Journal of Applied Informatics and Computing (JAIC)
Vol.x, No.x, Juli 201x, pp. xx~xx
e-ISSN: 2548-6861

Evaluasi Fungsi Protect (Perlindungan) NIST CSF 2.0 Terhadap Ancaman Social Engineering Pada Platform Roblox

Anne Natalya Hutagalung [1]*, Antoni Haikal [2]**
Teknik Informatika, Politeknik Negeri Batam
Rekayasa Keamanan Siber, Politeknik Negeri Batam
annehutagalung03@gmail.com [1], antoni@polibatam.ac.id [2]

Article Info

Article history:

Received 2026-05-12
Revised …
Accepted …

Keyword:

NIST CSF 2.0,

Social Engineering,

Roblox,

Gap Analysis,

Metaverse,

ABSTRACT

Penelitian ini bertujuan untuk mengevaluasi persepsi pengguna terhadap implementasu fungsi Protect pada kerangka kerja NIST Cyberseccurity Framework (CSF) 2.0 sebagai upaya mitigasi ancaman social engineering di platform Roblox. Penelitian ini menggunakan pendekatan kuantitatif dengan Teknik purposive sampling terhadap 200 responden pengguna aktif Roblox di Indonesia. Data dianalisis menggunakan perangkat lunak SPSS untuk mengukur tingkat kematangan (Maturity Level) berdasarkan model CMMI serta menghitung nilai kesenjangan (GAP) antara persepsi pengguna dan target ideal. Hasil penelitian ini men unjukkan bahwa berdasarkan persepsi 200 responden, implementasi fungsi Protect pada Roblox di persepsikan berada pada level 4 (Quantitatively Managed). meskipun demikian, masih ditemukan GAP rata-rata sebesar 0,20 terhadap target ideal. Temuan pada sub-kategori Awareness & Training (AT) menunjukkan bahwa edukasi proaktif mengenai ancaman keamanan siber masih menjadi titik lemah utama menurut persepsi pengguna, dengan nilai gap tertinggi mencapai 0,39 pada indikator edukasi pengguna. Hal ini bersfat indikatif berdasarkan persepsi pengguna dan buka merupakan hasil audit teknis resmi terhadap keamanan Roblox sebagai organisasi.

I. PENDAHULUAN

Roblox merupakan salah satu platform Metaverse yang paling popular saat ini, dan didefinisikan sebagai ruang virtual 3D yang dimana penggunanya diwakili oleh avatar dan dapat berinteraksi satu sama lain[1]. platform ini dikembangkan oleh CEO Roblox Bernama David Baszucki, game ini banyak di gemari oleh kalangan muda [2]. Pada platform ini pengguna bisa mengekspresikan identitas mereka secara bebas, realistis dan personal serta terhubung lebih erat dengan teman-teman secara virtual melalui fitur komunikasi chat, voice, dan juga Obrolan party[3]. Platform ini juga menyediakan Roblox Studio sehingga pengguna dapat berkreasi dan membangun pengalaman 3D imersif, avatar, dan asset digital yang menjangkau audiens global. Kreasi yang dihasilkan pengguna dapat dimonetisasi menjadi penghasilan nyata melalui Robux*(corp.roblox.com, 2024).*

Selain sebagai media hiburan, Roblox juga memiliki sistem ekonomi virtual melalui penggunaan mata uang digital Robux. Pengguna dapat membeli item premium, akses game tertentu, maupun melakukan transaksi digital menggunakan Robux yang diperoleh melalui top-up menggunakan e-wallet, mobile banking, maupun minimarket dan lainnya[4]. Tingginya aktivitas sosial dan ekonomi dalam platform ini menjadikan Roblox sebagai salah satu platform digital dengan tingkat interaksi pengguna yang sangat tinggi.

Kondisi ini memunculkan berbagai ancaman social engineering seperti, penyebaran informasi palsu(phishing), penipuan berbasis hadiah atau top-up palsu, peretasan, dan kebocoran data penting[5]. Platform Roblox juga dapat menimbulkan risiko psikologis, termasuk sebagai kecanduan[4]. Selain itu, interaksi sosial yang terbuka juga berpotensi dimanfaatkan oleh pelaku kejahatan untuk membangun kepercayaan dan mengeksploitasi korban secara finansial maupun seksual[6]. Beberapa penelitian sebelumnya

e-ISSN: 2548-6861

menunjukkan bahwa platform metaverse seperti Roblox memiliki risiko keamanan berupa phishing, scam, groomoing, serta kerentanan pengguna terhadap manipulasi social. Adele Serio (2024), Han et al. (2023), dan Atherton (2024). Namun, penelitian ini belum ada membahas terkait NIST CSF 2.0 dan pendekatan CMMI[5][7].

Tingginya interaksi sosial dan aktivitas ekonomi pengguna, juga membuat jumlah pemain Roblox di Indonesia menjadi informasi penting untuk melihat tingkat eksposur terhadap ancaman keamanan. Namun, data mengenai jumlah pemain Roblox di Indonesia menunjukkan perbedaan signifikan karena metode pengukurannya berbeda. Menurut survei APJII yang di kutip oleh Kompas.com, sekitar 2,07% pengguna internet Indonesia memainkan Roblox, yang di proyeksikan menjadi 1,33 juta pemain secara nasional[8], [9]. Sebagai bentuk mitigasi, Roblox telah menerapkan berbagai mekanisme keamanan, seperti verifikasi usia, parental control, pembatasan komunikasi antara anak dan pengguna dewasa yang tidak dikenal, serta penggunaan teknologi kecerdasan buatan AI Sentinel untuk mendeteksi perilaku mencurigakan dalam percakapan pengguna[10]. Upaya tersebut menunjukkan bahwa Roblox telah menerapkan sejumlah kontrol keamanan yang sejalan dengan fungsi Protect dalam NIST Cybersecurity Framework (CSF) 2.0.

upaya-upaya tersebut menunjukkan bahwa Roblox telah menerapkan sejumlah mekanisme yang sejalan dengan fungsi Protect dalam NIST CSF 2.0, seperti pengendalian akses, perlindungan data, dan pengelolaan kesadaran keamanan pengguna[11]. Namun, efektivitas implementasi mekanisme pengamanan tersebut masih perlu di evaluasi khususnya dari persepsi pengguna karena berbagai insiden dan celah keamanan masih terus ditemukan*(corp.roblox.com)*. Penelitian ini secara metodologis memfokuskan evaluasi pada fungsi Protect (PR) dalam kerangka kerja NIST Cybersecurity Framework 2.0. Hal ini disebabkan karena fungsi Identify (ID) dan Govern (GV) dalam NIST CSF 2.0 berada pada level strategis organisasi yang berkaitan dengan proses internal perusahaan seperti manajemen risiko, kebijakan keamanan, struktur pengambilan keputusan, serta strategis keamanan siber secara keseluruhan. Informasi tersebut bersifat internal dan tidak tersedia secara publik pada platform digital seperti Roblox. Fungsi Detect (DE) berkaitan dengan kemampuan organisasi dalam mendeteksi insiden secara real-rime melalui system monitoring dan ini memerlukan akses ke sistem. Begitu juga hal nya dengan Fungsi Respond (RS) dan Recover (RC) yang berupa prosedur tanggap insiden dan pemulihan pasca insiden. Fungsi ini bersifat reaktif dan tidak dapat di observasi langsung[12].

