Analisa Manajemen Resiko Keamanan Pada Sistem Informasi Akademik (Simak) Uin Raden Fatah Palembang Menggunakan Metode *Failure Mode And Effect Analysis* (FMEA)

Yesi Ramayani[1], Tri Oktarina[2]
Program Studi Sistem Informasi Universitas Bina Darma Palembang
Jl. Jenderal A. Yani No. 3, 9/10 Ulu, Kec. Seberang Ulu I, Palembang, Sumatera Selatan, Indonesia
E-mail: *yesiramayani109@gmail.com[1], tri_oktarina@binadarma.ac.id[2]*

Abstract *- The Academic Information System (SIMAK) of UIN Raden Fatah Palembang is a service information system provided by PUSTIPD (Center for Information Technology and Databases) to help Students and Lecturers, one of which is to view personal data, value data, KRS data. In implementing this SIMAK, there can be risks due to errors in implementing its use, one of which is system connection errors, damaged hardware, failed network, failed data backup, power failure, misuse of access rights, cybercrime. To minimize the effects of these threats can apply risk management that aims to overcome risks by anticipating losses that occur and implementing procedures that are able to minimize the occurrence of losses. With the management risk management of this information system, the author uses the Failure Mode and Effect Analysis (FMEA) method with a qualitative approach method. FMEA which is used to capture potential failures, risks and impacts is prioritized with a priority number called risk priority number (RPN). The results of this study show that there are 6 categories in the priority rpn value in SIMAK, namely, 1 very high category value, 3 high category values, 4 medium category values, 3 low category values, 6 very low category values and 1 category value with almost no failures.*

Keywords*: Risk Management, Academic Information Systems, Failure Mode and Effect Analysis*

Intisari - Sistem Informasi Akademik (SIMAK) UIN Raden Fatah Palembang merupakan sistem informasi pelayanan diberikan oleh pihak PUSTIPD (Pusat Teknologi Informasi dan Pangkalan Data) membantu Mahasiswa dan Dosen salah satunya untuk melihat data pribadi, data nilai, data krs. Dalam menerapkan SIMAK bisa muncul resiko akibat terjadi kesalahan dalam menerapkan penggunaannya salah satunya koneksi *system error, hardware* yang rusak, *network* yang gagal, *backup* data yang gagal, *power failure*, penyalahgunaan hak akses, *cybercrime*. Untuk meminimalkan efek dari ancaman tersebut dapat menerapkan manajemen resiko yang bertujuan mengatasi resiko guna mengantisipasi kerugian yang terjadi serta mengimplementasikan prosedur yang mampu menimimalkan terjadinya kerugian. Dengan adanya pengelolaan manajemen resiko sistem informasi ini Penulis menggunakan metode *Failure Mode and Effect Analysis* (FMEA) dengan metode pendekatan kualitatif. FMEA yang dipergunakan untuk mengetahui potensi kegagalan, resiko, akibat serta memprioritaskan kategori tersebut dengan nomor prioritas yaitu *Risk Priority Number* (RPN). Hasil dari penelitian ini menunjukkan bahwa terdapat 6 kategori dalam prioritas nilai RPN pada SIMAK yaitu, 1 nilai berkategori sangat tinggi, 3 nilai berkategori tinggi, 4 nilai berkategori sedang, 3 nilai berkategori rendah, 6 nilai berkategori sangat rendah dan 1 nilai berkategori hampir tidak ada kegagalan.

Kata kunci: Manajemen Resiko, Sistem Informasi Akademik, *Failure Mode and Effect Analysis*

I. PENDAHULUAN

Universitas Negeri Islam (UIN) Raden Fatah adalah perguruan tinggi agama islam negeri di Palembang. UIN memiliki sistem informasi pembelajaran secara online, seperti *E-Learning*, Silayak, dan SIMAK. Sistem Informasi Akademik (SIMAK) UIN Raden Fatah Palembang merupakan sistem informasi pelayanan yang diberikan oleh pihak c untuk Mahasiswa dan dosen

dalam mendapatkan informasi di bidang akademik. Dalam proses kegiatan yang dilakukan pada SIMAK ini dapat membantu Mahasiswa dan Dosen salah satunya untuk melihat data pribadi, data nilai, data krs, dll. penulis melakukan wawancara ke pada *staf IT* dari UIN Raden Fatah Palembang Kampus B, dalam membantu menjaga keamanan SIMAK ini staff IT UIN Raden Fatah Palembang menggunakan aplikasi tambahan yaitu, *Firewall.*

