AT-TAKLIM : Jurnal Pendidikan Multidisiplin E-ISSN : 3062-9489
https://journal.hasbaedukasi.co.id/index.php/at-taklim
Halaman: 417 - 432

ANALISIS MANAJEMEN RISIKO SISTEM KEPEGAWAIAN (SIMPEG) DI RADIO REPUBLIK INDONESIA DENGAN METODE NIST SP 800-30

Devi Agustin Utari[1], Anik Hanifatul Azizah[2]
Universitas Esa Unggul, Jakarta, Indonesia
Email: deviutari19@gmail.com

Keywords

SIMPEG; Risk Assessment; NIST SP 800-30; NIST SP 800-53 Rev 5

Abstract

RRI uses the Information System of Human Resources (SIMPEG), which is used by the RRI Public Broadcasting Institution (LPP RRI), to access personnel data. During the operation of SIMPEG RRI, the system has never been subjected to risk management and there are several problems such as power outages, full backup server storage, and server down because the hardware used is outdated so its use is less than optimal which causes SIMPEG RRI to be inaccessible. Therefore, this study will discuss the system's risk assessment to avoid other risks that have a negative impact on SIMPEG RRI. This study uses the NIST SP 800-30 method for risk assessment and the NIST SP 800-53 Rev 5 method for control recommendations. In conducting this risk assessment, the author collects data and information using qualitative methods, which is assisted by a questionnaire as a tool to support interviews and observations. After the risk assessment analysis was carried out, it was found that there were 10 Moderate risks and 6 Low risks. Control recommendations are arranged based on risk levels of 18 control groups with the number of moderate risk control recommendations being 12 control groups and low risk recommendations being 6 control groups.

SIMPEG; Penilaian Risiko; NIST SP 800-30; NIST SP 800-53 Rev 5

RRI menggunakan Sistem Informasi Manajemen Kepegawaian (SIMPEG) yang digunakan oleh Lembaga Penyiaran Publik RRI (LPP RRI) untuk mengakses data kepegawaian. Selama SIMPEG RRI beroperasi, sistem belum pernah dilakukan manajemen risiko dan terdapat beberapa permasalahan seperti pemadaman listrik, storage server backup yang penuh, dan server down karena hardware yang digunakan sudah lampau sehingga penggunaanya menjadi kurang optimal yang menyebabkan SIMPEG RRI tidak dapat diakses. Oleh karena itu, penelitian ini akan membahas terkait penilaian risiko pada sistem untuk menghindari adanya risiko lainnya yang berdampak buruk pada SIMPEG RRI. Penelitian ini menggunakan metode NIST SP 800-30 untuk penilaian risiko dan metode NIST SP 800-53 Rev 5 untuk rekomendasi kontrol. Dalam melakukan penilaian risiko ini, penulis mengumpulkan data dan informasi menggunakan metode kualitatif dan dibantu dengan kuisioner sebagai alat untuk pendukung wawancara. Setelah dilakukan analisis penilaian risiko diketahui bahwa terdapat risiko dengan tingkatan Moderate sebanyak 10 risiko dan risiko dengan tingkatan Low sebanyak 6 risiko. Rekomendasi kontrol yang

disusun berdasarkan tingkatan risiko sebanyak 18 kelompok kontrol dengan jumlah rekomendasi kontrol risiko tingkatan Moderate sebanyak 12 kelompok kontrol dan risiko tingkatan Low sebanyak 6 kelompok kontrol.

1. PENDAHULUAN

Sistem informasi memiliki manfaat yang penting pada organisasi dalam menyediakan informasi bagi pihak internal maupun eksternal. Saat ini, informasi bukan hanya digunakan untuk meningkatkan efisiensi, tetapi juga untuk menilai dan meningkatkan kualitas SDM yang dimiliki organisasi. Dengan adanya pemanfaatan teknologi informasi membantu dalam peningkatan efisiensi organisasi untuk mengelola informasi dilihat dari aspek kecepatan dan ketepatan waktu dalam memproses data, serta keakuratan informasi yang dihasilkan.