Sebaliknya, fungsi Protect (PR) berfokus pada kontrol teknis dan operasional yang dapat diamati langsung, seperti kontrol akses, verifikasi identitas, pembatasan komunikasi, pelatihan kesadaran pengguna, dan teknologi protektif berbasis sistem. Oleh karena itu, fungsi Protect dinilai paling relevan dan terukur untuk mengevaluasi efektivitas mitigasi ancaman social engineering pada platform Roblox. Oleh karena itu, penelitian ini akan menilai seberapa jauh Roblox telah menerapkan fungsi Protect sesuai dengan standar NIST CSF 2.0, serta mengidentifikasi gap atau kekurangan dalam proteksi terhadap ancaman social engineering[13].

Untuk mengetahui tingkat implementasi fungsi Protect pada Roblox, penelitian ini menggunakan model Capability Maturity Model Integration (CMMI) sebagai metode pengukuran tingkat kematangan keamanan. Model CMMI digunakan untuk menginterpretasikan hasil kuesioner berdasarkan skala Likert ke dalam level kematangan tertentu, mulai dari Initial hingga Optimizing. Dengan pendekatan ini, penelitian diharapkan dapat memberikan gambaran mengenai tingkat kematangan kontrol keamanan Roblox dalam menghadapi ancaman social engineering serta mengidentifikasi gap keamanan yang masih perlu diperbaiki.

Kajian Teori dan Literatur

Social Engineering

Berdasarkan Roblox Official Safety Statement pihak Roblox secara proaktif melaporkan konten yang berpotensi berisiko ke National Center for Missing & Exploited Children (NCMEC), pada tahun 2023 tercatat 13.316 laporan kasus grooming dan eksploitasi anak yang berasal dari platform digital[14]. Salah satu kasus yang terjadi di Indonesia Ketika seorang pria asal Balikpapan diduga melakukan grooming dan sextortion terhadap seorang remaja berusia 15 Tahun melalui platform Roblox. Pelaku membangun komunikasi melalui fitur interaksi dalam game, setelah korban mempercayai si pelaku kemudian melakukan manipulasi psikologis dan meminta materi pribadi yang kemudian digunakan sebagai alat pemerasan, Dampaknya adalah trauma psikologis pada korban[15].

Platform Roblox

Roblox sudah berisi dunia virtual dan game yang dibangun oleh ratusan ribu pengguna. Pengguna berinteraksi secara social atau bermain game Bersama, bertukar hampir 60 miliar pesan. Roblox memiliki delapan fitur utama metaverse: identitas, teman, imersif, anywhere, low friction, berbagai konten, ekonomi, dan keamanan yang menarik pengguna muda[1].

Statistic Roblox di Indonesia

Roblox masuk kategori 5 Besar game online yang paling sering dimainkan. Hasil dari Survei Penetrasi Internet yang dilakukan APJII persentase penggunaan internet game online khususnya di Indonesia mencapai 2,07% responden mengaku memainkan Roblox. Dengan durasi bermain game online terbanyak adalah 1-2 jam per hari (34,91%), dan 8,05% pengguna yang bermain lebih dari 4 jam per hari[8].

Gambar 1 1Survei APJII, 2025

Fitur Utama

fitur komunikasi dan interaksi yang menjadi daya tarik sekaligus faktor risiko keamanan, antara lain:

NO	Fitur	Keterangan
1	Chat Text	komunikasi dalam game (Chat Publik)
2	Voice Chat	komunikasi suara real-time
3	Party Chat	komunikasi sekelompok pengguna
4	Avatar dan identitas	mengekspresikan diri
5	Robux	Mata Uang Virtual
6	Roblox Studio	tools pengembangan game
7	Parental Control	fitur pengawasan orang tua
8	AI Sentinel	memantau & mendeteksi perilaku mencurigakan

Gambar 1 2 fitur chat, voice, party

Gambar 1 3 sebelum terdetect AI Sentinel

Gambar 1 4 setelah terdetect AI Sentinel
Sumber : Tangkapan Layar Peneliti dalam Roblox

NIST Cybersecurity Framework 2.0

NIST Cybersecurity Framework (CSF) 2.0 adalah kerangka kerja keamanan siber yang dikembangkan oleh National Institute of Standards and Technology (NIST), sebuah lembaga standar dan teknologi di bawah Departemen Perdagangan Amerika Serikat. Kerangka kerja ini dirancang untuk membantu organisasi dalam mengidentifikasi, mengelola, dan mengevaluasi risiko keamanan siber secara lebih efektif dan terstruktur [12].
NIST 2.0 terdiri dari *enam fungsi utama* yang membentuk siklus manajemen risiko siber yang komprehensif :

1. Govern (GV)
2. Identify (ID)
3. Protect (PR)
4. Detect (DE)
5. Responds (RS)
6. Recover (RC)

Fungsi Protect (PR) dalam NIST CSF 2.0:

1. PR.AA *(Identity Management, Authentication, and Access Control):* Manajemen identitas, autentikasi, dan kontrol akses
2. PR.AT *(Awareness and Training):* Pelatihan dan peningkatan kesadaran keamanan siber bagi seluruh personel dan pengguna platform
3. PR.DS *(Data Security):* Perlindungan data baik dalam kondisi diam (at rest), transit (in transit), maupun saat digunakan (in use)
4. PR.PS *(Platform Security)**:*** Keamanan platform perangkat lunak dan perangkat keras yang dikonfigurasi secara aman
5. PR.IR *(Infrastructure Resilience):* Ketahanan infrastruktur teknologi yang dirancang untuk tetap resilien dalam menghadapi gangguan.

