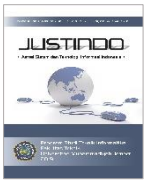
JUSTINDO
Jurnal Sistem dan Teknologi Informasi Indonesia
p-ISSN 2502-5724
e-ISSN 2541-5735

Jurnal Sistem dan Teknologi Informasi Indonesia
JUSTINDO Vol. 8 No. 1, Februari 2023, hal. 47-56
http://ejurnal.unmuhjember.ac.id/index.php/JUSTINDO/index
https://doi.org/10.32528/justindo.v8i1.219



Penilaian Risiko Keamanan Informasi pada *Website* dengan *Metode DREAD* dan *ISO 27005:2018*

Information Security Risk Assessment on the Website using the DREAD Method and ISO 27005:2018

Gina Cahya Utami*[1], Aden Bahtiar Supramaji[2], Khairunnisak Nur Isnaini[3]

[1,2,3]*Prodi Informatika, Fakultas Ilmu Komputer, Universitas Amikom Purwokerto*
Email: [1]ginacu12@gmail.com, [2]adenbahtiar36@gmail.com, [3]nisak@amikompurwokerto.ac.id
**Penulis Koresponden*

Diterima: 01 Januari 2023 | Direvisi: 03 Februari 2023 | Disetujui: 15 Februari 2023

ABSTRAK

Risiko keamanan informasi dapat terjadi dimana saja, termasuk di dalam sebuah *website*. Salah satunya yaitu di *website* IITC. Risiko yang terjadi pada *website* IITC salah satunya didapati kesalahan dalam sistem *upload* berkas peserta yang mana berkas tersebut tidak masuk ke dalam penyimpanan, masalah ini masuk ke dalam aspek *availability* atau ketersediaan data, apabila data hilang maka dapat berpotensi mengakibatkan kerugian berupa proses bisnis dan penyelenggaraan acara terhambat . Dari risiko-risiko tersebut dilakukan penelitian yang bertujuan untuk melakukan penilaian risiko keamanan informasi pada *website* IITC. Metode yang digunakan yaitu DREAD dan ISO 27005:2018. Metode DREAD digunakan untuk melakukan penilaian risiko pada *website* yang terdiri dari proses identifikasi ancaman, dokumentasi ancaman, dan penilaian risiko. Metode ISO 27005:2018 dalam penelitian ini melengkapi proses dalam identifikasi ancamannya. Dari hasil penelitian, risiko paling tinggi pada *website* IITC ditemukan pada aspek keamanan informasi *availability* dengan kerusakan bagian *upload* berkas. Penilaian risiko mendapatkan nilai rata-rata sebesar 11,5 yang artinya masuk ke dalam tingkat sedang, sehingga dapat diartikan bahwa *website* IITC masih dapat digunakan namun butuh beberapa prioritas perbaikan. Saran penelitian selanjutnya yaitu membahas risiko keamanan informasi berdasarkan aset-aset pada *website*, identifikasi risiko menggunakan *tools* atau *software*, dan proses penilaian menggunakan *framework* lain..

Kata kunci: penilaian risiko, keamanan informasi, *dread, iso 27005:2018*

ABSTRACT

Information security risks can occur anywhere, including on a website. One of them is on the IITC website. One of the risks that occur on the IITC website is an error in the participant file upload system where the file does not enter storage, this problem goes into the availability aspect of data, if data is lost it can potentially result in losses in the form of business processes and organizing events hampered Based on these risks, this research aims to assess information security risks on the IITC website. The methods in this research are DREAD and ISO 27005:2018. The DREAD method is used to carry out a risk assessment on the website, which consists of the threat identification process, threat documentation, and risk assessment. The ISO 27005:2018 method in this study completes the process of identifying threats. From the research results, the highest risk on the IITC website was found in the availability of information security aspects with damage to the file upload section. The risk assessment obtained an average score of 11.5, which means it is at the moderate level, so it means that the IITC website can still be used but needs several priority improvements. Suggestions for further research are discussing information security risks based on assets on the website, risk identification using tools or software, and the assessment process using other frameworks.

Keywords: *risk assessment, information security, dread, iso 27005:2018*

1. Pendahuluan

Penggunaan *website* sebagai media informasi dan pendaftaran, dapat memberikan peluang terhadap risiko serangan dan ancaman siber, hal ini berpotensi untuk mengganggu kelancaran dan keberlangsungan dari instansi atau organisasi (Triandi, 2019).

IITC atau Intermedia *Information Technology Information* merupakan salah satu program kegiatan mahasiswa yang diselenggarakan oleh UKM Intermedia Universitas Amikom Purwokerto. Acara IITC sendiri memiliki berbagai rangkaian acara berupa *pre-event* berupa *road show*, *main event* berupa perlombaan di berbagai bidang IT untuk para pelajar dan mahasiswa serta *webinar* teknologi untuk umum, dan *closing event* berupa *awarding* (penganugerahan penghargaan kepada para peraih juara lomba). *Website* IITC dapat di akses melalui link berikut https://iitc.intermediaamikom.org/. *Website* sendiri merupakan kumpulan halaman-halaman yang digunakan untuk menampilkan informasi berupa teks, gambar, animasi, suara, ataupun gabungan dari semuanya, baik bersifat statis maupun dinamis yang membentuk suatu rangkaian bangunan yang saling terkait, yang masing-masing dihubungkan dengan jaringan-jaringan halaman (Al et al., 2021)

Website IITC digunakan sebagai media utama pelaksanaan kegiatan seperti sebagai media pendaftaran peserta, laman pemberitahuan informasi terkini, penyedia profil dan informasi acara, serta sebagai media promosi dan identitas acara IITC Intermedia. Pada *website* IITC Intermedia tersimpan akun pengguna yang berisi data peserta kegiatan seperti nama lengkap, email, dan nomor telepon pribadi, selain itu detail riwayat transaksi pendaftaran yang berisi nomor rekening peserta dan kode transaksi tersimpan di dalam akun pengguna. *Website* IITC Intermedia digunakan sebagai media penyimpanan hasil karya peserta lomba kegiatan seperti *source code*, karya seni, dan lainnya yang akan dilombakan pada acara.