Risiko merupakan akibat dari sebuah proses yang sedang berlangsung atau yang akan datang dimana hal tersebut dapat menimbulkan suatu kerugian (Syahrial Sidik & Wahyuari, 2023). Risiko yang terjadi pada sistem akan sangat mempengaruhi setiap aktivitas yang sedang berjalan didalamnya sehingga akan memberikan kerugian secara material maupun konsekuensi yang signifikan terhadap organisasi. Oleh karena itu, untuk mengurangi risiko-risiko yang kemungkinan terjadi pada sistem perlu dilakukan manajemen risiko.

Manajemen risiko adalah kegiatan yang bertujuan mencapai keseimbangan antara efisiensi serta peluang untuk mendapat keuntungan dan mengurangi kerentanan dan kerugian (Budiono et al., 2021). Manajemen risiko juga dapat dikatakan sebagai proses atau kegiatan mengidentifikasi risiko, melakukan analisis risiko dan mengendalikan risiko yang kemungkian terjadi pada suatu aktivitas atau kegiatan (Syahrial Sidik & Wahyuari, 2023). Manajemen risiko merupakan proses menyeimbangkan biaya operasional dari tindakan perlindungan untuk mencapai keuntungan dalam kemampuan misi dengan melindungi sistem dan data yang mendukung organisasi (Gary Stoneburner, Alice Goguen, 2002). Dengan manajemen risiko ini, memberikan upaya kepada organisasi untuk mengelola dan mengontrol berbagai risiko pada sistem yang timbul agar tidak terpengaruh oleh dampak negatif yang timbul dari risiko tersebut.

Dalam penerapan manajemen risiko terdapat beberapa metode yang digunakan seperti NIST SP 800-30, ISO 27001 dan Octave. Metode NIST SP 800-30 didasari pada analisis keamanan untuk mengidentifikasi, menilai dan mengelola risiko pada sistem teknologi informasi yang mencakup perihal ancaman hingga penilaian dan identifikasi sumber penilaian (Juliasari & Zulfikar, 2022). ISO 27001 merupakan salah satu standar Sistem Manajemen Keamanan Informasi dengan menerapkan siklus plan-do-check-act (PDCA) (Sartika & Bisma, 2021). Sedangkan Metode Octave dikembangkan untuk melakukan evaluasi risiko, identifikasi aset, identifikasi kerentanan dan ancaman terhadap aset serta melakukan evaluasi potensi ancaman (Rido et al., 2023).

Penilaian Risiko merupakan salah satu proses dari manajemen risiko. Penilaian risiko merupakan proses awal dalam melakukan manajemen risiko. Penilaian risiko dilakukan untuk menentukan potensi ancaman dan risiko pada sistem. Hasil dari penilaian risiko yaitu identifikasi kontrol risiko untuk mengurangi atau menghilangkan risiko selama proses mitigasi risiko. Penilaian risiko memiliki 9 tahapan di dalamnya, diawali dengan Karakterisasi Sistem, Identifikasi Ancaman, Identifikasi Kerentanan, Analisis Kontrol, Penentuan Kemungkinan, Analisis Dampak, Penentuan Risiko, Rekomendasi Kontrol dan Dokumentasi Hasil Penilaian Risiko (Izatri et al., 2020).

