

Informasi Pelaksanaan Wawancara :

Informasi Pelaksanaan Interviewer	
Interviewer	: Tasya Rafiiqa
Narasumber	: Arief Yulham E., A.Md
Hari, Tanggal	: Senin, 29 Mei 2023
Pukul	: 10.00 Wib - selesai
Lokasi	: Ruangan Unit Teknologi Informasi
Informasi Narasumber I	
Nama	: Arief Yulham E., A.Md
Jabatan	: Ka. Unit Teknologi Informasi
Instansi	: RSUD Ibnu Sina Kab. Gresik
Lama Bekerja	: 12 Tahun
Informasi Narasumber II	
Nama	: Mufid Ali Fatoni, S.Kom
Jabatan	: Staff Unit Teknologi Informasi
Instansi	: RSUD Ibnu Sina Kab. Gresik
Lama Bekerja	: 5 Tahun
Informasi Narasumber III	
Nama	: Aufa Anggun Probo Kusumo, S.Kom
Jabatan	: Staff Unit Teknologi Informasi
Instansi	: RSUD Ibnu Sina Kab. Gresik
Lama Bekerja	: 3 Tahun

Interview protocol digunakan untuk identifikasi risiko pada organisasi dan pengelolaan keamanan informasi. Interview protocol akan mengacu pada metode OCTAVE. Didalam metode OCTAVE terdapat 3 fase untuk mengetahui asset kritis organisasi dan pengelolaan keamanan informasi. Berikut ialah 3 fase metode OCTAVE:

- Fase 1 : Organizational View
Tujuannya ialah untuk mengetahui asset kritis, serta keamanan informasi yang telah diimplementasikan. Pada fase ke-1 ini peneliti melakukan interview dengan Kepala Unit TI di RSUD Ibnu Sina Kab. Gresik. Berikut merupakan interview protocol fase 1:

No	ORGANIZATION VIEW
	Aset Kritis
1	Pertanyaan:
	Aset apa saja yang ada di Unit TI RSUD Ibnu Sina Kab. Gresik?
	Jawaban:
	SIMRS E-hos, Komputer/PC client, Server, Printer, Jaringan, CCTV, AC.
2	Pertanyaan:
	Aset apa yang paling penting di Unit TI RSUD Ibnu Sina Kab. Gresik?
	Jawaban:
	Semua aset penting, tetapi yang paling penting adalah Server. Server digunakan untuk penyimpanan data SIMRS. Selain Server, Jaringan juga termasuk aset penting karena semua media elektronik saling berhubungan dan tukar-menukar data melalui jaringan.
3	Pertanyaan:
	Seberapa besar pengaruh jaringan terhadap keberlangsungan penggunaan sistem informasi yang ada di RSUD Ibnu Sina Kab. Gresik?
	Jawaban:
	Sangat besar pengaruhnya, karena jaringan digunakan untuk tukar-menukar data antar media/komputer. Jika jaringan trouble, maka akan menghambat akses komputer ke server begitupun sebaliknya. Apabila server down, maka user bisa tetap bisa menggunakan internet. Apabila jaringan/hardware jaringan mengalami kerusakan maka tidak bisa mengakses E-HOS dan internet.
4	Pertanyaan:
	Sistem informasi apa yang terdapat di RSUD Ibnu Sina Kab. Gresik?
	Jawaban:
	- SIMRS E-HOS,