Berdasarkan dari hasil observasi, *website* IITC seringkali mengalami permasalahan yang tidak diinginkan seperti lama waktu pemrosesan data yang tidak konsisten dan media pengunggahan berkas yang bermasalah berupa hilangnya berkas setelah berkas di unggah. Apabila kendala-kendala pada *website* IITC terus dibiarkan, maka dapat berpotensi mengakibatkan kerugian berupa proses bisnis dan penyelenggaraan acara terhambat, terlebih lagi kendala tersebut termasuk dalam kategori risiko keamanan informasi.

Secara umum, keamanan informasi adalah perlindungan aset-aset informasi terhadap kehilangan atau kerusakan data untuk memastikan kelangsungan bisnis atau instansi, dan meminimalkan risiko bisnis atau instansi (Kristanto et al., 2019). Keamanan informasi bertujuan untuk mencegah dan meminimalisir adanya modifikasi serta pemanfaatan informasi dari pihak yang tidak diinginkan (Triandi, 2019).

Pada keamanan informasi terdapat beberapa risiko-risiko yang dapat muncul. Secara umum kemungkinan risiko yang dapat terjadi pada sebuah *website* diantaranya *malware*, virus, *SQL Injection.* Langkah antisipasi yang dapat dilakukan terkait adanya adanya risiko ancaman dan serangan siber, maka dibutuhkan penilaian risiko terhadap keamanan informasi yang berpotensi untuk menghambat dan merugikan organisasi atau instansi. Penilaian risiko dapat digunakan sebagai acuan dalam melakukan mitigasi atau perbaikan serta untuk menghindari aktivitas atau kegiatan yang tidak diinginkan (Jonny et al., 2021).

Metode penilaian risiko dapat dilakukan dengan beberapa cara, salah satunya adalah metode DREAD. DREAD merupakan singkatan dari *Damage, Potential, Reproducibility, Exploitability, Affected, and Discoverability*. Metode tersebut merupakan suatu model dari Microsoft untuk penghitungan risiko dan dapat memberikan informasi penilaian risiko untuk ancaman yang teridentifikasi (Hendayun et al., 2021). Metode DREAD dapat digunakan sebagai metode untuk melakukan perhitungan risiko keamanan berdasarkan acuan yang telah ditentukan sebelumnya, hasil dari perhitungan ini akan digunakan untuk menilai tingkat ancaman yang akan dikategorikan menjadi rendah, sedang, dan tinggi (Laksono & Prayudi, 2021).

ISO 27005:2018 digunakan untuk mengidentifikasi risiko keamanan informasi. ISO 27005 merupakan bagian dari keluarga ISO 27000, berdasarkan pada ISO 27001, sebuah organisasi atau instansi dapat menilai risiko keamanan dan menyusun aturan dan spesifikasi tertentu berdasarkan hasil identifikasi dan penilaian tersebut (Munawar et al., 2020). Menurut penelitian

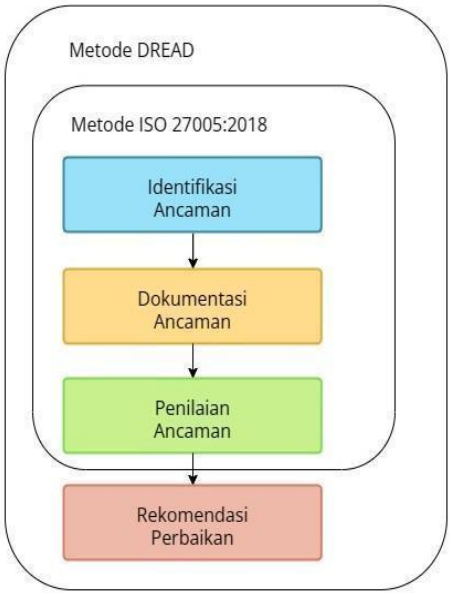
yang dilakukan oleh Diva Rizky Amananda Aspek keamanan informasi pada ISO 270001 terdiri dari beberapa aspek, diantaranya adalah aspek kerahasian (*confidentiality*), aspek kesediaan (*confidentiality*), dan aspek integritas (*integrity*) (Tiorentap Diva Rizky Amanda & Hosizah, 2020). ISO 27005 merupakan sebuah kerangka khusus yang terstruktur dan digunakan sebagai metode untuk mengidentifikasi risiko keamanan (Handayani et al., 2018). ISO 27005 dipilih karena dapat memberikan panduan dalam penerapan panduan manajemen risiko berbasis proses untuk memberikan dukungan terhadap penerapan dan pemenuhan persyaratan manajemen risiko informasi. ISO 27005 mendapatkan perubahan terbaru pada 2018.

