Mata Kuliah :	Infomation Security Audit	Semester :	7	Kode :	**SM721383**	SKS :	3
Prodi :	Manajemen	Dosen :	Candiwan				
Capaian Pembelajaran :	Pemahaman ISA						

(1) Minggu Ke	(2) Kemampuan Akhir yang Diharapkan	(3) Bahan Kajian	(4) Bentuk Pembelajaran	(5) Kriteria Penilaian	(6) Bobot Nilai
1.	Mahasiswa mengetahui cara mengaudit secara umum dan paham mengenai keamanan IT.	1. Audit secara umum 2. Pentingnya Audit Keamanan Informasi 3. Menjelaskan peran auditor	1. Presentasi 2. Tanya Jawab 3. Diskusi	Pemahaman audit dan keamanan informasi.	
2.	Mahasiswa dapat mengetahui dan memahami "IT security Standards and Frameworks"	"IT security Standards and Frameworks" : a. ISO27000 Series. b. COBIT c. NIST	1. Presentasi 2. Tanya Jawab 3. Diskusi 4. **Tugas 1 (**group atau individu) .	Pemahaman standard keamanan khususnya : ISO27000 Series, COBIT & NIST	5 %
3.	Mahasiswa dapat mengetahui cara mengaudit untuk item analysis resiko pada suatu perusahaan.	1. Penilaian Asset. 2.Macam-macam ancaman, vulnerability serta kemungkinan kejadian gangguan akibat acaman tsb pada suatu perusahaan. 3. Metoda perhitungan "riks score".	1. Presentasi 2. Tanya Jawab 3. Diskusi 4. **Tugas 2 (**group atau individu untuk membuat list resiko keamanan yg dihadapi perusahaan)	Dapat mengidentifikasi risiko yg ada, serta menghitung nilai resiko.	5 %

4.	Mahasiswa dapat memahami management resiko pada suatu perusahaan sehingga perusahaan dapat meminimalize resiko.	Metoda Manegement resiko pada beberapa referensi atau standard.	1. Presentasi 2. Tanya Jawab 3. Diskusi	Mahasiswa dapat menggunakan metoda management resiko pd perusahaan.	
5	Mahasiswa dapat memahami dan melakukan audit untuk : "Security policy & Organisation of Information Security".	1. Audit "Security policy 2. Audit "Organisation of Information Security " berdasarkan standard /referensi.	1. Presentasi 2. Tanya Jawab 3. Diskusi	Mahasiswa mempertimbangkan kebijakan keamanan dan organisasi dalam melakukan auditnya.	
6	Mahasiswa dapat memahami dan melakukan audit untuk "Asset Management & *Building & Maintaining an Effective Security Awareness Program".*	1. Audit pengelolaaan asset berdasarkan standar/referensi. 2. Audit bentuk-bentuk dan cara untuk melakukan "effective security awareness".	1. Presentasi 2. Tanya Jawab 3. Diskusi	Dalam auditnya mahasiswa dapat : -membedakan asset yg ada dalam perusahan. -mengidentifikasi betuk-bentuk awareness keamanan informasi.	
7	**Mahasiswa dapat memresentasi rencana audit keamanan informasi untuk project (perusahaan) yang dipilih.**	**Rencana audit mahasiswa.**	**Mahasiswa presentasi rencana audit keamanan informasi pada perusahaan respondent. Diskusi antar mahasiswa (Tugas 3).**	**Rencana audit harus lengkap dari pengetahuan keamanan informasi, audit dan maturity level, risk**	10%
8	***UTS***	Materi ujian diambil dari materi minggu ke-1 sd minggu ke-7	Ujian tertulis.	Mahasiswa dapat menjawab semua pertanyaan yang diberikan .	25 %
9	Mahasiswa dapat memahami dan melakukan audit untuk "Physical security & Access Control".	1. Physical security pada suatu perusahaan, khususnya ISP, telkomunikasi dll 2. "Access Control" pada perushaan khususnya ISP, telkomunikasi dll.	Presentasi dan tanya jawab dengan mahasiswa.	Mahasiswa mempertimbangkan "physical security" dan "access control " pada organisasi dalam melakukan auditnya.	

10	Mahasiswa dapat memahami dan melakukan audit untuk "*Information Security Incident Management (ISIM)", serta pemahaman/penggunaan tools untuk audit*	1. ISIM berdasarkan standar / referensi. 2. Memahami "incident respond team" pada suatu perusahaan dan negara. 3.*Pemahaman / penggunaan tools untuk audit*	1. Presentasi dan tanya jawab dengan mahasiswa. 2. Tanya Jawab. 3. Diskusi 4. Tugas 4 : Mahasiswa mencari artiket mengenai "insident response team" pada beberpa perusahaan atau beberapa negara.	Mahasiswa mempertimbangkan ISIM pada organisasi dalam melakukan auditnya.	2.5 %
11	Mahasiswa dapat memahami dan melakukan audit untuk "Systems development and maintenance (SDM)".	Systems development and maintenance (SDM) berdasarkan ISO27001 atau referensi lain (COBIT, NIST).	Presentasi dan tanya jawab dengan mahasiswa.	Mahasiswa mempertimbangkan SDM pada organisasi dalam melakukan auditnya.	
12	Mahasiswa dapat memahami dan melakukan audit untuk "Network and Communications Controls & Criptography".	"Network and communication & Criptography" berdasarkan Standard : ISO27001 atau referensi lain (COBIT, NIST).	1. Presentasi dan tanya jawab dengan mahasiswa. 2. Tanya Jawab. 3. Diskusi 4. **Tugas 5** : Mahasiswa mencari artiket mengenai fungsi port2 yg sering dipakai dalam dunia internet dan setting terbuka/tertutup untuk meningkatkan keamanan.	Mahasiswa mempertimbangkan "operation and communication" pada organisasi dalam melakukan auditnya.	2.5 %

13	Mahasiswa dapat memahami dan melakukan audit untuk "Supplier and Third Party Relationship".	1. "Supplier telationship" berdasarkan ISO27001 atau referensi lain (COBIT, NIST). 2. "Third Party telationship" berdasarkan ISO27001 atau referensi lain (COBIT, NIST).	Presentasi dan tanya jawab dengan mahasiswa. **Tugas 6** : **m**empelajari contoh surat NDA pada suatu perusahaan.	Mahasiswa mempertimbangkan aturan "supplier and third party relationship" pada organisasi dalam melakukan auditnya.	5 %
14	Mahasiswa dapat memahami dan melakukan audit untuk "*Business Continuity Management* & Compliance Controls (BCM & CC)".	Item pengendalian pada 1. "*Business Continuity Management (BCM).* *2."*Compliance Controls " CC)".	Presentasi dan tanya jawab dengan mahasiswa.	Mahasiswa mempertimbangkan BCM & CC pada organisasi dalam melakukan auditnya.	
15	*Mahsasiswa dapat mempresentasi Project Akhir audit keamaan informasi dengan mempertimbangkan semua aspek yang sudah dipelajari.*	Bahan (konten) presentasi harus ada item yg tersedia pada standard, risk assessmet, risk metodology, maturity level dll.	Presentasi dan tanya jawab dengan mahasiswa **(Tugas 7**)	Mahasiswa mempetimbangkan sumua item yg ada pada standar dalam melakukan auditnya.	20%
16	***UAS***	**Materi ujian diambil dari materi minggu ke-9 sd minggu ke-15..**	**Ujian tertulis.**	**Mahasiswa dapat menjawab semua pertanyaan yang diberikan .**	**25 %**