Dalam menerapkan SIMAK bisa muncul risiko akibat terjadinya kesalahan dalam menerapkan penggunaannya salah satunya, koneksi *system error, hardware* yang rusak atau bermasalah, *network* yang gagal, *backup* data yang gagal, *power failure,* penyalahgunaan hak akses, *cybercrime* dan lainnya. Untuk meminimalkan efek dari ancaman atau masalah tersebut penulis menerapkan manajemen risiko yang bertujuan mengatasi risiko guna mengantisipasi kerugian yang terjadi serta mengimplementasikan mekanisme yang bisa untuk meminimalkan terjadinya kerugian[1]. Dengan adanya pengelolaan dan manajemen risiko sistem informasi ini penulis menggunakan metode *Failure Mode And Effect Analysis* (FMEA).

Failure Mode and Effect Analysis (FMEA) ini dipergunakan dapat mengetahui potensi kegagalan, resiko, dampak serta memprioritaskan kategori tersebut dengan nomor prioritas yaitu *Risk Priority Number* (RPN). RPN diperoleh dengan mengalikan *Severity*, *Occurrence*, dan *Detection.* Rentan nilai RPN adalah 1-1000 (semakin besar angka RPN maka semakin besar pula resiko kegagalan yang terjadi). Hasil dari analisa penelitian ini nanti dapat mengetahui beberapa kategori dengan hasil dari perhitungan nilai RPN dan dapat mengetahui mitigasi dari hasil RPN yang tinggi.

II. SIGNIFIKASI STUDI

Manajemen resiko merupakan proses analisa mengidentifikasi dan pengendalian yang mengurangi resiko yang ada pada sebuah organisasi atau sebuah perusahaan yang bertujuan untuk memberikan perlindungan dan memperkecil setiap kegagalan yang ada pada organisasi atau perusahaan dari tingkat resiko yang tertinggi yang bisa menghambat proses tujuan suatu organisasi atau perusahaan. Adapun pengertian manajemen resiko merupakan pengelolaan identifikasi yang mengatur risiko dan menghasilkan strategi buat mengelolanya melalui sumber daya yang ada [2]. Adapun manfaat dari manajemen resiko sendiri ialah dapat membantu sebuah organisasi atau perusaan mencapai tujuannya, dapat memperkecil kemungkinan terjadinya pada setiap kegagalan untuk menyiapkan tindakan solusi untuk kedepannya.

Terdapat penelitian sebelumnya yang sudah ditulis oleh [3] yang membahas tentang Manajemen Resiko Redesign Sistem Pembelajaran Rekam Medis dengan Metode Failure Mode Effect Analysis dan di dapat hasil setelah melakukan analisa evaluasi serta monotoring implementasi redesign sistem penjajaran rekam medis asal SNF sebagai TDF menggunakan metode FMEA bisa secara signifikan menurunkan resiko diproses menerima permintaan rekam medis, pengambilan dan penyimpanan rekam medis mampu secara signifikan memperkecil risiko pada proses mendapatkan permintaan rekam medis, pengambilan serta penyimpanan rekam medis. Terdapat peneliti lainnya yang ditulis oleh [4] yang membahas tentang Analisis Risiko Sistem Informasi Pada RSIA Eria Bunda menggunakan Metode FMEA dan didapat hasil setelah melakukan analisa yaitu ada 1 kegiatan menggunakan kategori tinggi, 6 aktivitas kategori sedang serta 19 aktivitas menggunakan kategori rendah.

A. Lokasi Penelitian

Penelitian ini dilaksanakan di Universitas Kampus B UIN Raden Fatah Palembang yang beralamat di daerah Jakabaring.

B. Data Penelitian

Untuk mendapatkan data, penulis menggunakan pendekatan kualitatif yaitu wawancara terhadap staff yang mengelola SIMAK tersebut dan melakukan pengamatan langsung terhadap SIMAK.

C. Bahan Penelitian

Dalam penelitian ini penulis menggunakan alat dan bahan yaitu, laptop asus X441M, printer, *hardisk*, Ms. Wors 2010, Ms. Excel, Zotero.