e-ISSN: 2548-6861

Level Tingkat Kematangan dalam CMMI

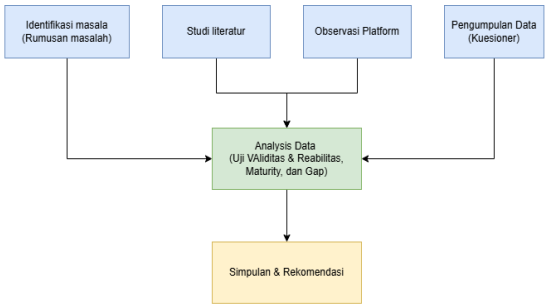
Dalam penelitian ini, model CMMI dipilih dalam penelitian ini karena menyediakan skala kematangan yang baku (Level 1-5) dan telah terbukti pada penelitian sebelumnya mampu mengkonversi hasil kuesioner menjadi nilai maturity level yang dapat dibandingkan dengan target ideal serta digunakan untuk *gap analysis.* Skema konversi skor rata-rata likert ke level CMMI pada penelitian ini diadaptasi dari penelitian Umar, Riadi, dan Handoyo[16], yang mengombinasikan framework COBIT 5 (sub-domain DSS05) dengan CMMI dan memperoleh nilai maturity sebesar 4,458 (Kategori Managed and Measurable), sehingga membuktikan validitas pendekatan ini untuk mengevaluasi tingkat kematangan keamanan sistem informasi. skor rata-rata Likert dan level CMMI sebagai berikut:

Table 1 Maturity Level CMMI

Skor Rata-Rata Likert	Level CMMI	Nama Level	Interpetasi
1,00 – 1,49	1	Initial	Tidak ada kontrol keamanan yang terstruktur
1,50 – 2,49	2	Managed	Kontrol dasar ada namun belum konsisten
2,50 – 3,49	3	Defined	Kontrol telah didefinisikan dan didokumentasikan
3,50 – 4,49	4	Quantitatively Managed	Kontrol diukur dan dipantau secara kuantitatif
4,50 – 5,00	5	Optimizing	Kontrol dioptimalkan secara berkelanjutan

II. METODE

Penelitian ini dilakukan berdasarkan hasil analisis permasalahan yang teridentifikasi dengan menggunakan pendekatan mixed-methods yang dimana data kualitatif dikumpulkan dan dianalisis terlebih dahulu kemudian dilengkapi dengan data kuantitatif yang dimana peneliti mengirimkan kuesioner melalui online kepada pengguna Roblox yang ada di Indonesia untuk memperdalam pemahaman tentang fenomena yang diteliti. Metode deskriptif diterapkan untuk memberikan gambaran mendalam mengenai fenomena keamanan yang diteliti, meliputi profil karakteristik responden, pengalaman Riwayat insiden keamanan, serta pemetaan kondisi aktual implementasi fungsi Protect. Kemudian, Peneliti akan melakukan evaluasi terhadap efektivitas fungsi Protect NIST CSF 2.0 dalam memitigasi ancaman social engineering pada platform Roblox.



Gambar 1 5Tahapan Penelitian

Metode ini menjadi pilihan yang paling efisien dan realistis, memungkinkan peneliti untuk mengumpulkan data dengan cepat dari responden yang tersedia dan bersedia berpartisipasi secara daring, sehingga target responden dapat terpenuhi dalam batas waktu yang ada.jumlah sampel yang diperlukan adalah 200 responden, sampel penelitian ini menggunakan *Purposive Sampling* karena membutuhkan responden yang memenuhi karakteristik spesifik, yakni *(1)Pengguna aktif Roblox Indonesia(2)memiliki pengalaman bermain lebih dari 1 bulan.* Untuk menentukan jumlah sampel yang akan digunakan dalam penelitian maka digunakan teori Roscoe(1975). Menurut Roscoe [17], ukuran sampel yang layak dalam penelitian adalah 30 sampai 500 responden, maka jumlah anggota sampel minimal 10 kali dari variable yang diteliti.

Berdasarkan point diatas maka penentuan jumlah sampel mengacu pada Roscoe (1975). Penelitian ini memiliki 1 variabel utama (Fungsi Protect NIST CSF 2.0) yang diukur melalui 5 sub-kategori dan 19 item indikator. Berdasarkan pendekatan konservatif menggunakan jumlah item (10x19=190), maupun pendekatan sub-kategori (10x5=50), jumlah 200 responden telah melampaui kedua batas minimum tersebut.[17]. Meskipun sudah memenuhi kelayakan ukuran sampel perlu ditegaskan bahwa Teknik purposive sampling dalam penelitian ini bertujuan untuk memahami pandangan, sikap, pengalaman pengguna, dan memperoleh gambaran persepsi pengguna terhadap implementasi fungsi Protect NIST CSF 2.0 pada platform Roblox, bukan untuk menghasilkan sampel proporsional secara statistik terhadap struktur demografis populasi pengguna Roblox di Indonesia secara keseluruhan. oleh karena itu, hasil yang diperoleh dari penelitian ini bersifat indikatif dan kontekstual terhadap karakteristik sampel penelitian, sehingga generalisasi temuan ke seluruh populasi pengguna Roblox Indonesia perlu dilakukan dengan hati-hati.