Penelitian keamanan *website* elearning.unla.ac.id. yang dilakukan oleh Mokhamad Hendayun yang berjudul Pengujian dan Penilaian Kerentanan *E-Learning* Universitas Langlangbuana Menggunakan Metode STRIDE dan DREAD (Hendayun et al., 2021). Metode DREAD digunakan untuk menilai jenis ancaman yang ditemukan pada *website* elearning.unla.ac.id. dari penelitian tersebut didapatkan bahwa metode DREAD dapat digunakan menentukan level tingkat keamanan guna meminimalisir risiko keamanan yang mungkin terjadi. Penelitian lain yang dilakukan oleh Syasya Sahira (Sahira et al., 2020)., menggunakan metode ISO/IEC 27005:2018 untuk pengujian Aplikasi *E-Office* yang dikelola oleh PT Telkom Indonesia. ISO/IEC 27005:2018 digunakan untuk melakukan identifikasi jenis ancaman dan kemungkinan risiko yang terjadi pada Aplikasi *E-Office*. Dari hasil penelitian didapatkan bahwa ditemukan risiko dengan berbagai macam tingkatan mulai dari rendah, sedang, dan tinggi pada Aplikasi *E-Office*. Penelitian sebelumnya terkait analisis risiko oleh (Ramadhintia & Bisma, 2021), metode OCTAVE Allegro digunakan untuk penilaian risiko pada Aplikasi Ujian *Online* pada lembaga pendidikan. Dari hasil penelitian didapatkan bahwa metode OCTAVE dapat digunakan untuk penilaian risiko dengan hasil ditemukannya tujuh area yang berhasil diidentifikasi dan diberikan mitigasi sesuai *relative risk score.* Penelitian tentang analisis keamanan informasi pada keamanan fisik yang dilakukan oleh (Isnaini & Solikhatin, 2020) untuk memastikan bahwa universitas x dapat membangun keamanan fisik yang sesuai dengan prinsip CIA (confidentiality, integrity, availability). Metode penelitian yang digunakan penelitian kuantitatif serta COBIT 5 digunakan sebagai kerangka kerja untuk mengukur performa dan hasil keamanan fisik yang sudah diimplementasikan pada universitas x. Dari hasil evaluasi pada DSS5.5.5 dari COBIT didapatkan bahwa keamanan fisik universitas x berada pada tingkat 3 yang berarti keamanan fisik saat ini berjalan pada 2 prosedur standar operasi. Penelitian tentang evaluasi prinsip dasar keamanan informasi pada Universitas Amikom Purwokerto dengan menggunakan COBIT 5 oleh (Isnaini & Suhartono, 2022). Penelitian ini bertujuan untuk mencari tahu tingkatan dari prinsip keamanan informasi Universitas Amikom Purwokerto dengan menggunakan metode kualitatif deskriptif. Pengumpulan data dilakukan kepada 83 responden yang merupakan karyawan di Universitas Amikom Purwokerto. Dari hasil penelitian didapatkan berada pada tingkat 3 yang berarti karyawan telah menjalankan prosedur meskipun mereka belum menerapkan manajemen keamanan informasi. Pada penelitian sebelumnya yang dilakukan oleh (Cahyanto et al., 2017) mengenai keamanan informasi pada analisis dan deteksi malware. Metode *malware* analisis dinamis dan stastis untuk menganalisa cara kerja malware. Pada hasil penelitian didapatkan bahwa malware dapat melakukan login secara *remote* tanpa diketahui pemilik akses yang mana termasuk dalam risiko keamanan informasi.

Melihat pentingnya faktor keamanan informasi yang tersimpan pada *website* IITC Intermedia, maka penelitian ini bertujuan untuk melakukan penilaian terhadap risiko keamanan pada *website* IITC. Diharapkan penelitian ini mampu mengidentifikasi, menganalisis, dan mengevaluasi risiko keamanan informasi agar *website* IITC aman dari berbagai ancaman kedepannya. Selain itu penelitian ini juga dapat menjadi referensi bagi penelitian selanjutnya.

2. Metode Penelitian

Proses penelitian yang dilakukan pada *website* IITC *(Intermedia* Information *Technology Competition)* disusun menggunakan langkah-langkah yang disajikan pada Gambar 1. Proses penilaian risiko menggunakan metode DREAD dikombinasikan dengan metode ISO 27005:2018 untuk melengkapi proses dalam identifikasi ancamannya.



Gambar 1. Proses penilaian risiko menggunakan DREAD, ISO 27005:2018.

2.1. Implementasi Metode DREAD

Secara umum, model DREAD terdiri dari tiga tahap penting, yaitu identifikasi ancaman, dokumentasi ancaman, dan penilaian risiko atau penentuan tingkat ancaman (Suprihanto et al., 2018).

2.1.1 Identifikasi Ancaman

Tahap pertama dalam penelitian ini akan dilakukan identifikasi ancaman pada *website* IITC *(Intermedia Information Technology Competition)*. Tahap ini merupakan proses mencari informasi ancaman yang terdapat pada *website* IITC.

Proses identifikasi ancaman pada penelitian ini menggunakan tahap *risk identification* (identifikasi risiko) yang diterapkan pada metode ISO 27005:2018. Tahap tersebut bertujuan untuk mengetahui risiko yang dapat mengakibatkan kerugian bagi perusahaan, atau dalam penelitian ini yaitu sebuah *website,* sekaligus untuk memperoleh informasi tentang bagaimana kerugian tersebut dapat terjadi (Adianto et al., 2020).

2.1.2 Dokumentasi Ancaman

Tahap selanjutnya yaitu pembuatan dokumentasi ancaman yang berisi deskripsi ancaman, target 3 ancaman, dan teknik ancaman.

2.1.3 Penilaian Risiko

Tahap menganalisis atau memberi penilaian risiko terhadap *website* IITC *(Intermedia Information Technology Competition)* pada penelitian ini menggunakan metode DREAD. Tabel 1 menjelaskan mengenai sistem penilaian risiko menggunakan metode DREAD.