	<ul style="list-style-type: none"> - Sistem Informasi Akutansi Keuangan (SIAK), - Sistem Informasi Kepegawaian (SIMPAG), - Sistem Informasi Farmasi (HEPPY), - Sistem Informasi Jasa Pelayanan (DOMPET RIA)
5	Pertanyaan:
	Siapa saja yang mempunyai kepentingan menggunakan aplikasi dan layanan TI?
	Jawaban:
	Seluruh pegawai RSUD Ibnu Sina Kab. Gresik.
Keamanan Informasi untuk Aset Kritis	
1	Pertanyaan:
	Apakah aplikasi dan layanan TI di lingkungan RSUD Ibnu Sina Kab. Gresik sudah memberikan <i>checklist</i> terkait kebutuhan keamanan asset informasi yang dimiliki?
	<ul style="list-style-type: none"> a. Jika sudah, apa saja kebutuhan keamanan yang dilihat dari <i>checklist</i> tersebut yang sudah terpenuhi? b. Jika belum, perlukan adanya <i>checklist</i> terkait kebutuhan keamanan asset informasi yang dimiliki?
	Jawaban:
	Sudah, dilakukan berupa Monev (monitoring evaluasi) terkait keamanan data dan informasi. Berupa <i>checklist</i> perbaikan server simrs, perbaikan jaringan data, serta penanganan waktu henti (downtime).
2	Pertanyaan:
	Adakah aturan dalam melakukan pengamanan terkait akses informasi pada aplikasi dan layanan TI?
	Jawaban:
	Ada, berupa surat keputusan direktur tentang hak akses sistem informasi manajemen rumah sakit.
3	Pertanyaan:
	Apakah ada pemeriksaan secara rutin terhadap keamanan asset?
	Jawaban:
	Ada.
4	Pertanyaan:

	Apakah ada kegiatan maintenance pada asset?
	Jawaban:
	Ada.
5	Pertanyaan:
	Apakah ada mekanisme untuk mencegah pembobolan asset?
	Jawaban:
	Ada. Untuk mekanismenya seperti penanaman antivirus disemua komputer dan jaringan di RS. Kemudian, mengaktifkan <i>firewall</i> jaringan untuk memfilter koneksi jaringan yang masuk dari luar RS. Adanya penanaman virtual machine/VM ware (PC) bisa diinstall beberapa OS (contoh: windows server, linux server).
6	Pertanyaan:
	Apakah sensitifitas informasi dilindungi oleh tempat penyimpanan yang aman?
	Jawaban:
	Ya. Tempat penyimpanan data terpisah dari ruang kerja karyawan.
Ancaman Aset Kritis	
1	Pertanyaan:
	Apakah asset informasi RSUD Ibnu Sina Kab. Gresik pernah mengalami ancaman?
	a. Jika pernah, apa saja ancaman yang pernah dialami? b. Jika belum, ancaman apakah yang memungkinkan terjadi?
	Jawaban:
Pernah, ancaman yang pernah dialami yaitu adanya serangan malware. Adapun kemungkinan ancaman yang terjadi yaitu, kebocoran data yang timbul akibat penyalahgunaan hak akses pada SIMRS.	
2	Pertanyaan:
	Berikan contoh bagaimana pihak dalam yang bertindak secara tidak sengaja dapat menggunakan akses fisik untuk mengancam sistem ini?
	Jawaban:
	Bisa jadi dengan pencurian aset perangkat keras atau penyalahgunaan data elektronik.
3	Pertanyaan:

	Bagaimana melakukan pencegahan terhadap ancaman asset TI?
	Jawaban:
	Memasang CCTV, pemberian password di setiap masing-masing PC, pembatasan hak akses terhadap SIMRS, pembatasan hak akses ruang server dengan pemasangan kunci fingerprint pada ruang server.
4	Pertanyaan:
	Seberapa sering terjadinya server down pada server?
	Jawaban:
	Seminggu sekali, pasti maintenance.
5	Pertanyaan:
	Seberapa sering terjadinya pembobolan data?
	Jawaban:
	Tidak ada.
6	Pertanyaan:
	Apakah pada aplikasi dan layanan TI dilakukan <i>update</i> antivirus?
	Jawaban:
	Ya, sudah dilakukan update antivirus.
7	Pertanyaan:
	Apakah ada SOP untuk meng <i>update</i> sistem tersebut?
	Jawaban:
	Ada.
Praktik Keamanan	
1	Pertanyaan:
	Apakah ada informasi mengenai aplikasi dan layanan TI di RSUD Ibnu Sina Kab. Gresik?
	Jawaban:
	Ada, pada website RSUD Ibnu Sina Kab. Gresik serta adanya pembagian brosur layanan Kesehatan berbasis IT.
2	Pertanyaan:
	Apakah aplikasi dan layanan TI menerapkan <i>framework</i> atau standar keamanan khusus asset informasi?
	a. Jika iya, standart atau <i>framework</i> apa yang digunakan?