D. Metode Penelitian dan Evaluasi

Untuk menganalisa manajemen resiko keamanan pada SIMAK UIN Raden Fatah Palembang ini Penulis memakai metode Failure Mode and Effect Analysis (FMEA) serta jenis pendekatan metode menggunakan kualitatif. Metode *Failure Mode and Effect Analysis* (FMEA) kali pertama dikeluarkankan akhir tahun 1940-an di dunia militer oleh US Armed Forces. Metode ini kali pertama diterapkan di industri penerbangan pada tahun 1960 dengan fokus peningkatan kepuasan pelanggan serta keamanan dan pencegahan produk cacat [5]. Penelitian ini berfokus pada penghitungan nilai RPN pada setiap kegagalan yang ada pada SIMAK dan dihitung menggunakan rumus RPN menggunakan Ms. Excel. Tujuan Metode *Failure Mode and Effect Analysis* (FMEA) sendiri adalah untuk mengambil tindakan dalam meminimalisir kegagalan, dimulai dengan konsekuensi tertinggi.

Adapun langkah – langkah pembuatan FMEA :

1. Menganalisa setiap kemungkinan potensi mode kegagalan yang dapat terjadi.
2. Menganalisa akibat yang ada dari terjadinya setiap potensi kegagalan.
3. Mengidentifikasi potensi kegagalan yang dapat terjadi pada tiap proses *severity, Occurrence and Detection.*
4. Menghitung RPN *(Risk Priority Number) = Severity x Occurrence x Detection.*

Keterangan :

RPN : Nomor Prioritas
Severity : Keparahan
Occurrence : Penyebab
Detection : Kontrol

5. Membuat *mitigasi* risiko atau saran rencana perbaikan (*recommended action*).

III. HASIL DAN PEMBAHASAN

UIN Raden Fatah Palembang untuk menaikkan kinerja sistem pembelajaran yang artinya bagian dari proses usaha sistem akademik maka perlu dilakukan analisa potensi kegagalan serta akibat dari kegagalan tersebut.

A. Potential failure mode

Ada berbagai macam hasil mode kegagalan yang terjadi berdasarkan hasil wawancara yang dilakukan dalam proses mengumpulkan data, sebagai berikut :

1. Data
   Data yang berkaitan dengan proses pembelajaran sistem informasi akademik UIN Raden Fatah Palembang.
2. Jaringan
   Jaringan yang digunakan dalam akses informasi.
3. *Server*
   Komputer yang dipakai sebagai kawasan menyimpan data serta bisa diakses oleh semua pengguna yang membutuhkannya.
4. Laptop / *PC*
   Dipakai oleh pengguna dalam kelangsungan proses bisnis.
5. Layanan Teknologi Informasi
   Karyawan yang memberikan akses kepada orang lain dan password yang jarang diganti.

TABEL I
IDENTIFIKASI RESIKO

No. *Code*	**Resiko**
R1	Kebakaran
R2	*Cybercrime*
R3	*Power Failure*
R4	*System Error*
R5	*Hardware* Rusak
R6	*Network* gagal
R7	Penyalahgunaan Hak Akses
R8	*Human Error*
R9	Ruangan yang Tidak Memadai
R10	*Backup* Data gagal
R11	Pelanggaran Terhadap Peraturan yang Ada

TABEL II
DAMPAK DARI KEGAGALAN

No. *Code*	***Potential Failure Mode***
R1	Hubungan arus pendek
R2	Kurangn keamanan
R3	Hubungan arus pendek
	Pemadaman Listrik
R4	Kesalahan fungsi di *system*
	Hardware kurang mendukung
R5	*Maintenance* tak teratur
	Virus
	Human error
R6	*Jaringan* lemah
R7	*Staff* yang menyampaikan hak aksesnya pada orang lain
	Password staff yang jarang diganti
R8	Kesalahan *input* data
	Data yang ada kurang *update*
	Kecilnya pengetahuan tentang *system*
R9	*Server* yang ditempatkan bersamaan dengan ruang IT
R10	*Server down*
R11	Kurangnya sosialisasi peraturan terhadap karyawan

B. Severity

Menurut [6] *severity* adalah penilaian yang berhubungan dengan seberapa besar kemungkinan terjadinya dampak yang mengakibatkan adanya kegagalan. Berikut melakukan perhitungan nilai pada tingkat dampak kegagalan yang telah diberikan oleh *staff* pengelola SIMAK, sebagai berikut.