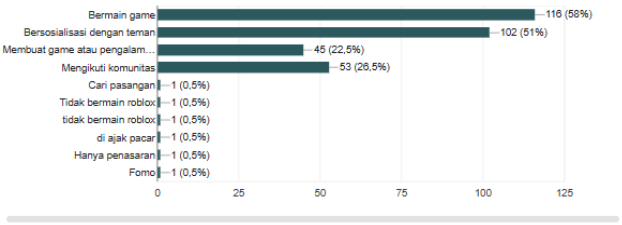
III. HASIL DAN PEMBAHASAN

Penelitian ini menyajikan hasil evaluasi fungsi Protect (PR) NIST CSF 2.0 terhadap ancaman social engineering pada platform Roblox berdasarkan data dari 200 responden pengguna Roblox Di Indonesia, untuk menjawab empat rumusan maslah yang telah ditetapkan, meliputi tingkat kematangan (Maturity Level), kesejangan (GAP) implementasi keamanan, sub-kategori dengan celah tersbesar, serta rekomendasi nya. Perlu ditegaskan bahwa hasil tingkat kematangan (Maturity Level) dalam penelitian ini merupakan representasi persepsi pengguna terhadap pengalaman Mereka menggunakan fitur-fitur keamanan pada platform Roblox, dan bukan merupakan hasil audit atau pengujian teknis langsung terhadap sistem, infrastruktur, maupun kebijakan internal Roblox Corporation. Sebagai platform milik korporasi asing dengan sistem yang bersifat tertutup (proprietary) dan tidak dapat diakses secara teknis oleh pihak luar, evaluasi fungsi protect NIST CSF 2.0 pada penelitian ini dilakukan melalui sudut pandang pengguna (user-perceived security). Kondisi ini menjadi dasar perlunya evaluasi sistematis menggunakan fungsi Protect (PR) NIST CSF 2.0 yang mencakup *lima sub-kategori: PR.AA, PR.AT, PR.DS, PR.PS, dan PR.IR*. Hasil evaluasi diukur menggunakan skala Likert (1–5) dengan target skor 4,00 dan dikonversi ke Maturity Level berbasis model CMMI, sementara analisis GAP dihitung sebagai selisih antara skor aktual dengan skor target. Responden mendominasi perempuan sejumlah (53,5%) dengan 107 orang, sementara Laki-laki berjumlah 93 orang (46,5%). Mayoritas reponden berada pada rentang usia >20 Tahun (64%) dengan 128 orang, mencerminkan populasi yang didominasikan oleh orang dewasa. Berdasarkan lama penggunaannya kurang dari 1 Tahun (72,5%), 1-3 tahun (20,5%), dan lebih dari 3 Tahun (7%). Sebelum data utama dikumpulkan, instrumen penelitian telah diuji untuk memastikan bahwa mereka konsisten dan akurat. Hasil ini akan dijelaskan secara rinci, memberikan dasar validasi alat yang digunakan untuk pengumpulan data utama,

Pada tabel dibawah mengungkapkan bahwa beberapa responden pernah mengalami *setidaknya satu jenis insiden keamanan atau lebih dari satu di platform Roblox*. Ini membuat total frekuensi yang ada menjadi lebih dari 200 yaitu 231 frekuensi.

Table 2 Karakreristik Responden

Karakteristik	Kategori	Frekuensi	Persentase
Jenis Kelamin	Laki-laki	93	46,5%
	Perempuan	107	53,5%
Total		200	100%
Usia	<13 Tahun	2	1%
	13-15 Tahun	16	8%
	16-20 Tahun	54	27%
	>20 Tahun	128	64%
Total		200	100%
Lama Penggunaan	< 1 Tahun	145	72,5%
	1-3 Tahun	41	20,5%
	< 3 Tahun	14	7%
Total		200	100%
Frekuensi Bermain	Jarang	50	25,4%
	kadang - kadang	79	40,1%
	sering	39	19,8%
	setiap hari	29	14,7%
	Tidak Menjawab	3	-
Total		200	100%
Jenis Insiden	Scam Robux	25	12,5%
	Phishing/Link Palsu	28	14%
	Grooming	10	5%
	Pembajakan Akun	27	13,5%
	Tidak pernah	137	68,5%
	Lainnya	4	2%
Total		200	100%



Gambar 1 6 Karakteristik Berdasarkan Alasan Bermain

Tabel 3 dan gambar 1.7 menampilkan hasil pengujian yang menunjukkan bahwa instrumen yang digunakan valid dan reliable. Instrument penelitian telah melalui uji validitas dan reliabilitas, ujia validitas dilakukan untuk memastikan bahwa setiap item pertanyaan dalam kuesioner benar-benar mengukur konsep atau variable yang dimaksudkan. Dalam hasil uji ini, yang melibatkan 200 responden, kriteria validitas ditetapkan berdasarkan perbandingan nilai r-hitung dengan nilai r-tabel. Dengan signifikan 5%. Nilai r-tabel yang digunakan adalah 0,138.

e-ISSN: 2548-6861

Rumus : *df = n – 2*

df = 200 -2

df = 198

α = 5% (0,05)

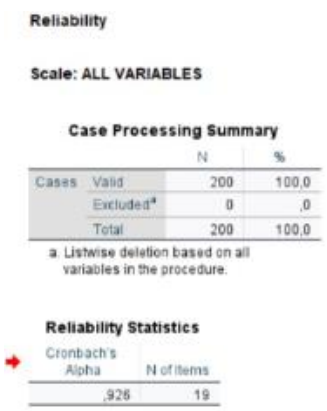
Nilai *r table* didapat melalui Tabel Pearson Product Moment
Hasilnya **r tabel = 0,138**
Nilai ini menjadi batas apakah item valid atau tidak

Jika Nilai $R_{Hitung} \geq R_{Tabel}$ = Valid
Jika Nilai $R_{Hitung} \leq R_{Tabel}$ = TidakValid

Table 3 Hasil Validitas

No	Sub-Kategori	Jumlah Item	r Hitung (min)	Keterangan
1	PR.AA (Identify & Acces Control)	4	0,614	Valid
2	PR.AT (Awareness & Training)	4	0,611	Valid
3	PR.DS (Data Security)	4	0,581	Valid
4	PR.PS (Platform Security)	4	0,660	Valid
5	PR.IR (Infrastructure Resilience)	3	0,616	Valid
	Total	**19**	**> 0,138**	**Valid**

Sumber: diolah oleh peneliti,2026



Reliability

Scale: ALL VARIABLES

Case Processing Summary

		N	%
Cases	Valid	200	100,0
	Excluded[a]	0	,0
	Total	200	100,0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
,926	19

Gambar 1 7 Hasil Uji Reliable
Sumber : diolah oleh peneliti,2026

Berdasarkan hasil uji reabilitas menggunakan metode *Cronbach's Alpha* pada aplikasi SPSS, diperoleh nilai *sebesar 0,926 dengan jumlah 19 item*. Hasil pengolahan ini menjunjukkan bahwa seluruh *200 responden dinyatakan valid*. Nilai Cronbach's Alpha *sebesar 0,926 berada pada rentang 0,81-1,00 yang dikategorikan Sangat Reliabel*[18] Hal ini menunjukkan bahwa kuesioner yang digunakan konsisten dalam mengukur konstruk yang di inginkan dan dapat dipercaya sebagai alat pengumpul data dalam penelitian ini. Hasil analisis deskriptif dari SPSS terlihat pada table 3 dan gambar 1.7 menunjukkan bahwa data penelitian memiliki karakteristik yang sesuai untuk analisis lebih lanjut. Penelitian ini menggunakan skala penilaian dari satu, yang berarti 'sangat tidak setuju', hingga lima, yang berarti 'sangat setuju'. Angka rata-rata, yang merupakan nilai rata-rata dari semua jawaban responden untuk setiap pertanyaan, memberikan gambaran umum tentang arah atau kecendrungan jawaban.

