] dan [2] | Ketepatan dalam menganalisis dan mengevaluasi konsep dan teknik pada gangguan (intrusi) keamanan aplikasi dan jaringan teknologi informasi | **Kriteria :** Ketepatan dalam menganalisis dan mengevaluasi konsep dan teknik pada gangguan (intrusi) keamanan aplikasi dan jaringan teknologi informasi  **Bentuk :**  Diskusi |  |
| 4 | Kuis 1 | | | | | | 10% |  | 1. E-learning: [https://elearning.binadarma.ac.id](https://elearning.binadarma.ac.id/) 2. Buku Referensi [1] dan [2] |
| 5 | Mampu menganalisis dan mendemonstrasikan aspek mitigasi dan konfigurasi deteksi intrusi pada keamanan jaringan Bagian 1 (CPMK 1.4) | *Network Risk Mitigation in Intrusion Detection* | Kuliah dan Diskusi *(Role-Play & Simulation, Small Group Discussion)* | 1. E-learning: [https://elearning.binadarma.ac.id](https://elearning.binadarma.ac.id/) 2. Buku Referensi [1] dan [2] | Ketepatan dalam menganalisis dan mendemonstrasikan aspek mitigasi dan konfigurasi deteksi intrusi pada keamanan jaringan Bagian 1 | **Kriteria :** Ketepatan dalam menganalisis dan mendemonstrasikan aspek mitigasi dan konfigurasi deteksi intrusi pada keamanan jaringan Bagian 1  **Bentuk :**  Tugas dan Diskusi 1 | 5% |
| 6 | Mampu menganalisis dan mendemonstrasikan aspek mitigasi dan konfigurasi deteksi intrusi pada keamanan jaringan Bagian 2 (CPMK 1.5) | *Network Risk Mitigation in Intrusion Detection* | Kuliah dan Diskusi *(Role-Play & Simulation, Small Group Discussion)* | 1. E-learning: [https://elearning.binadarma.ac.id](https://elearning.binadarma.ac.id/) 2. Buku Referensi [1] dan [2] | Ketepatan dalam menganalisis dan mendemonstrasikan aspek mitigasi dan konfigurasi deteksi intrusi pada keamanan jaringan Bagian 2 | **Kriteria :** Ketepatan dalam menganalisis dan mendemonstrasikan aspek mitigasi dan konfigurasi deteksi intrusi pada keamanan jaringan Bagian 2  **Bentuk :**  Tugas dan Diskusi 2 | 5% |
| 7 | Mampu menganalisis dan mengevaluasi persiapan, pengorganisasian, dan pencegahan dalam tanggap insiden dan reaksi/respon terhadap insiden, pemulihan dan pemeliharaan teknologi informasi Bagian 1 (CPMK 1.6) | 1. *Incident Response Preparation, Organisation and Prevention* 2. *Incident Response Reaction, Recovery and Maintenance* | Kuliah, Tugas dan Diskusi *(Discovery Learning, Small Group Discussion)* | 1. E-learning: [https://elearning.binadarma.ac.id](https://elearning.binadarma.ac.id/) 2. Buku Referensi [1] dan [2] | Ketepatan dalam menganalisis dan mengevaluasi persiapan, pengorganisasian, dan pencegahan dalam tanggap insiden dan reaksi/respon terhadap insiden, pemulihan dan pemeliharaan teknologi informasi Bagian 1 | **Kriteria :** Ketepatan menganalisis dan mengevaluasi persiapan, pengorganisasian, dan pencegahan dalam tanggap insiden dan reaksi/respon terhadap insiden, pemulihan dan pemeliharaan teknologi informasi Bagian 1  **Bentuk :**  Diskusi |  |
| 8 | Ujian Tengah Semester (UTS) | | | | | | 25% |  | 1. E-learning: [https://elearning.binadarma.ac.id](https://elearning.binadarma.ac.id/) 2. Buku Referensi [1] dan [2] |