TABEL III
PERHITUNGAN SEVERITY

No. *Code*	**Resiko**	***Severity***
R1	Kebakaran	7
R2	*Cybercrime*	5
R3	*Power Failure*	3
R4	*System Error*	2
R5	*Hardware* Rusak	1
R6	*Network* gagal	1
R7	Penyalahgunaan Hak Akses	2
R8	*Human Error*	1
R9	Ruangan yang Tidak Memadai	5
R10	*Backup* Data gagal	3
R11	Pelanggaran Terhadap Peraturan yang Ada	6

C. *Occurrence and Detection*

Menurut [7] *Occurrence* adalah kemungkinan terjadinya kegagalan selama menggunakan system. Sedangkan *Detection* adalah pengukuran terhadap kemampuan pengendalian kegagalan yang dapat terjadi. Berikut adalah perhitungan nilai dari *Occurrence and Detection* yang diberikan oleh *staff* pengelola SIMAK:

TABEL IV
PERHITUNGAN OCCURENT AND DETECTION

No. *Code*	Resiko	*Potential Failure Mode*	*occ*	*detec*
R1	Kebakaran	Hubungan arus pendek	1	7
R2	*Cybercrime*	Kurang keamanan	3	1
R3	*Power Failure*	Hubungan arus pendek	3	6
		Pemadaman Listrik	9	7
R4	*System Error*	Kesalahan fungsi pada sistem	2	5
		Hardware tidak mendukung	1	1
R5	*Hardware* Rusak	*Maintenance* tidak teratur	5	6
		Virus	1	1
		Human error	7	5
R6	*Network* Gagal	*Human error*	3	5
		Jaringan down	7	7
R7	Penyalahgunaan Hak Akses	*Staff* yang memberikan hak aksesnya pada orang lain	2	3
		Password staff yang jarang diganti	8	8
R8	*Human Error*	Kesalahan *input* data	3	5
		Data yang tersedia kurang update	5	6
		Kurangnya pengetahuan tentang sistem	5	8
R9	Ruang yang Tidak Memadai	Server yang diletakkan berdekatan dengan ruang IT	2	2
R10	*Backup* Data Gagal	*Server down*	5	7
R11	Pelanggaran Terhadap Peraturan yang Berlaku	Kurang sosialisasi peraturan pada karyawan	9	8

D. *Calculate RPN Value*

Selanjutnya adalah menentukan nilai RPN dari hasil kali antara *severity*, *occurent dan detection*. Berikut hasil RPN dari SIMAK UIN:

TABEL V
PERHITUNGAN RPN

No. *Code*	Resiko	*Potential Failure Mode*	RPN
R1	Kebakaran	Hubungan arus pendek	49
R2	*Cybercrime*	Kurangnya keamanan	15
R3	*Power Failure*	Hubungan arus pendek	54
		Pemadaman Listrik	189
R4	*System Error*	Kesalahan fungsi pada sistem	20
		Hardware yang tidak mendukung	2
R5	*Hardware* Rusak	*Maintenance* yang tak teratur	30
		Virus	1
		Human error	35
R6	*Network* Gagal	*Human error*	15
		Jaringan *down*	49
R7	Penyalahgunaan Hak Akses	*Staff* yang memberikan hak aksesnya kepada orang lain	12
		Password staff yang jarang diganti	128
R8	*Human Error*	Kesalahan *input* data	15
		Data yang tersedia kurang *update*	30
		Kurangnya pengetahuan mengenai sistem	40
R9	Ruang yang Tidak Memadai	*Server* yang diletakkan berdekatan dengan ruang IT	20

No. *Code*	Resiko	*Potential Failure Mode*	RPN
R10	*Backup* Data Gagal	*Server down*	105
R11	Pelanggaran Terhadap Peraturan yang Berlaku	Kurang sosialisasi peraturan pada karyawan	432