Tabel 1. Penilaian risiko metode DREAD (Faridi et al., 2021)

	Tinggi (3)	Sedang (2)	Rendah (1)
D	Sistem lumpuh; Dapat mengakses administrator; Sistem diambil alih; Dapat menambah konten	Bocornya informasi sensitif	Bocornya informasi biasa
R	Serangan dapat terjadi setiap saat dan berulang-ulang	Serangan dapat terjadi pada saat tertentu	Serangan sulit dilakukan walaupun memiliki kerentanan
E	Serangan dengan mudah dilakukan	Serangan berhasil namun membutuhkan beberapa kali percobaan	Membutuhkan orang yang sangat ahli dalam melakukan serangan.
A	Semua pengguna, konfigurasi default, pelanggan	Beberapa pengguna, konfigurasi non-default	Persentase yang sangat kecil dari pengguna, fitur tidak jelas;
D	Informasi kesalahan sistem dapat terlihat dengan jelas. Kerentanan ditemukan dengan mudah.	*Bug* sistem jarang terlihat.	Kesalahan sulit diidentifikasi

Pada Tabel 1 penilaian risiko dengan metode DREAD dibagi menjadi tiga kategori penilaian yaitu rendah dengan skor 1, sedang dengan skor 2, dan tinggi dengan skor 3. Huruf D dalam penilaian

DREAD disini merupakan *damage potential* yang berisi mengenai seberapa luas kerusakan jika terjadi serangan. Sedangkan R merupakan *reproducibility*, berisi tentang seberapa mudah serangan dapat terjadi kembali. E merupakan *exploitability,* yang berisi mengenai seberapa mudah ancaman melakukan serangan. A disini merupakan *affected users* yang berisi tentang seberapa luas dampak bagi pengguna. dan yang terakhir yaitu D atau *discoverability*, yang berisi seberapa mudah menemukan kerentanan.

Tingkat risiko diperoleh dari nilai total penjumlahan kategori ancaman DREAD dengan kisaran total antara 5-15. Rincian tingkatan dapat dilihat pada tabel 2.

Tabel 2. Tingkat risiko (Laksono & Prayudi, 2021)

Nilai	Tingkat Risiko
5 – 7	Rendah
8 – 11	Sedang
12 – 15	Tinggi

Pada Tabel 2, total yang didapat dari penjumlahan kategori ancaman DREAD apabila berjumlah antara 5 sampai dengan 7 maka akan berada pada tingkat rendah. Apabila total berada pada kisaran angka 8 sampai dengan 11 maka berada pada tingkat sedang. Apabila totalnya mencapai angka 12 sampai dengan 15 maka tergolong pada tingkat tinggi.

2.2. Rekomendasi Perbaikan

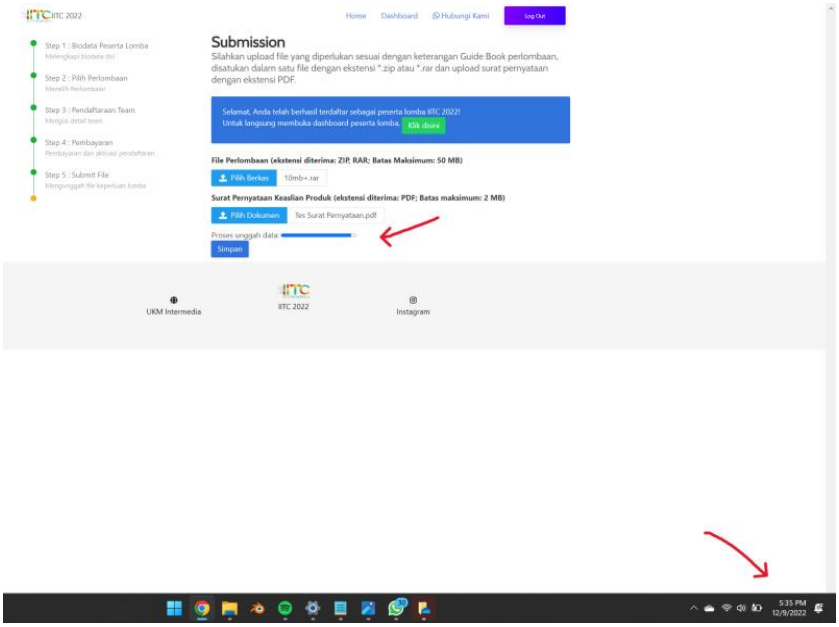
Tahap selanjutnya setelah mengetahui nilai dan tingkat risiko dari setiap ancaman yakni menyusun mitigasi atau rekomendasi perbaikan sebagai langkah untuk mencegah risiko dari setiap ancaman (Laksono & Prayudi, 2021).

3. Hasil Dan Pembahasan

3.1. Implementasi Metode DREAD

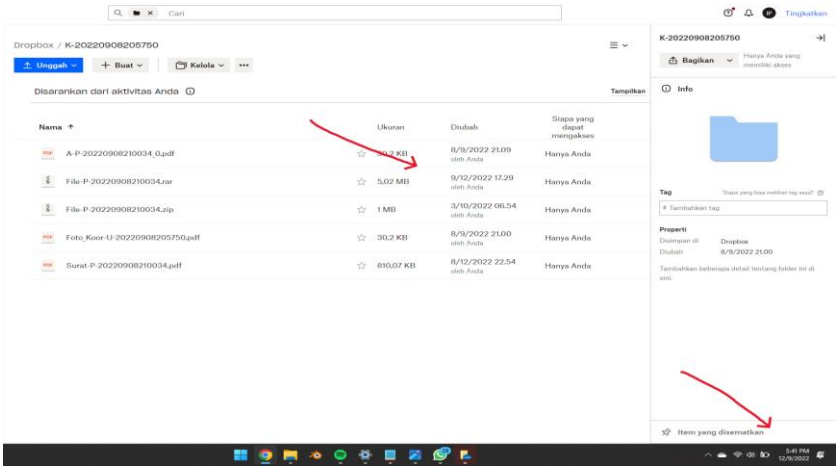
3.1.1 Identifikasi Ancaman menggunakan ISO 27005:2018