Analisis deskriptif dilakukan untuk menggambarkan nilai rata-rata(mean) skor persepsi responden terhadap implementasi setiap sub-kategori fungsi Protect NIST CSF 2.0 pada platform Roblox. Penilaian menggunakan skala likert 1-5, dimana 1 berarti sangat tidak setuju dan 5 berarti sangat setuju. Skor rata-rata yang diperoleh selanjutnya digunakan sebagai dasar penentuan Maturity level dan gap analysis:

Mean :

$$\bar{x} = \frac{\sum(f \times x)}{N}$$

$$\bar{x} = \frac{\sum(3 \times 1) + (8 \times 2) + (50 \times 3) + (92 \times 4) + (47 \times 5)}{200}$$

$$\bar{x} = \frac{3 + 16 + 150 + 368 + 235}{200}$$

$$\bar{x} = 3,86$$

Berikut Hasil Analisis deskriptif setiap Kategori:

Rata – rata skor sub-kategori PR.AA adalah 3,76 dari target level 4,00. Dari ke empat indikator pembatasan akses dengan pengguna dikenal (PR.AA2) memperoleh skor terendah (3,69), yang mengindikasikan masih adanya celah dalam pembatasan interaksi antara pengguna yang belum dikenal. Salah satu jalur utama social engineering berbasis impersonation. Sementara verifikasi login (PR.AA1) memperoleh skor tertinggi (3,86), mencerminkan bahwa mekanisme verifikasi dasar dinilai cukup efektif oleh pengguna. Secara keseluruhan, sub-kategori PR.AA dipersepsikan berada pada Maturity Level 4 (Quantitatively Managed) berdasarkan skala CMMI menurut persepsi responden, dengan kesenjangan rata-rata sebesar 0,24 terhadap target maturity level yang ditetapkan.

Table 4 indikator PR.AA

Kode	indikator	mean	target	Gap
PR.AA 1	Verifikasi Login	3.86	4	0.14
PR.AA 2	Membatasi akses dengan pengguna tak dikenal	3.69	4	0.31
PR.AA 3	fitur pembatasan akun/ parental control	3.77	4	0.23
PR.AA 4	membatasi koneksi pertemanan	3.74	4	0.26
Rata-Rata	**Keseluruhan PR.AA**	**3.76**	**4**	**0.24**

Sumber: diolah oleh peneliti,2026

Seluruh sub-kategori PR.AT memperoleh rata-rata skor 3,81 yang merupakan salah satu skor tertinggi diantara semua sub-Kategori. Indikator panduan keamanan dalam platform (PR.AT3) mendapatkan skor mendekati target (3,99), yang menunjukkan bahwa panduan keamanan yang tersedia pada platform sudah sangat dirasakan manfaatnya oleh pengguna. Sebaiknya, indikator edukasi keamanan siber untuk pengguna (PR.AT1) mendapatkan skor terendah (3,61) dengan Gap 0,39, mengindikasikan bahwa edukasi proaktif terkait ancaman social engineering masih perlu ditingkatkan. Secara keseluruhan, sub-kategori PR.AT dipersepsikan berada pada Maturity Level 4 (Quantitatively Managed) menurut persepsi responden dengan Gap rata-rata 0,19.

Table 5 indikator PR.AT

Kode	indikator	mean	target	Gap
PR.AT1	edukasi keamanan siber ke pengguna	3.61	4	0.39
PR.AT2	notifikasi peringatan ancaman/phishing	3.93	4	0.07
PR.AT3	panduan keamanan dalam platform	3.99	4	0.01
PR.AT4	pelaporan insiden oleh pengguna	3.72	4	0.28
Rata-Rata	**Keseluruhan PR.AT**	**3.81**	**4**	**0.19**

Sumber: diolah oleh peneliti,2026

Rata – rata skor PR.DS adalah 3,84 yang tertinggi kedua diantara seluruh sub-kategori dengan nilai Gap rata-rata 0,16 yang merupakan gap terkecil. Hal ini mengindikasikan bahwa pengguna merasakan adanya kontrol yang relatif kuat terkait bagaimana data mereka dikelola dan dibagikan. Indikator enkripsi data transaksi Robux (PR.DS3) dan kontrol privasi akun (PR.DS4) memperoleh skor yang sama (3,89), mencerminkan kepercayaan pengguna terhadap keamanan transaksi keuangan dan pengaturan privasi pada platform. Sub-kategori ini dipersepsikan berada pada Maturity Level 4 (Quantitatively Managed) berdasarkan skala CMMI menurut persepsi responden.

Table 6 indikator PR.DS

Kode	indikator	mean	target	Gap
PR.DS 1	perlindungan data pribadi	3.76	4	0.24
PR.DS 2	pembatasan data dengan pihak ke-3	3.85	4	0.15
PR.DS 3	enkripsi data transaksi Robux	3.89	4	0.11
PR.DS 4	kontrol privasi akun	3.89	4	0.11
Rata-Rata	**Keseluruhan PR.DS**	**3.84**	**4**	**0.16**

Sumber: diolah oleh peneliti,2026

Sub-kategori PR.PS memperoleh rata-rata skor 3,77 dengan gap sebesar 0,23. Indikator yang memiliki skor paling rendah adalah perlindungan terhadap link eksternal (PR.PS-03), yang mendapatkan skor terendah (3,71) dengan gap (0,29). Temuan ini sangat relevan mengingat phishing melalui link palsu merupakan modus social engineering yang paling banyak dilaporkan oleh responden. Sementara itu, AI sentinel untuk deteksi perilaku mencurigakan (PR.PS-01) mendapat skor tertinggi (3,82) pada sub-kategori ini, menunjukkan bahwa fitur AI Sentinel sudah cukup diakui keberadaannya. Sub-kategori ini dipersepsikan berada pada Maturity Level 4 (*Quantitatively Managed)* berdasarkan skala CMMI menurut persepsi responden.

e-ISSN: 2548-6861

Table 7 indikator PR.PS

Kode	indikator	mean	target	Gap
PR.PS1	AI sentinel untuk deteksi perilaku mencurigakan	3.82	4	0.18
PR.PS2	Fitur Report responsif	3.77	4	0.23
PR.PS3	perlindungan terhadap link eksternal	3.71	4	0.29
PR.PS4	pembaruan keamanan secara berkala	3.80	4	0.20
Rata-Rata	**Keseluruhan PR.PS**	**3.77**	**4**	**0.23**