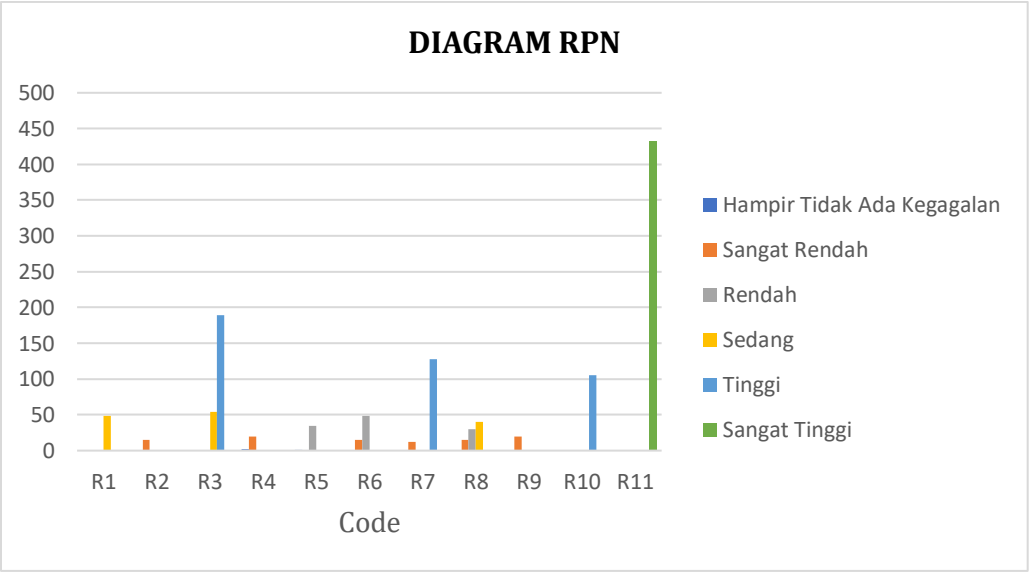
E. Prioritize RPN

Dari menghitung hasil RPN maka selanjutnya nilai RPN akan di urutkan berdasarkan dari yang tertinggi ke rendah. Berikut daftar RPN:

TABEL VI
PRIORITAS RPN

No. *Code*	*Potential Failure Mode*	RPN	Kategori
R11	Kurang sosialisasi peraturan pada karyawan	432	Sangat Tinggi
R3	Pemadaman Listrik	189	Tinggi
R7	Password staff yang jarang diganti	128	Tinggi
R10	*Server down*	105	Tinggi
R3	Hubungan arus pendek	54	Sedang
R1	Hubungan arus pendek	49	Sedang
R6	*Jaringan down*	49	Sedang
R8	Kurang mengetahui mengenai sistem	40	Sedang
R5	*Human error*	35	Rendah
R5	*Maintenance* tidak teratur	30	Rendah
R8	Data yang ada tidak *update*	30	Rendah
R4	Kesalahan fungsi pada sistem	20	Rendah
R9	Server yang diletakkan bersamaan dengan ruang IT	20	Rendah
R2	Kurang keamanan	15	Sangat Rendah
R6	*Human error*	15	Sangat Rendah
R8	Kesalahan *input* data	15	Sangat Rendah
R7	*Staff* yang memberikan hak aksesnya pada orang lain	12	Sangat Rendah
R4	*Hardware* tidak mendukung	2	Hampir Tidak Ada Kegagalan
R5	*Virus*	1	Hampir Tidak Ada Kegagalan

Di bawah ini dapat dilihat diagram level dari hasil perhitungan nilai RPN pada SIMAK UIN Raden Fatah Palembang.



Gambar 1. Level Diagram RPN SIMAK

F. Mitigasi Resiko

Mitigasi Resiko merupakan fase penanganan risiko dimana agen risiko terpilih berasal dari fase pertama dinilai menggunakan tindakan penanganan[6]. Berdasarkan hasil tabel 6 dan diagram di atas maka *potential failure mode* yang akan *dimitigasi* yaitu *code* R11, R10, R7, dan R3 karena memiliki tingkat yang sangat tinggi dan tinggi. Berikut ini merupakan tabel dari *mitigasi* pada SIMAK UIN Raden Fatah Palembang :

TABEL VII
MITIGASI SIMAK

No.	Potensi Kegagalan	Penyebab	Mitigasi
R11	Pelanggaran pada peraturan yang ada	Kurang sosialisasi peraturan pada karyawan	Memperketat peraturan yang ada dan menerapkan tindakan atau pinalti untuk yang melanggar
R10	*Backup* data gagal	*Server down*	Pemantauan yang selalu berkala dan selalu memastikan keadaan
R7	Penyalahgunaan hak akses	*Password staff* yang jarang diganti	Manajemen akses pengguna yang sebaiknya staff harus selalu mengganti password masimal 3 bulan sekali
R3	*Power failure*	Pemadaman Listrik	Monitoring yang bertahap dan menyiapkan keamanan pada kabel-kabel yang ada agar terjaga