Hasil dari observasi langsung terhadap *website* IITC dan wawancara kepada salah satu pengembang *website* IITC, didapatkan bahwa pada *website* IITC ditemukan kendala pada laman akun peserta di bagian unggah berkas seperti pada Gambar 2. Kesalahan pada proses unggah berkas ini menyebabkan berkas yang sudah diunggah oleh akun pengguna gagal dan tidak masuk ke dalam penyimpanan sistem, yang mana kendala tersebut tidak sesuai dengan aspek keamanan informasi ketersediaan data atau *availability.*



Gambar 2. Laman pengunggahan berkas peserta

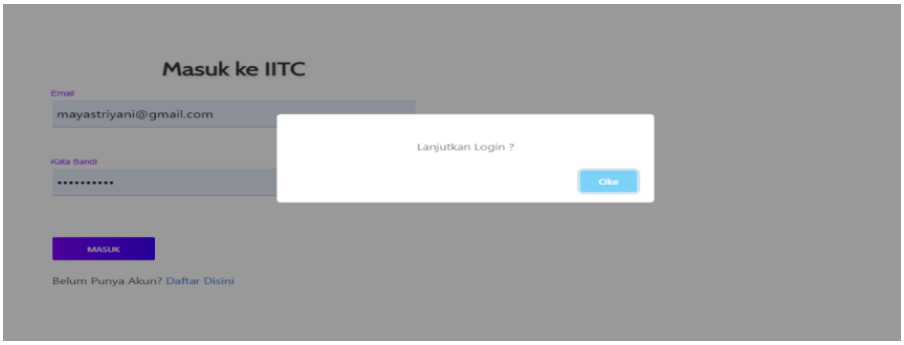
Pada Gambar 2 dilakukan proses pengunggahan berkas pada pukul 17.35 dengan ukuran berkas lebih dari 10 MB.



Gambar 3. Berkas gagal diunggah dan tidak masuk kedalam system

Pada Gambar 3, terlihat bahwa proses unggah berkas yang dilakukan sebelumnya tidak masuk ke dalam penyimpanan sistem yang ditunjukkan dengan perbedaan waktu pengunggahan berkas, maka hal ini membuktikan bahwa pada *website* IITC tidak memenuhi aspek keamanan informasi ketersediaan data atau *availability*.

Pada pengamatan selanjutnya, ditemukan bahwa pada halaman *login* peserta yang ditunjukkan pada Gambar 4, pada saat peserta melakukan *login* kedalam *website* tidak tersedia pengamanan lebih lanjut seperti autentikasi berupa *e-mail* ataupun SMS untuk membuktikan memang benar yang berusaha untuk *login* merupakan pemilik asli.



Gambar 4. Halaman *login* peserta

Langkah selanjutnya setelah peserta memasukkan *e-mail* dan kata sandi, peserta hanya diberikan opsi untuk melanjutkan *login*, maka hal tersebut membuktikan bahwa *website* IITC belum memenuhi aspek keamanan informasi *integrity* atau integritas.

Pada observasi berikutnya dilakukan proses wawancara kepada salah satu dari tim pengembang *website* IITC, dari hasil wawancara didapatkan bahwa SDM dari tim pengembang IITC masih kurang, hal ini didukung dengan proses pembuatan dan pengembangan *website* IITC dilakukan oleh mahasiswa yang belum seluruhnya teruji keahlian dan kemampuannya pada bidang tersebut melalui sertifikasi keahlian atau kompetensi.

Pada wawancara berikutnya didapatkan bahwa data peserta kegiatan IITC yang tersimpan di dalam sistem belum termanajemen dengan baik. Hal ini berpotensi untuk membuka peluang penyalahgunaan hak akses terhadap data peserta yang tersimpan, yang mana hal tersebut belum sesuai dengan aspek keamanan informasi *confidentiality* atau kerahasiaan.

Langkah selanjutnya yaitu dilakukan observasi pada *website* IITC dan wawancara kepada salah satu pengembang *website* IITC, langkah selanjutnya yakni melakukan identifikasi ancaman menggunakan ISO 27005:2018 dengan tipe *software* atau perangkat lunak. Berikut acuan tabel acuan dalam ISO 27005:2018 yang digunakan untuk mengidentifikasi ancaman pada *website* IITC pada Tabel 3.