SIMPEG merupakan salah satu sistem penerapan e-government yang menyediakan pelayanan administrasi kepegawaian sehingga memudahkan dalam mengakses data dan informasi pegawai (Dewi et al., 2022). Informasi pegawai tersebut seperti Nama, NIP, Alamat, SK CPNS, SK PNS, Kepangkatan, Jabatan, Unit Kerja, Gaji, Tingkat Pendidikan serta diklat-diklat yang pernah diikuti (Manurung & Julaeha, 2023). Dalam melakukan pengelolaan pegawainya, RRI menggunakan Sistem Informasi Manajemen Kepegawaian untuk digunakan oleh Lembaga Penyiaran Publik RRI (LPP RRI) sesuai Keputusan Mendagri No. 17 Tahun 2000 tentang Sistem Informasi Manajemen Kepegawaian Depdagri dan Pemda. Sistem ini merupakan salah satu asset SPBE LPP RRI untuk kategori office (E-Office). Dengan adanya SIMPEG dapat membantu para pegawai untuk mengakses data kepegawaian seperti melihat dokumen kepegawaian, melihat dan menginput

laporan kinerja pegawai secara online serta melihat dokumen pensiun dari seluruh pegawai yang tersebar di seluruh Indonesia. Tujuan adanya sistem informasi manajemen kepegawaian ini yaitu untuk membantu pihak sumber daya manusia dalam mengelola data pegawai-pegawai RRI untuk menghasilkan informasi yang dibutuhkan pihak manajerial ataupun pihak-pihak terkait secara efisien.

Setelah melakukan wawancara dengan pihak Teknologi dan Media Baru (TMB) dan Sumber Daya Manusia dan Umum (SDM) didapatkan informasi bahwa Sistem Informasi Manajemen Kepegawaian (SIMPEG) belum melakukan manajemen risiko oleh pihak TMB. Selain itu hasil wawancara didapatkan adanya beberapa permasalahan yang pernah terjadi selama SIMPEG RRI beroperasi, seperti pemadaman listrik selama kurang dari 3 jam. Kemudian dilakukan penanggulangan dengan menggunakan UPS (Uninterruptible Power Supply) yang dapat membantu sistem untuk tetap beroperasi. Selain itu, storage server backup yang penuh sehingga perlu mengatur retention backup menjadi 2 hari terakhir. Dan juga pernah terjadi beberapa kali server down karena hardware yang digunakan sudah lampau sehingga penggunaanya menjadi kurang optimal. Adanya permasalahan server down ini menyebabkan SIMPEG RRI tidak dapat diakses.

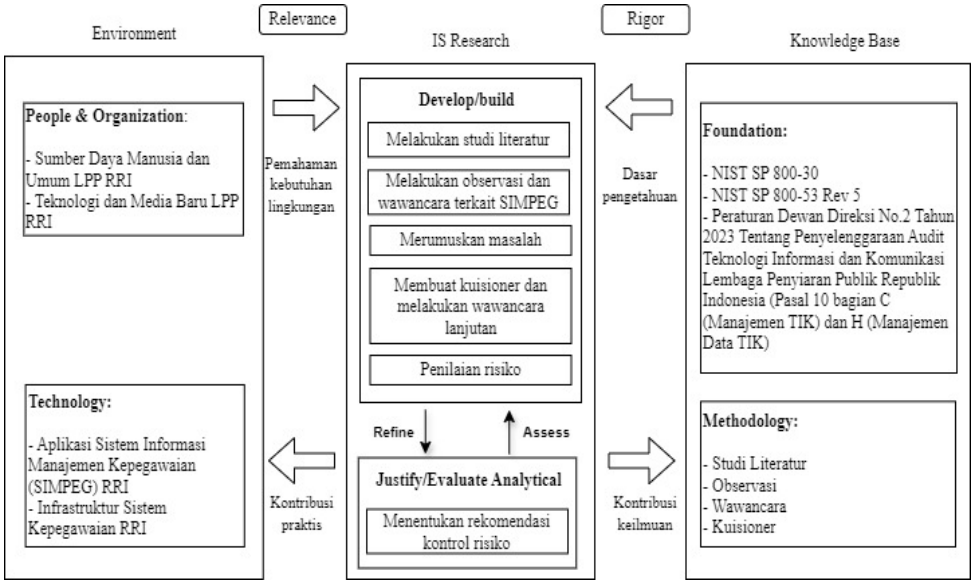
Oleh karena itu, perlu dilakukan penilaian risiko pada sistem untuk menghindari adanya risiko kerentanan lainnya pada SIMPEG RRI sehingga mempengaruhi kinerja sistem dan menghambat aktivitas di organisasi. Dari temuan-temuan kerentanan yang dapat terjadi pada sistem kemudian dianalisis menggunakan metode NIST SP 800-30 untuk mengetahui tingkat kerentanan yang ditemukan kemudian dapat diberikan kontrol rekomendasi sesuai tingkatan yang telah dilakukan penilaian. Kontrol rekomendasi ini berisi bagaimana mengurangi cara mencegah, kerentanan serta menghindari, menerima dampak-dampak yang timbul dari kerentanan yang terjadi agar tidak menghambat aktivitas yang berkaitan dengan SIMPEG RRI.