| 9 | Mampu menganalisis dan mengevaluasi persiapan, pengorganisasian, dan pencegahan dalam tanggap insiden dan reaksi/respon terhadap insiden, pemulihan dan pemeliharaan teknologi informasi Bagian 2 (CPMK 1.7) | 1. *Incident Response Preparation, Organisation and Prevention* 2. *Incident Response Reaction, Recovery and Maintenance* | Kuliah, Tugas dan Diskusi *(Discovery Learning, Small Group Discussion)* | 1. E-learning: [https://elearning.binadarma.ac.id](https://elearning.binadarma.ac.id/) 2. Buku Referensi [1] dan [2] | Ketepatan dalam menganalisis dan mengevaluasi persiapan, pengorganisasian, dan pencegahan dalam tanggap insiden dan reaksi/respon terhadap insiden, pemulihan dan pemeliharaan teknologi informasi Bagian 2 | **Kriteria :** Ketepatan dalam menganalisis dan mengevaluasi persiapan, pengorganisasian, dan pencegahan dalam tanggap insiden dan reaksi/respon terhadap insiden, pemulihan dan pemeliharaan teknologi informasi Bagian 2  **Bentuk :**  Diskusi |  |
| 10 | Mampu  menganalisa dan mengevaluasi prinsip-prinsip investigasi dari komputer forensik untuk mitigasi risiko dan praktik terbaik dalam menggunakan alat bantu komputer forensik Bagian 1 (CPMK 1.8) | 1. *Principles and Investigations of Computer Forensics for risk mitigation* 2. *Computer Forensics – Tools and Acquisitions* | Kuliah dan Diskusi *(Role-Play & Simulation, Small Group Discussion)* | 1. E-learning: [https://elearning.binadarma.ac.id](https://elearning.binadarma.ac.id/) 2. Buku Referensi [1] dan [2] | Ketepatan dalam menganalisa dan mengevaluasi prinsip-prinsip investigasi dari komputer forensik untuk mitigasi risiko dan praktik terbaik dalam menggunakan alat bantu komputer forensik | **Kriteria :** Ketepatan dalam menganalisa dan mengevaluasi prinsip-prinsip investigasi dari komputer forensik untuk mitigasi risiko dan praktik terbaik dalam menggunakan alat bantu komputer forensik  **Bentuk :**  Tugas dan Diskusi 3 | 5% |
| 11 | Mampu menganalisa dan mengevaluasi prinsip-prinsip investigasi dari komputer forensik untuk mitigasi risiko dan praktik terbaik dalam menggunakan alat bantu komputer forensik Bagian 2 (CPMK 1.9) | 1. *Principles and Investigations of Computer Forensics for risk mitigation* 2. *Computer Forensics – Tools and Acquisitions* | Kuliah dan Diskusi *(Role-Play & Simulation, Small Group Discussion)* | 1. E-learning: [https://elearning.binadarma.ac.id](https://elearning.binadarma.ac.id/) 2. Buku Referensi [1] dan [2] | Ketepatan dalam menganalisa dan mengevaluasi prinsip-prinsip investigasi dari komputer forensik untuk mitigasi risiko dan praktik terbaik dalam menggunakan alat bantu komputer forensik Bagian 2 | **Kriteria :** Ketepatan dalam menganalisa dan mengevaluasi prinsip-prinsip investigasi dari komputer forensik untuk mitigasi risiko dan praktik terbaik dalam menggunakan alat bantu komputer forensik Bagian 2  **Bentuk:** Tugas dan Diskusi 4 |  |
| 12 | Kuis 2 | | | | | | 10% |  | 1. E-learning: [https://elearning.binadarma.ac.id](https://elearning.binadarma.ac.id/) 2. Buku Referensi [1] dan [2] |