Tabel 3. Acuan tabel ISO 27005:2018

Tipe	Contoh Kerentanan	Contoh Ancaman
Perangkat Lunak	Tidak ada atau tidak cukupnya pengujian perangkat lunak	Penyalahgunaan Hak
	Kerusakan pada perangkat lunak yang paling mencolok	Penyalahgunaan Hak
	Tidak ada fitur *logout* ketika meninggalkan perangkat lunak	Penyalahgunaan Hak
	Pembuangan/penggunaan kembali media penyimpanan tanpa mekanisme yang tepat	Penyalahgunaan Hak
	Kurangnya jejak audit	Penyalahgunaan Hak
	Alokasi hak akses yang salah	Penyalahgunaan Hak
	Perangkat lunak yang didistribusikan secara luas	Korupsi data
	Menerapkan program aplikasi pada data salah di waktu yang kurang tepat	Korupsi data
	Tampilan antar muka yang rumit	Kesalahan dalam penggunaan
	Kurangnya dokumentasi	Kesalahan dalam penggunaan
	Pengaturan parameter yang salah	Kesalahan dalam penggunaan
	Pengaturan tanggal yang salah	Kesalahan dalam penggunaan
	Kurangnya mekanisme autentikasi dan identifikasi seperti autentikasi pengguna	Penempaan hak
	Tabel kata sandi yang tidak terlindungi	Penempaan hak
	Manajemen kata sandi yang buruk	Penempaan hak
	Pengaktifan pelayanan yang tidak perlu	Pemrosesan data yang ilegal
	Perangkat lunak yang masih baru atau belum matang sepenuhnya	Malfungsi perangkat lunak
	Syarat pengembang belum jelas atau tidak lengkap	Malfungsi perangkat lunak
	Kurangnya pengendalian perubahan yang efektif	Malfungsi perangkat lunak
	Penggunaan dan pengunduhan perangkat lunak yang tidak terkontrol	Mengutak atik perangkat lunak
	Kurangnya salinan cadangan	Mengutak atik perangkat lunak
	Kurangnya perlindungan fisik pada bangunan, jendela, dan pintu	Pencurian media atau dokumen
	Kegagalan dalam membuat laporan manajemen	Penggunaan peralatan tidak sah

Berdasarkan dari acuan tabel ISO 27005:2018, berikut hasil pemetaan terhadap ancaman *website* IITC yang teridentifikasi menggunakan ISO 27005:2018 disajikan pada Tabel 4 di bawah ini.

Tabel 4. Hasil identifikasi ancaman menggunakan ISO 27005:2018

No.	Tipe	Kerentanan	Ancaman
1.	Perangkat Lunak	Pada laman peserta, untuk bagian *upload* berkas sering terjadi kesalahan dan data tidak terkirim	Penyalahgunaan Hak
2.	Perangkat Lunak	Kurangnya mekanisme autentikasi dan identifikasi seperti autentikasi pengguna	Penempaan Hak
3.	Perangkat Lunak	Data peserta periode kedua pelaksanaan kegiatan IITC tidak semuanya dibuang/hapus, namun beberapa masih ada yang tersimpan sebagian	Penyalahgunaan Hak
4.	Perangkat Lunak	SDM pengembang belum terlalu ahli dan kompeten dalam bidang yang diposisikan dalam proses pengembangan perangkat lunak	Malfungsi Perangkat Lunak

Hasil dari pengidentifikasian menggunakan ISO 27005:2018 seperti yang tertera pada Tabel 4, didapatkan bahwa terdapat empat kerentanan dengan tipe perangkat lunak atau *software*. Dari empat kerentanan tersebut terbagi menjadi dua ancaman penyalahgunaan hak, satu ancaman penempaan hak, dan satu ancaman malfungsi perangkat lunak.

3.1.2 Dokumentasi Ancaman

Proses dokumentasi ancaman berhasil dilakukan, selanjutnya dilakukan dokumentasi ancaman. Fungsi dari dokumentasi yaitu untuk mengetahui bagian-bagian dari fitur yang memiliki ancaman. Dokumentasi tiap ancaman disajikan pada tabel-tabel di bawah ini.

Tabel 5. Hasil dokumentasi ancaman 1

Deskripsi Ancaman	Penyalahgunaan Hak
Target Ancaman	Perangkat lunak, adanya kesalahan sistem *upload* berkas
Teknik Ancaman	Terdapat kesalahan sistem yang mengakibatkan berkas yang diunggah melalui akun peserta tidak masuk ke dalam penyimpanan sistem

Pada Tabel 5, terdapat contoh kerentanan berupa adanya kesalahan pada sistem *upload* berkas yang divalidasi oleh hilangnya berkas saat dilakukan proses pengunggahan berkas yang mana hal tersebut masuk ke dalam deskripsi ancaman penyalahgunaan hak.

Tabel 6. Hasil Dokumentasi Ancaman 2

Deskripsi Ancaman	Penempaan Hak
Target Ancaman	Perangkat lunak, kurangnya identifikasi dan *authentication* pada pengguna
Teknik Ancaman	Kurangnya mekanisme autentikasi & identifikasi seperti autentikasi pengguna pada saat *login*

Pada tabel 6, terdapat contoh kerentanan berupa kurangnya autentikasi dan identifikasi kepada pengguna yang divalidasi dengan tidak adanya validasi lebih lanjut kepada pengguna saat melakukan *login.*

Tabel 7. Hasil dokumentasi ancaman 3

Deskripsi Ancaman	Penyalahgunaan Hak
Target Ancaman	Perangkat lunak, pembuangan atau penggunaan kembali media penyimpanan tanpa alasan yang tepat dan jelas
Teknik Ancaman	Data peserta periode kedua pelaksanaan kegiatan IITC tidak semuanya dibuang/hapus, namun beberapa masih ada yang tersimpan sebagian

Pada tabel 7, berisi tentang contoh kerentanan pada perangkat lunak yang divalidasi dengan kurangnya manajemen terhadap data peserta kegiatan pada tahun sebelumnya.

Tabel 8. Hasil dokumentasi ancaman 4

Deskripsi Ancaman	Malfungsi Perangkat Lunak
Target Ancaman	Perangkat lunak, kurangnya kemampuan pengembang
Teknik Ancaman	SDM pengembang belum terlalu ahli dan kompeten dalam bidang yang diposisikan dalam proses pengembangan perangkat lunak

Pada tabel 8, terdapat contoh kerentanan berupa kurangnya kemampuan pengembang dari *website* IITC yang divalidasi dengan proses pembuatan dan pengembangan *website* IITC dilakukan oleh mahasiswa yang belum sepenuhnya teruji keahlian dan kemampuannya dalam bidang tersebut melalui sertifikasi keahlian atau kompetensi.