	b. Jika tidak, perlukan adanya standart atau <i>framework</i> khusus pengamanan asset informasi?
	Jawaban:
	Ya. Standart keamanan berdasarkan login dan captcha saja dan <i>framework</i> yang digunakan yaitu codeigniter (CI), Laravel, Yii.
3	Pertanyaan:
	Apakah di RSUD Ibnu Sina Kab. Gresik sudah melakukan penilaian risiko untuk kewanan informasi?
	Jawaban:
	Sudah.
4	Pertanyaan:
	Apakah RSUD Ibnu Sina Kab. Gresik menerima dan bertindak atas laporan rutin dari informasi yang berhubungan dengan keamanan?
	Jawaban:
	Ya, contohnya complain terkait pendaftaran online. Akses E-HOS dari luar RS, memiliki alamat IP sendiri bukan domain.
5	Pertanyaan:
	Apakah kendala dalam melakukan implementasi standart atau <i>framework</i> pengamanan asset informasi pada RSUD Ibnu Sina Kab. Gresik?
	Jawaban:
	Ada, kendalanya kesulitan untuk memahami dan mempelajari perkembangan dari framework itu sendiri.
6	Pertanyaan:
	Apakah di RSUD Ibnu Sina Kab. Gresik sudah memiliki kebijakan dan prosedur dalam melindungi informasi ketika bekerja sama dengan Rumah Sakit lain?
	Jawaban:
	Sudah ada, RSUD Ibnu Sina sudah memiliki kebijakan dan prosedur terkait melindungi informasi.
Organisasi	
1	Pertanyaan:
	Apa masalah yang sering terjadi pada E-HOS System?
	Jawaban:

	Lemot atau server down.
2	Pertanyaan:
	Pernahkah terjadi pencurian informasi pada E-hos system? a. Jika pernah, informasi apa yang telah dicuri? Apa penyebab asset informasi tersebut bermasalah? b. Jika belum, informasi apa saja yang memungkinkan terjadinya pencurian?
	Jawaban:
	Tidak, yang mungkin terjadi penyalahgunaan hak akses oleh pegawai internal sendiri.
3	Pertanyaan:
	Apakah kapasitas server yang dimiliki Unit TI di RSUD Ibnu Sina Kab. Gresik sudah mencukupi?
	Jawaban:
	Sementara ini cukup, akan tetapi dikarenakan masih menggunakan server yang lama sehingga rencana pengadaan/ <i>update</i> server pada tahun 2024.
4	Pertanyaan:
	Berapa kali dalam setahun Unit TI di RSUD Ibnu Sina Kab. Gresik melakukan evaluasi terhadap keamanan teknologi informasi?
	Jawaban:
	2 kali dalam setahun atau 6 bulan sekali melakukan evaluasi keamanan.
5	Pertanyaan:
	Apakah di Unit TI RSUD Ibnu Sina Kab. Gresik sudah melakukan verifikasi untuk setiap bidang dalam mengurus hak akses dan otorisasi?
	Jawaban:
	Sudah, setiap karyawan sudah memiliki hak akses masing-masing.
6	Pertanyaan:
	Bagaimana kode etik yang diterapkan pada Unit TI RSUD Ibnu Sina Kab. Gresik terkait pengamanan asset informasi?
	Jawaban:
	Untuk kode etik pada RSUD Ibnu Sina sudah ada, seperti aturan yang berisi tentang penerbitan surat teguran/SP untuk karyawan yang melakukan

	penyalahgunaan hak akses yang berhubungan dengan keamanan aset informasi.
--	---

- Fase 2 : Technological View

Tujuannya ialah untuk mengetahui komponen utama dari asset kritis, teknologi untuk mengamankan komponen utama asset kritis. Pada fase ke-2 ini peneliti melakukan interview dengan staff bidang TI. Berikut daftar pertanyaan untuk fase ke-2:

TECHNOLOGICAL VIEW	
Komponen Kunci	
1	Pertanyaan:
	Perangkat TI apa saja yang dimiliki oleh RSUD Ibnu Sina Kab. Gresik?
	Jawaban:
	<ul style="list-style-type: none"> - Software : E-HOS System - Hardware : Komputer, Server, CCTV, AC, Printer - Network : Perangkat Jaringan - User : Pengguna
Kerentanan Teknologi	
1	Pertanyaan:
	Apakah di RSUD Ibnu Sina Kab. Gresik terdapat prosedur untuk menjaga kerentanan teknologi seperti meninjau sumber informasi, mengelola keamanan tempat penyimpanan, dan mengidentifikasi komponen infrastruktur?
	Jawaban:
	Ya, terdapat prosedur untuk menjaga kerentanan teknologi.
2	Pertanyaan:
	Bagaimana bentuk penanggulangan terkait adanya gangguan pada E-hos system?
	Jawaban:
	Identifikasi gangguan/masalah yang terjadi, kemudian menindaklanjuti gangguan tersebut sesuai dengan SPO perbaikan SIMRS.
3	Pertanyaan:
	Apakah Unit TI RSUD Ibnu Sina Kab. Gresik menjadwalkan dan melakukan evaluasi kerentanan E-hos system secara berkala?
	Jawaban:

	Ya, untuk evaluasi rutinitas setiap hari dilakukan akan tetapi untuk penjadwalan dilakukan dalam 6 bulan sekali.
4	Pertanyaan:
	Apakah Unit TI RSUD Ibnu Sina Kab. Gresik memiliki dokumen mengenai jenis-jenis kerentanan dan metode serangannya?
	Jawaban:
	Ya, dokumentasi secara elektronik.
5	Pertanyaan:
	Siapa yang bertanggung jawab manajemen kerentanan E-hos system di RSUD Ibnu Sina Kab. Gresik?
	Jawaban:
	Unit Teknologi Informasi
6	Pertanyaan:
	Apakah RSUD Ibnu Sina Kab. Gresik menyediakan kesempatan bagi staff TI untuk mengikuti pelatihan guna mengelola kerentanan teknologi dan menggunakan alat-alat evaluasi kerentanan?
	Jawaban:
	Ya.

- Fase 3 : Risk Analysis

Tujuannya ialah melakukan identifikasi risiko, perencanaan mitigasi. Pada fase ke-3 ini peneliti melakukan interview dengan Kepala Unit TI dan staff bidang TI. Berikut merupakan daftar pertanyaan untuk fase ke-3 yaitu:

	RISK ANALYSIS
	Strategi Perlindungan
1	Pertanyaan:
	Adakah strategi dalam melakukan pengamanan data dan informasi di RSUD Ibnu Sina Kab. Gresik?
	a. Jika sudah ada, strategi pengamanan data dan informasi apa yang diterapkan?
	b. Jika belum ada, perlukah adanya pengamanan data dan informasi?
	Jawaban:
	Ada, sesuai dengan SPO Keamanan Data dan Informasi.

Rencana Mitigasi Risiko	
1	Pertanyaan:
	Apakah aplikasi E-hos system dan layanan TI di RSUD Ibnu Sina Kab. Gresik memiliki <i>Disaster Recovery Plan (DRP)</i> pada asset informasinya?
	<ul style="list-style-type: none"> a. Jika sudah ada, asset informasi apakah yang sudah tercover oleh <i>DRP</i> tersebut? b. Jika belum ada, perlukah adanya <i>Disaster Recovery Plan (DRP)</i> pada asset informasi?
	Jawaban:
	Ada, informasi DBMS (<i>Database Management System</i>). Secara otomatis <i>terbackup</i> .