2. METODE PENELITIAN

A. Desain Penelitian

Penulis menyusun tahapan penelitian menggunakan kerangka penelitian sistem informasi yang dikembangkan oleh Hevner. Kerangka konseptual hevner

digunakan untuk memahami, mengeksekusi dan mengevaluasi penelitian sistem informasi dengan menggabungkan *behavioral-science* dan *design-science paradigms*. Didalam kerangka kerja ini memiliki tiga komponen yaitu *Environment, IS Research* dan *Knowledge Base* (Theresia Meiriati, 2020)



Kerangka Berpikir Penelitian ini melibatkan pihak Sumber Daya Manusia dan Umum LPP RRI dan pihak Teknologi dan Media Baru LPP RRI untuk mengumpulkan informasi terkait asset dan risiko pada Sistem Informasi Manajemen Kepegawaian (SIMPEG) RRI. Pengumpulan informasi dilakukan dengan melakukan observasi, wawancara dan kuisioner untuk mengkaji lebih dalam informasi yang didapatkan. Setelah informasi yang dibutuhkan sudah didapatkan, maka dapat dilakukan penilaian risiko sesuai dengan metode NIST SP 800-30. Penyusunan rekomendasi kontrol disusun berdasarkan dokumen NIST SP 800-53 Rev 5 dan penyusunan rekomendasi kontrol ini akan disesuaikan dengan tingkatan dari penilaian risiko yang sudah dilakukan sehingga hasil rekomendasi kontrol dapat dijadikan pertimbangan untuk diimplementasikan oleh organisasi.

B. NIST SP 800-30

Penelitian ini menggunakan metode NIST SP 800-30 untuk melakukan manajemen risiko pada Sistem Informasi Manajemen Kepegawaian (SIMPEG) RRI.

1. Karakterisasi Sistem (*System Characterization*)

Menentukan ruang lingkup penilaian risiko terkait sumber daya dan informasi pada SIMPEG. Penetapan ruang lingkup dilakukan dengan mengumpulkan informasi penting untuk mendefinisikan risiko (seperti *hardware*, *software*, data dan informasi, divisi yang bertanggung jawab dan infrastruktur). Penetapan ruang lingkup ini dapat dilakukan dengan pemberian kuisioner, wawancara ataupun peninjauan dokumen-dokumen (seperti dokumen kebijakan, dokumentasi sistem, dokumentasi keamanan dari sistem).

2. Identifikasi Ancaman (*Threat Identification*)

Identifikasi ancaman dilakukan dengan mempertimbangkan sumber ancaman yang berpotensi menyebabkan kerusakan pada sistem yang berasal dari alam, manusia atau lingkungan, potensi dari kerentanan dan pengendalian pada sistem.

3. Identifikasi Kerentanan (*Vulnerability Identification*)

Identifikasi kerentanan dapat dilakukan dengan mengidentifikasi sumber kerentanan dari potensi ancaman pada sistem yang dievaluasi (Fahrudin et al., 2022).

4. Analisis Kontrol (*Control Analysis*)

Analisis kontrol merupakan pengendalian yang sudah diterapkan oleh perusahaan terhadap sistem untuk meminimalisir kemungkinan ancaman yang dapat menimbulkan kerentanan pada kerja sistem.