Sumber: diolah oleh peneliti,2026

Sub-kategori PR.IR memperoleh rata-rata skor 3,81 dengan Gap 0,19. Notifikasi jika adanya aktivitas mencurigakan (PR.IR2) mendapatkan skor 3,92 dengan gap terendah sebesar 0,08 menunjukkan bahwa sistem pemberitahuan aktivitas mencurigakan pada platform Roblox dinilai sudah sangat efektif oleh pengguna. Sementara itu, sistem meminimalisir insiden (PR.IR3) mendapatkan skor terendah (3,75), mengindikasikan masih adanya ruang peningkatan dalam hal prosedur respons dan pemulihan pasca insiden dari perspektif pengguna. Sub-kategori ini dipersepsikan berada pada Maturity Level 4 *Quantitatively Managed* berdasarkan skala CMMI menurut persepsi responden.

.

Table 8 indikator PR.IR

Kode	indikator	mean	target	Gap
PR.IR1	pemulihan akun	3.77	4	0.23
PR.IR2	notifikasi jika ada aktivitas mencurigakan	3.92	4	0.08
PR.IR3	sistem minimimalisir insiden	3.75	4	0.25
Rata-Rata	**Keseluruhan PR.AA**	**3.81**	**4**	**0.19**

Sumber: diolah oleh peneliti,2026

Hasil Pengukuran Maturity Level

Pengukuran Maturity level dilakukan untuk menentukan posisi kematangan implementasi fungsi Protect NIST CSF 2.0 pada Platform Roblox berdasarkan persepsi pengguna. Skala Maturity yang digunakan mengadaptasi CMMI (Capability Maturity Model Integration) yang terdiri dari 5 level.

Konversi skor rata-rata Likert (skala 1-5) ke dalam skala Maturity CMMI dilakukan secara langsung, dimana skor 3,50-4,49 dikategorikan pada Maturity Level 4 Quantitatively Managed . maturity Level 4 yang diperoleh tidak dapat dimaknai sebagai klaim bahwa Roblox "sudah aman" secara teknis pada level 4, melainkan sebagai indikasi bahwa kontrol-kontrol keamanan yang dapat diamati dan dirasakan oleh pengguna (seperti verifikasi login, parental vontrol, AI Sentinel, enkripsi transaksi, dan fitur pelaporan) di persepsikan telah berjalan secara konsisten dan terukut dari sudut padang pengguna atau 200 responden.

Table 9Maturity Level

Sub-Kategori	Nama Sub-Kategori	Rata-Rata Skor	Target	Gap	Maturnity Level CMMI
PR.AA	Identify Management & Acces Control	3.76	4	0.24	Level 4 - Quantitatively Managed
PR.AT	Awareness and Training	3.81	4	0.19	Level 4 - Quantitatively Managed
PR.DS	Data Security	3.84	4	0.16	Level 4 - Quantitatively Managed
PR.PS	Platform Security	3.77	4	0.23	Level 4 - Quantitatively Managed
PR.IR	Infrastructure Resilience	3.81	4	0.19	Level 4 - Quantitatively Managed
Rata-Rata	***Keseluruhan Fungsi Protect***	***3.80***	***4***	***0.20***	***Level 4 - Quantitatively Managed***

Sumber: diolah oleh peneliti,2026

Maturity Level pada tabel diatas merupakan hasil interpretasi berdasarkan persepsi 200 responden pengguna aktif Roblox terhadap indikator keamanan yang dievaluasi, bukan merupakan hasil audit teknis langsung terhadap system Roblox

Berdasarkan tabel rekapitulasi diatas, seluruh sub kategori fungsi Protect NIST CSF 2.0 pada platform Roblox berada pada Maturity Level 4 (Quantitatively Managed) berdasarkan model CMMI menurut persepsi 200 responden. Hal ini menunjukkan bahwa berdasarkan penilaian pengguna, mekanisme perlindungan yang dievaluasi telah dinilai memiliki tingkat pengelolaan yang terukur dan dapat dipantau menggunakan indikator keamanan yang telah ditentukan. Namun, masih terdapat gap rata-rata sebesar 0,20 terhadap target maturity level yang ditetapkan, yang menunjukkan bahwa masih terdapat peluang peningkatan untuk mencapai tingkat kematangan yang lebih tinggi, yaitu Maturity Level 5 (Optimizing).

Sub-Kategori dengan gap terbesar adalah PR.AA (Identify Management & Acces Control) dengan gap 0,24, khususnya pada indikator pembatasan akses dengan pengguna tak dikenal. Hal ini menunjukkan bahwa berdasarkan persepsi responden, aspek pengelolaan identitas dan pembatasan interaksi pengguna masih emmiliki ruang peningkatan dalam mitigasi risiko social engineering. Sementara itu, sub-kategori dengan gap terkecil adalah PR.DS (Data Security) dengan nilai gap 0,16 yang menunjukkan bahwa aspek perlindungan data dinilai relative lebih baik oleh responden dibandingkan sub-kategori lainnya.

Pembahasan Temuan

Berdasarkan persepsi responden hasil analisis, indikator dengan gap terbesar dari seluruh sub-kategori adalah edukasi keamanan siber untuk pengguna (PR.AT1) dengan gap 0,39 diikuti oleh pembatasan akses dengan pengguna tak dikenal (PR.AA2) dengan gap 0,31, dan perlindungan terhadap link eksternal (PR.PS3) dengan gap 0,29. Ketiga indikator dengan gap terbesar ini secara langsung berkaitan dengan mekanisme yang paling sering dieksploitasi dalam serangan social engineering pada platform Roblox, yaitu manipulasi psikologis melalui interaksi sosial, pembangunan kepercayaan dengan orang asing, dan pengiriman link phishing. Temuan ini mengonfirmasi bahwa meskipun Roblox telah menerapkan berbagai fitur control keamanan, kesadaran pengguna dan perlindungan terhadap tautan berbahaya masih menjadi titik lemah utama.