3.1.3 Penilaian Risiko

Berdasarkan hasil identifikasi ancaman yang telah dilakukan dengan menggunakan ISO 27005:2018, selanjutnya dilakukan penilaian dengan menggunakan metode DREAD. Penilaian akan didasarkan kepada tabel 2 untuk mengukur nilai total dan juga tingkat risiko yang akan ditimbulkan.

Tabel 9. Hasil penilaian risiko

Ancaman	D	R	E	A	D	Total	Tingkat
Pada laman peserta untuk bagian *upload* berkas sering terjadi kesalahan dan data tidak terkirim	1	3	3	3	3	13	Tinggi
Kurangnya mekanisme autentikasi dan identifikasi seperti autentikasi pengguna	1	2	2	2	2	9	Sedang
Data peserta periode kedua pelaksanaan kegiatan IITC tidak semuanya dibuang/hapus, namun beberapa masih ada yang tersimpan sebagian	3	3	2	3	2	12	Tinggi
SDM pengembang belum terlalu ahli dan kompeten dalam bidang yang diposisikan dalam proses pengembangan perangkat lunak	3	3	2	2	2	12	Tinggi
Rata-rata						11,5	Sedang

Berdasarkan hasil dari Tabel 9 terlihat bahwa hasil penilaian risiko menggunakan metode DREAD didapatkan tiga ancaman dengan tingkat yang tinggi dan satu ancaman dengan tingkat yang sedang, sedangkan secara keseluruhan didapatkan nilai sebesar 11,5 yang masuk ke dalam tingkat sedang.

Hasil identifikasi dengan menggunakan ISO 27005:2018 yang digunakan sebagai penunjang dalam penilaian risiko keamanan informasi, maka ISO 27005:2018 mampu memberikan hasil identifikasi ancaman dengan memberikan kriteria berupa tipe, kerentanan, dan ancaman yang ditemukan pada *website* IITC. Hasil identifikasi ancaman dengan menggunakan ISO 27005:2018 akan diberikan penilaian dan tingkat risiko dengan menggunakan metode DREAD. Perhitungan dengan menggunakan metode DREAD mampu memberikan nilai dan tingkat dari risiko *website*

IITC. Hasil dan tingkat penilaian dengan menggunakan metode DREAD digunakan sebagai acuan dalam memberikan mitigasi atau saran perbaikan untuk *website* IITC, sehingga dari hasil penelitian, didapatkan bahwa penilaian risiko keamanan informasi dengan metode DREAD dan ISO 27005:2018 pada *website* IITC Intermedia berhasil dilakukan. Didapatkan risiko paling tinggi pada aspek keamanan informasi *availability* atau ketersedian dengan kerusakan bagian *upload* berkas mendapatkan nilai 13, didapatkan risiko paling rendah pada aspek keamanan informasi integrity atau integritas dengan kurangnya autentikasi atau identifikasi tambahan saat akun pengguna melakukan *login* mendapatkan nilai 9, serta rata-rata nilai *website* IITC sebesar 11.5 yang masuk ke dalam kategori sedang, sehingga dapat diartikan bahwa *website* IITC masih dapat digunakan namun butuh beberapa prioritas perbaikan pada bagian *upload* berkas dengan nilai tertinggi pada aspek keamanan informasi *availability* atau ketersediaan.

3.2. Rekomendasi Perbaikan

Setelah mengetahui nilai dan tingkat risiko pada Tabel 9, beberapa rekomendasi yang perlu dilakukan antara lain *maintenance software* berkala untuk meminimalisir kerusakan dan menjaga agar kualitas sistem dapat berjalan sebagaimana mestinya (Wijaya & Karmilasari, 2021), perbaikan terhadap fitur pengunggahan berkas, dan pengkajian ulang terhadap SDM dari pengembang *website* IITC. Pengkajian ulang terhadap SDM didasarkan pada penelitian yang dilakukan oleh (Syahindra et al., 2022) untuk memperbaiki kinerja personel yang lalai dan kurangnya pelatihan dalam hal keamanan informasi. Rekomendasi perbaikan didasarkan pada tingkat tertinggi dari resiko yang berhasil diidentifikasi dan dilakukan penilaian.

4. Kesimpulan

Berdasarkan hasil dari penelitian, didapatkan bahwa penilaian risiko keamanan informasi dengan metode DREAD dan ISO 27005: 2018 pada *website* IITC Intermedia mendapatkan rata-rata nilai sebesar 11.5 dengan kategori sedang. ISO 27005:2018 dapat digunakan untuk mengidentifikasi risiko keamanan informasi *website* IITC dan DREAD dapat digunakan untuk melakukan penilaian terhadap risiko yang telah diidentifikasi, didapatkan bahwa risiko paling tinggi pada aspek keamanan informasi *availability* atau ketersediaan. Rekomendasi perbaikan yang diberikan diharapkan mampu memberikan gambaran terkait prioritas perbaikan yang dapat dilakukan pada *website* IITC Intermedia.

Penelitian selanjutnya dapat dilakukan diantaranya yang pertama dengan membahas lebih jauh risiko keamanan informasi berdasarkan aset-aset informasi yg ada didalam sebuah *website*. Kedua, identifikasi risiko dapat dilakukan dengan menggunakan *tools* atau *software* untuk menunjang proses identifikasi. Ketiga, proses penilaian dapat menggunakan *framework* lain dalam menilai risiko keamanan informasi seperti OCTAVE, FAIR, dan NIST.