5. Penentukan Kemungkinan (*Likelihood Determination*)

Penentuan tingkatan kemungkinan perlu mempertimbangkan motivasi dan kemampuan sumber ancaman, sifat kerentanan dan keberadaan dan efektivitas pengendalian yang ada.

6. Analisis Dampak (*Impact Analysis*)

Analisis dampak dilakukan untuk mengukur tingkat risiko dampak buruk yang diakibatkan dari kerentanan. Informasi untuk melakukan analisis dampak pada sistem dapat diperoleh dari misi sistem, kekritisan sistem dan data dan sensitivitas sistem dan data.

7. Penentuan Risiko (*Risk Determination*)

Penentuan risiko dilakukan berdasarkan kemungkianan sumber ancaman, besarnya dampak dari kerentanan berdasarkan sumber ancaman dan kecukupan pengendalian keamanan yang telah ada atau yang sedang direncanakan.

8. Rekomendasi Pengendalian (*Control Recommendation*)

Rekomendasi pengendalian dilakukan untuk mengurangi tingkat risiko terhadap sistem. Peenyusunan rekomendasi pengendalian tidak semua rekomendasi dapat diterapkan untuk mengurangi kerugian perlu disesuaikan kembali dengan melakukan evaluasi selama proses mitigasi risiko. Penyusunan rekomendasi pengendalian pada penelitian ini mengacu pada dokumen NIST SP 800-53 Rev 5. Di dalam dokumen NIST SP 800-53 Rev 5 ini terdapat 20 kelompok kontrol keamanan dan privasi (Security and Privacy Controls for Information Systems and Organizations, 2020).

9. Dokumentasi Hasil (*Result Documentation*)

Laporan penilaian risiko disajikan dengan pendekatan sistematis dan analitis untuk menilai risiko sehingga pihak manajemen dapat memahaminya sehingga akan mempermudah dalam mengurangi dan memperbaiki risiko.

3. HASIL DAN PEMBAHASAN

1. Karakterisasi Sistem (*System Characterization*)

Tahapan ini merupakan langkah pertama yaitu melakukan identifikasi ruang lingkup pada SIMPEG RRI dengan mengumpulkan informasi aset-aset teknologi informasi yang dapat menyebabkan risiko sehingga mempengaruhi keamanan informasi pada sistem. Dari hasil wawancara diketahui storage server backup data SIMPEG yang full sehingga menyebabkan data baru tidak terlindungi. Oleh karena itu, informasi aset teknologi informasi pada sistem akan diklasifikasikan sesuai dengan panduan NIST SP 800-30 meliputi *Hardware*, *Software*, Data dan Informasi dan Sumber daya Manusia untuk mengetahui risiko-risiko yang dapat terjadi pada aset tersebut.

2. Identifikasi Ancaman (*Threat Identification*)

Identifikasi ancaman merupakan tahapan untuk mengetahui potensi ancaman pada SIMPEG RRI yang dapat memicu kerentanan.

Tabel 1 Identifikasi Kejadian Ancaman

Informasi Ancaman	Sumber Ancaman
Kerusakan aset yang sudah menua	Kegagalan perlengkapan TI (*Hardware* pada *Server*)
Server Down	Kegagalan perlengkapan TI (*Server*)

Serangan dari luar yang menyebabkan gangguan jaringan	Individu di luar organisasi
Terganggunya daya listrik pada jaringan	Kegagalan perlengkapan TI (Jaringan)
Kerusakan perangkat jaringan	Bencana Alam
Serangan DDoS	Individu di luar organisasi
Password guessing	Individu di luar organisasi
Penyimpanan data backup penuh	Kelemahan aksesibilitas
Pemanfaatan celah keamanan	Individu di luar organisasi
Kesalahan penginputan data	Individu di dalam organisasi (Staff SDM, Admin Satker dan Pegawai)
Gagalnya sinkronisasi data karena jaringan terputus	Kegagalan perlengkapan TI (Jaringan)
Kegagalan sinkronisasi data karena kualitas data	Previleged User (Staff SDM, Admin Satker)
Kegagalan *backup* data	Kegagalan perlengkapan TI (Penyimpanan)
Keterbatasan dalam mencari data dan informasi pegawai	Pengembang SIMPEG
Kesalahan pengoperasian sistem	Previleged User (Staff SDM dan Admin Satker)
Kelalaian penanganan data dan informasi	Individu di dalam organisasi (Staff SDM, Admin Satker dan Staff TMB)