Implikasi terhadap Ancaman Social Engineering

Hasil evaluasi menunjukkan bahwa dari perspektif pengguna, fungsi Protect NIST CSF 2.0 pada platform Roblox telah di implementasikan pada tingkat yang memadai (Level 4 CMMI). Namun, temuan insiden keamanan yang masih terjadi seperti phishing (14%), pembajakan akun (13,5%), dan scam Robux (12%) mengindikasikan bahwa gap yang ada, meskipun relatif kecil secara kuantitatif, tetap berdampak signifikan terhadap keamanan pengguna actual dilapangan. Hal ini menunjukkan adanya kesenjangan antara persepsi pengguna mengenal keamanan platform dengan realitas insiden yang terjadi. Fenomena ini dapat dijelaskan oleh dua faktor utama: pertama, banyak pengguna belum sepenuhnya memahami atau menggunakan fitur keamanan yang tersedia (low Awareness); kedua, pelaku social engineering terus beradaptasi dengan kontrol yang ada dan mencari celah baru yang belum tertutup oleh system.

REKOMENDASI

Berdasarkan hasil evaluasi, data yang mendasari rekomendasi ini diperoleh melalui kuesioner yang di isi oleh 200 responden. Berikut beberapa rekomendasi yang disusun berdasarkan temuan dari sampel penelitian :

1. ***Pada Kategori PR.AA (Identity Management & Access Control)*** menyarankan untuk Mewajibkan 2FA untuk akun bertransaksi Robux, menerapkan *behavioral analytics* untuk deteksi login real-time, serta memberlakukan *cooldown period* pada pesan privat..
2. ***PR.AT (Awareness & Training):*** Menyarankan menutup gap terbesar dengan mengembangkan edukasi siber melalui *mini-game* interaktif, memberikan *contextual security tips* otomatis pada momen kritis (seperti tawaran Robux gratis), dan memperkaya kategori fitur report abuse insiden khusus *social engineering* agar pengguna sekaligus mendapat edukasi tentang bentuk ancaman yang ada.
3. ***PR.DS (Data Security):*** Menyarankan menyusun ringkasan kebijakan privasi dalam bahasa yang ramah anak/multibahasa serta mengaktifkan fitur persetujuan eksplisit yang memberikan control penuh pengguna sebelum data mereka dibagikan ke pihak ke-3.
4. ***PR.PS (Platform Security):*** Menyarankan mengekspansi AI Sentinel untuk memantau pola perilaku mencurigakan lintas sesi serta memblokir tautan eksternal secara otomatis pada fitur voice chat dan party chat, didukung

e-ISSN: 2548-6861

dengan pembaruan system keamanan platform secara berkala.

5. ***PR.IR (Infrastructure Resilience):*** Roblox Corporation disarankan untuk menyempurnakan proses pemulihan akun & memperkuat sistem notifikasi otomatis saat terdeteksi aktivitas mencurigakan guna mencegah dampak pembajakan akun

IV. KESIMPULAN

Peneliti memberikan hasil penelitian Fungsi Protect (PR) NIST Cybersecurity Framework 2.0 terhadap social engineering pada platform Roblox yang dilakukan terhadap 200 responden pengguna Indonesia, dapat disimpulkan bahwa seluruh sub-kategori fungsi Protect NIST CSF 2.0 pada platform Roblox dipersepsikan oleh pengguna berada pada *Maturity Level 4 (Quantitatively Managed).* berdasarkan model CMMI, dengan skor *rata-rata keseluruhan sebesar 3,80* dari level target 4,00. Hal ini menunjukkan bahwa dari sudut pandang pengguna, kontrol keamanan Roblox telah dirasakan sudah cukup terukur dan konsisten. Namun belum mencapai level Optimal (Level 5-Optimizing). Perlu ditegaskan bahwa hasil ini merupakan persepsi pengguna dan bukan merupakan hasil audit teknis resmi terhadap sistem keamanan Roblox sebagai organisasi, sehingga tidak dapat dijadikan dasar untuk menyatakan bahwa Roblox 'sudah aman' secara teknis pada level tersebut.

Kesenjangan (GAP) *rata-rata antara implementasi aktual fungsi Protect pada Roblox dengan standar NIST CSF 2.0 adalah sebesar 0,20*. Sub-kategori dengan gap terbesar adalah *PR.AA (Identity Management & Acces Control) dengan gap 0,24*, sedangkan sub-kategori dengan gap terkecil adalah *PR.DS (Data Security) dengan gap 0,16*. Sub-kategori yang memiliki tingkat kematangan implementasi terendah dan menjadi celah utama serangan social engineering adalah PR.PS (Platform Security) dan PR.AA (Identity Management & Acces Control), khususnya pada indikator *perlindungan terhadap link eksternal (gap 0,29)* dan pembatasan akses dengan pengguna tak dikenal (gap 0,31). Kedua aspek ini secara langsung di eksploitasi oleh pelaku social engineering melalui Teknik phishing link berbahaya dan impersonation. Indikator dengan gap terbesar secara keseluruhan adalah *edukasi keamanan siber untuk pengguna (PR.AT1) dengan gap 0.39*, yang menunjukkan bahwa edukasi proaktif tentang ancaman social engineering kepada pengguna masih Menjadi kelemahan terbesar dalam ekosistem keamanan Roblox saat ini. *Terdapat 137 responden (68,5%)* menyatakan tidak pernah mengalami insiden keamanan di platform Roblox. Namun, terdapat jumlah responden yang pernah mengalami berbagai bentuk insiden, diantaranya *phishing/link palsu sebanyak 28 responden (14%), pembajakan akun 27 responden (13,5%), Scam Robux 25 Responden (12,5%), serta grooming 10 responden (5%).* Temuan ini menunjukkan bahwa ancaman social engineering pada platform Roblox benar-benar terjadi pada sebagian pengguna, sehingga gap keamanan teridentifikasi dalam penelitian ini bukan hanya bersifat teoritis, tetapi memiliki dampak nyata terhadap keamanan pengguna.

KETERBATASAN PENELITIAN

Penelitian ini memiliki beberapa keterbatasan yang perlu diakui dan dapat dijadikan dasar untuk penelitian lanjutan antara lain: Evaluasi hanya dilakukan dari perspektif pengguna melalui kuesioner, sehingga tidak mencerminkan kondisi implementasi teknis aktual dari sisi server dan infrastruktur internal Roblox Corporation, Penelitian ini tidak melakukan penetration testing atau simulasi serangan social engineering secara langsung, sehingga gap yang teridentifikasi berdasarkan persepsi pengguna mungkin berbeda dengan gap aktual dari perspektif keamanan teknis, Data insiden keamanan yang digunakan bersumber dari laporan yang tersedia secara publik, sehingga mungkin tidak mencerminkan keseluruhan insiden yang terjadi mengingat banyak insiden tidak dilaporkan secara formal. Mayoritas responden dalam penelitian berusia diatas 20 Tahun (64%) dan baru menggunakan Roblox kurang dari 1 Tahun (72,5%) sementara kelompok anak-anak(target utama ancaman social engineering di Roblox) hanya terwakili dalam proporsi kecil (1% untuk usia <13 tahun) hal ini disebabkan keterbatasan akses, sehingga sampel penelitian belum cukup representative untuk menggambarkan persepsi kelompok pengguna anak-anak dan remaja awa (dibawah 16 tahun) yang merupakan kelompok usia dengan tingkat eksposur tertinggi terhadap ancaman social engineering.