| 13 | Mampu menganalisa dan mengevaluasi teknik validasi komputer forensik yang digunakan dalam persiapan hingga pemulihan dan perawatan ketika terjadi bencana Bagian 1 (CPMK 1.10) | 1. *Computer Forensics – Analysis and validation* 2. *Disaster Recovery – Preparation, Operation and Maintenance* | Kuliah, Tugas dan Diskusi *(Discovery Learning, Small Group Discussion)* | 1. E-learning: [https://elearning.binadarma.ac.id](https://elearning.binadarma.ac.id/) 2. Buku Referensi [1], [2] dan [3] | Ketepatan dalam menganalisa dan mengevaluasi teknik validasi komputer forensik yang digunakan dalam persiapan hingga pemulihan dan perawatan ketika terjadi bencana Bagian 1 | Ketepatan dalam menganalisa dan mengevaluasi teknik validasi komputer forensik yang digunakan dalam persiapan hingga pemulihan dan perawatan ketika terjadi bencana Bagian 1  **Bentuk :**  Diskusi |  |
| 14 | Mampu menganalisa dan mengevaluasi teknik validasi komputer forensik yang digunakan dalam persiapan hingga pemulihan dan perawatan ketika terjadi bencana Bagian 1 (CPMK 1.11) | 1. *Computer Forensics – Analysis and validation* 2. *Disaster Recovery – Preparation, Operation and Maintenance* | Kuliah dan Diskusi *(Discovery Learning, Project Based Learning, Small Group Discussion)* | 1. E-learning: [https://elearning.binadarma.ac.id](https://elearning.binadarma.ac.id/) 2. Buku Referensi [1], [2] dan [3] | Ketepatan dalam menganalisa dan mengevaluasi teknik validasi komputer forensik yang digunakan dalam persiapan hingga pemulihan dan perawatan ketika terjadi bencana Bagian 1 | **Kriteria :** Ketepatan dalam menganalisa dan mengevaluasi teknik validasi komputer forensik yang digunakan dalam persiapan hingga pemulihan dan perawatan ketika terjadi bencana Bagian 1  **Bentuk :**  Diskusi |  |
| 15 | Mampu mendesain dan mendemonstrasikan kebutuhan bisnis yang berkelanjutan, meliputi persiapan, operasi dan perawatan dalam konteks mitigasi bencana dan gangguan keamanan teknologi informasi (CPMK 1.12) | *Business Continuity – Preparation, Operations and Maintenance* | Kuliah dan Diskusi *(Discovery Learning, Project Based Learning, Small Group Discussion)* | 1. E-learning: [https://elearning.binadarma.ac.id](https://elearning.binadarma.ac.id/) 2. Buku Referensi [1], [2] dan [3] | Ketepatan dalam mendesain dan mendemonstrasikan kebutuhan bisnis yang berkelanjutan, meliputi persiapan, operasi dan perawatan dalam konteks mitigasi bencana dan gangguan keamanan teknologi informasi | **Kriteria :** Ketepatan dalam mendesain dan mendemonstrasikan kebutuhan bisnis yang berkelanjutan, meliputi persiapan, operasi dan perawatan dalam konteks mitigasi bencana dan gangguan keamanan teknologi informasi  **Bentuk :**  Tugas dan Diskusi | 5% |
| 16 | Ujian Akhir Semester (UAS) | | | | | | 35% |

1. Pengalaman Belajar Mahasiswa *(Student Learning Experiences)*

Studi kasus.

1. Bentuk dan Bobot Penilaian
2. Bentuk Penilaian

Tugas = 20%

Kuis = 20%

UTS/MID = 25%

UAS = 35%

1. Bobot penilaian

≥ 85 = A

≥ 70 s.d < 85 = B

≥ 60 s.d < 70 = C

≥ 50 s.d < 60 = D

< 50 = E

1. Buku Sumber *(References)*
2. Snedaker, S., Rima, C. (2013). *“Business Continuity and Disaster Recovery Planning for IT Professionals”.* Netherlands: Elsevier Science.
3. Gibson, D. (2014). *“Managing Risk in Information Systems”*. United States: Jones & Bartlett Learning.
4. Aulia, N. A., Antoni, D., Syamsuar, D., & Cholil, W. (2021). *Sistem Tata Kelola Keamanan Teknologi Informasi Berbasis Framework COBIT 5 (Studi Kasus: SMA Negeri 1 Palembang).* Jurnal Informatika, 9(2), 30-37.