IV. KESIMPULAN

Berdasarkan dari hasil analisa diatas maka penulis dapat menyimpulkan sebagai berikut: (1) Terdapat 11 identifikasi resiko dan *potential failure mode* pada SIMAK. (2) Berdasarkan hasil pehitungan RPN pada SIMAK terdapat 6 kategori yaitu sangat tinggi, tinggi, sedang, rendah, sangat rendah dan hampr tidak ada kegagalan. Berdasarkan kategori – kategori tersebut maka terdapat 1 nilai berkategori sangat tinggi, 3 nilai berkategori tinggi, 4 nilai berkategori sedang, 3 nilai berkategori rendah, 6 nilai berkategori sangat rendah dan 1 nilai berkategori hamper tidak ada kegagalan. (3) Adapun kegagalan yang harus mendapat *mitigasi* berdasarkan kategori sangat tinggi pada kode R11 pelanggaran pada peraturan yang ada karena kurang sosialisasi peraturan pada karyawan dengan nilai RPN 432, kategori tinggi pada kode R3 *power failure* karena pemadaman listrik dengan nilai RPN 189, kode R7 penyalahgunaan hak akses karena *password staff* yang jarang diganti dengan nilai RPN 128 dan kode 10 *backup* data gagal karena *server down* dengan nilai RPN 105.

REFERENSI

[1] Vaughan, Emmett J., and Therese M. Vaughan. Essentials of insurance: A risk management perspective. Wiley, 1995.

[2] Tunnisa, Ulfa, and Nyndita Erviana. "Manajemen Resiko Redesign Sistem Penjajaran Rekam Medis dengan Metode Failure Mode and Effect Analysis (FMEA)." Indonesian of Health Information Management Journal (INOHIM) 8.1 (2020): 08-20.

[3] Suroso, Jarot S. "Analisis Risiko Sistem Informasi Pada RSIA Eria Bunda menggunakan Metode FMEA." Jurnal Komputer Terapan 6.2 (2020): 210-221.

[4] Trijaya, Aditya SuprihadI. "Analisis Resiko Kegagalan Castor 5 Inch Swivel K1 Rem Dengan Failure Mode And Effect Analysis Di Pt X." Diss. UAJY, 2016.

[5] Munaroh, Lailatul, Yusuf Amrozi, and Rizky Agung Nurdian. "Pengukuran Risiko Keamanan Aset TI Menggunakan Metode FMEA Dan Standar ISO/IEC27001: 2013." TMJ (Technomedia Journal) 5.2 (2020): 167-181.

[6] Kusuma, Antonius. "Analisa Kinerja Mesin Wtp Menggunakan Metode Fmea Dan Penjadwalan Preventif Maintenance." Waktu: Jurnal Teknik UNIPA 17.1 (2019): 15-25.

[7] Matondang, Nurhafifah, Ika Nurlaili Isnainiyah, and Anita Muliawatic. "Analisis manajemen risiko keamanan data sistem informasi (Studi kasus: RSUD XYZ)." Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi) 2.1 (2018): 282-287.

[8] Ahmad, Imam, et al. "Software development dengan Extreme Programming (XP) pada aplikasi deteksi kemiripan judul skripsi berbasis Android." INOVTEK Polbeng-Seri Informatika 5.2 (2020): 297-307.

[9] Santoso, Agustinus Budi, Ahmad Zainudin, and Edwin Zusrony. "Penerapan Google API Service Pada Sistem Informasi Geografis Untuk Pemasaran Dan Pemetaan Kelompok UKM Kota Salatiga." INOVTEK Polbeng-Seri Informatika 6.2 (2021): 248-258.

[10] Lestari, Ade Fitria, Hilda Amalia, and Ari Puspita. "Penerimaan Teknologi Zoom Cloud Meeting terhadap Minat Belajar Siswa Dari Rumah Dengan TAM." INOVTEK Polbeng-Seri Informatika 6.1 (2021): 27-36.