SARAN UNTUK PENELITIAN SELANJUTNYA

Berdasarkan keterbatasan penelitian ini, beberapa saran untuk penelitian selanjutnya adalah Melakukan evaluasi komprehensif yang mencakup seluruh enam fungsi NIST CSF 2.0 (Govern, Identify, Protect, Detect, Respond, dan Recover. Memperluas objek penelitian ke platform gaming atau metaverse lain seperti Minecraft, Fortnite, atau platform metaverse lainnya untuk menghasilkan perbandingan lintas platform yang lebih komprehensif. Melibatkan responden dari kelompok usia di bawah 13 tahun (dengan persetujuan orang tua) sebagai responden utama, dan Melakukan monitoring untuk memantau perkembangan maturity level keamanan platform secara periodik dari waktu ke waktu. Dengan mempertimbangkan keterbatasan metode purposive sampling dan jumlah responden yang digunakan, diperlukan penelitian lanjutan dengan cakupan sampel yang lebih luas dan metode probabilistik untuk meghasilkan kesimpulan yang dapat digeneralisasi.

UCAPAN TERIMA KASIH

Terimakasih kepada semua pihak yang telah memberikan dukungan dan kontribusi dalam menyelesaikan penelitian ini. Terimakasih kepada dosen pembimbing atas bimbingan, arahan dan waktunya dalam membantu menyelesaikan penelitian ini. Terimakasih juga kepada Orang Tua serta keluarga besar saya yang selalu memberi dukungan dan semangat kepada saya, serta Reponden pengguna Roblox yang telah membantu (khususnya VornixStudio, Ichel, Ezi, dan Manis partner Roblox) dan menjadi tempat bertukar pikiran selama penelitian sehingga Jurnal ini dapat diselesaikan dengan baik.

DAFTAR PUSTAKA.

[1] J. Han, G. Liu, and Y. Gao, "Learners in the Metaverse: A Systematic Review on the Use of Roblox in Learning," Mar. 01, 2023, *MDPI*. doi: 10.3390/educsci13030296.

[2] I. Sopiandi and D. Susanti, "Menganalisis Informasi Metaverse Pada Game Online Roblox Secara Garis Besar," *J. PETISI*, vol. 3, no. 1, 2022.

[3] R. Long, "ROBLOX AND EFFECT ON EDUCATION", doi: 10.13140/RG.2.2.33057.97129.

[4] P. Gabriel Kabanda, C. Tendeukai Chipfumbu, T. Chingoriwo, P. Gabriel Kabanda α, C. Tendeukai Chipfumbu σ, and T. Chingoriwo ρ, "A Cyber Security Model for a Roblox-based Metaverse Architecture Framework ACyberSecurityModelforaRoblox-basedMetaverseArchitectureFramework A Cyber Security Model for a Roblox-based Metaverse Architecture Framework," 2023.

[5] A. Serio, "Protecting young players in the Metaverse," 2024.

[6] N. Ruby Sacharissa and Y. Alifatus Shalehah, "PARASITISME MEDIA SOSIAL DALAM KONTEKS CHILD CYBER GROOMING PADA JEJARING SOSIAL GAMES HAGO," 2023.

[7] J. Han, G. Liu, and Y. Gao, "Learners in the Metaverse: A Systematic Review on the Use of Roblox in Learning," *Educ. Sci.*, vol. 13, no. 3, 2023, doi: 10.3390/educsci13030296.

[8] APJII, "No Title," SURVEI PENETRASI INTERNET DAN PERILAKU PENGGUNAAN INTERNET.

[9] tekno.kompas.com, "No Title," Roblox Disorot, Berapa Jumlah Pemainnya di Indonesia? [Online]. Available: https://tekno.kompas.com/read/2025/08/12/19140027/roblox-disorot-berapa-jumlah-pemainnya-di-indonesia

[10] P. Control, "No Title," linking to your child's account and setting up parental controls. [Online]. Available: https://about.roblox.com/parental-controls

[11] H. Ghozie Afiansyah, N. Annisa, and K. Febriyani, "Penyusunan Kebijakan Pengamanan dan Pengelolaan Infrastruktur Operasi Keamanan Siber Menggunakan NIST CSF 2.0 dan ISO/IEC 27001:2022."

[12] "The NIST Cybersecurity Framework (CSF) 2.0," Feb. 2024. doi: 10.6028/NIST.CSWP.29.

[13] Crossmark, "Public Draft: The NIST Cybersecurity Framework 2.0 National Institute of Standards and Technology Note to Reviewers," 2023.

[14] about.roblox.com, "No Title," Driving Civility and Safety for All Users. [Online]. Available: https://about.roblox.com/newsroom/2024/07/driving-civility-and-safety-for-all-users?utm_source=chatgpt.com

[15] tribratanews.polri.go.id, "No Title," Peras ABG di Swedia Lewat Gim Roblox, Polisi Berhasil Amankan Predator Anak Asal Balikpapan. [Online]. Available: https://tribratanews.polri.go.id/blog/keamanan-6/peras-abg-di-swedia-lewat-gim-roblox-polisi-berhasil-amankan-predator-anak-asal-balikpapan-90121

[16] R. Umar, I. Riadi, and E. Handoyo, "Analisis Keamanan Sistem Informasi Berdasarkan Framework COBIT 5 Menggunakan Capability Maturity Model Integration (CMMI)," *J. Sist. Inf. Bisnis*, vol. 9, no. 1, p. 47, 2019, doi: 10.21456/vol9iss1pp47-54.

[17] Sugiyono, "Sampel Jurnal," *Serv. Manag.*, pp. 33–42, 2015.

[18] A. Fransiska and Y. Yuliana, "Pengaruh Periklanan Terhadap Minat Beli Kamar Di Imelda Hotel Waterpark Convention Padang," *J. Pendidik. Dan Kel.*, vol. 11, no. 02, p. 156, 2020, doi: 10.24036/jpk/vol11-iss02/634.

.