5. DAFTAR PUSTAKA

Adianto, T., Ali, Y., Saptono, E., Penilaian, :, Serangan, R., & Pada…, S. (2020). *Risk Assessment of Cyber Attacks on Information Security Management System of PT. UAV*. *6*(1), 52–72. https://jatim.sindonews.com/read/8917/1/bssn-sebut-ada-10-sektor-yang-rentan-serangan-siber-

Cahyanto, T. A., Wahanggara, V., & Ramadana, D. (2017). Analisis dan Deteksi Malware Menggunakan Metode Malware Analisis Dinamis dan Malware Analisis Statis. *Justindo, Jurnal Sistem & Teknologi Informasi Indonesia*, *2*(1), 19–30. http://jurnal.unmuhjember.ac.id/index.php/JUSTINDO/article/view/1037

Faridi, M. K., Riadi, I., & Prayudi, Y. (2021). Pemodelan Ancaman Sistem Keamanan E-Health menggunakan Metode STRIDE dan DREAD. *Edumatic: Jurnal Pendidikan Informatika*, *5*(2), 157–166. https://doi.org/10.29408/edumatic.v5i2.3652

Handayani, N. U., Wibowo, A., Sari, D. P., Satria, Y., & Gifari, A. R. (2018). Penilaian Risiko Sistem Informasi Fakultas Teknik Universitas Diponegoro Menggunakan Metode Failure Mode Effect And Analysis Berbasis Framework ISO 27001. *Teknik*, *39*(2), 78–85. https://doi.org/10.14710/teknik.v39n2.15918

Hendayun, M., Utomo, H. P., & Nababan, D. P. (2021). *Pengujian dan Penilaian Kerentanan E-Learning Universitas Langlangbuana Menggunakan Metode STRIDE dan DREAD*. *2*(2), 2–6.

Isnaini, K. N., & Solikhatin, S. A. (2020). Information security analysis on physical security in university x using maturity model. *Jurnal Informatika*, *14*(2), 76. https://doi.org/10.26555/jifo.v14i2.a14434

Isnaini, K. N., & Suhartono, D. (2022). Evaluation of Basic Principles of Information Security at University Using COBIT 5. *MATRIK : Jurnal Manajemen, Teknik Informatika Dan Rekayasa Komputer*, *21*(2), 317–326. https://doi.org/10.30812/matrik.v21i2.1311

Jonny, J., Ambarwati, A., & Darujati, C. (2021). Penilaian Risiko Data Sistem Informasi Manajemen Puskesmas dan Aset Menggunakan ISO 27005. *Sistemasi*, *10*(1), 1. https://doi.org/10.32520/stmsi.v10i1.995

Laksono, A. C., & Prayudi, Y. (2021). Threat Modeling Menggunakan Pendekatan STRIDE dan DREAD untuk Mengetahui Risiko dan Mitigasi Keamanan pada Sistem Informasi Akademik. *JUSTINDO (Jurnal Sistem Dan Teknologi Informasi Indonesia)*, *6*(1), 9–20. https://doi.org/10.32528/justindo.v6i1.3944

Munawar, Z., Kom, M., & Putri, N. I. (2020). Keamanan Jaringan Komputer Pada Era Big [1] Z. Munawar, M. Kom, and N. I. Putri, "Keamanan Jaringan Komputer Pada Era Big Data. *Jurnal Sistem Informasi-J-SIKA*, 02, 1–7.

Ramadhintia, R., & Bisma, R. (2021). *Jurnal Sistem dan Teknologi Informasi Analisis Manajemen Risiko Aplikasi Ujian Online dengan Metode OCTAVE Allegro pada lembaga pendidikan*. *6*(2). http://jurnal.unmuhjember.ac.id/index.php/JUSTINDO

Sahira, S., Fauzi, R., Santosa, I., Industri, F. R., & Telkom, U. (2020). Analisis Manajemen Risiko Pada Aplikasi E-Office Yang Dikelola Oleh Pt Telkom Indonesia Menggunakan Standar Iso / Iec 27005 : 2018 Analysis of Risk Management in E-Office Application Managed By Pt Telkom Indonesia Using Iso / Iec 27005 : 2018 Standard. *Analisis Manajemen Risiko Pada Aplikasi E-Office Yang Dikelola Oleh Pt Telkom Indonesia Menggunakan Standar Iso / Iec 27005 : 2018 Analysis of Risk Management in E-Office Application Managed By Pt Telkom Indonesia Using Iso / Iec 27005 : 2018 Standard*, *7*(2), 6897–6909.

Suprihanto, D., Wardoyo, R., & Mustofa, K. (2018). Determination of weighting assessment on DREAD model using profile matching. *International Journal of Advanced Computer Science and Applications*, *9*(10), 68–72. https://doi.org/10.14569/IJACSA.2018.091009

Syahindra, I. P. S., Hetty Primasari, C., & Bagas Pradipta Iriantor, A. (2022). Evaluasi Risiko Keamanan Informasi Diskominfo Provinsi Xyz Menggunakan Indeks Kami Dan Iso 27005 : 2011. *Jurnal Teknoinfo*, *16*(2), 165. https://doi.org/10.33365/jti.v16i2.1246

Tiorentap Diva Rizky Amanda, & Hosizah. (2020). Aspek Keamanan Informasi dalam Penerapan Rekam Medis ElektronikdiKlinik Medical Check-Up MP. *Prosiding4SENWODIPA2020*, *November*, 53–66.

Wijaya, R. A., & Karmilasari, K. (2021). Pengukuran Kualitas Website Pengurus Cabang NU Depok Menggunakan Software Metric. *Jurnal Sisfokom (Sistem Informasi Dan Komputer)*, *10*(3), 438–443. https://doi.org/10.32736/sisfokom.v10i3.1267