3. **Identifikasi Kerentanan (*Vulnerability Identification*)**

Tahapan ini akan menghasilkan daftar kerentanan (kelemahan atau kekurangan) pada SIMPEG yang kemungkinan dapat menimbulkan ancaman pada sistem. Penulis mengembangkan daftar kerentanan untuk menemukan celah-celah kerentanan yang dapat merugikan SIMPEG.

Tabel 2 Identifikasi Kerentanan

Jenis Aset	**Peristiwa Ancaman**	**Kerentanan**

Hardware	Kerusakan aset yang sudah menua	Belum dilakukan pembaruan hardware
	Server Down	Kerusakan komponen pada *server*
	Serangan dari luar yang menyebabkan gangguan jaringan	
	Terganggunya daya listrik pada jaringan	Kesalahan operasi peralatan listrik
	Kerusakan perangkat jaringan	Kurangnya pemeliharaan perangkat secara berkala
Software	Serangan DDoS	Lemahnya mekanisma autentifikasi pada API
	Password guessing	Penggunaan *password* yang lemah dan mudah ditebak
	Penyimpanan data *backup* penuh	Pengaturan *retention backup* yang tidak tepat
	Pemanfaatan celah keamanan	Pengguna menggunakan *password default*
Data dan Informasi	Kesalahan penginputan data	Kelalaian pegawai dalam menginput data
	Gagalnya sinkronisasi data karena jaringan terputus	Ketidak stabilan jaringan
	Kegagalan sinkronisasi data karena kualitas data	Kualitas data yang diinput rendah (data duplikasi, data tidak lengkap, standarisasi yang kurang)
	Kegagalan *backup* data	Kapasitas penyimpanan data tidak memadai
Data dan Informasi	Kegagalan *backup* data	Perangkat lunak *backup* yang sudah usang

	Fitur pencarian data dan informasi pegawai yang tidak efisien	Tidak dapat mencari data dan informasi pegawai berdasarkan lokasi pegawai
Sumber Daya Manusia	Kesalahan pengoperasian sistem	Kurangnya pelatihan dalam mengoperasikan sistem
	Kelalaian penanganan data dan informasi	Kurangnya edukasi kepada pegawai terkait keamanan data

4. **Analisis Kontrol (*Control Analysis*)**

Analisis kontrol merupakan bentuk cara dalam meminimalisir atau menghilangkan kemungkinan ancaman yang dapat menimbulkan kerentanan pada kerja sistem. Berikut merupakan kontrol dari risiko yang terjadi karena adanya eksploitasi ancaman.

1. Rusaknya komponen-komponen server yang menyebabkan server down sehingga pengendalian dilakukan dengan migrasi ke server baru.
2. Hacker membuat traffic yang tinggi sehingga server tidak stabil. Sehingga pihak TMB melakukan shut down pada server untuk sementara waktu.
3. Sistem tidak dapat menampilkan nama-nama pegawai berdasarkan lokasi dinas pegawai.
4. Kesalahan atau tidak sesuai dalam menginput data sehingga perlu pengecekan data kembali untuk laporan update data pegawai.
5. Gagal backup karena kesalahan pengaturan waktu retention backup sehingga perlu adanya penetapan waktu yang jelas untuk melakukan backup.
6. Kurangnya pemeliharaan secara berkala terkait server-server yang digunakan.

5. Penentuan Kemungkinan (Likelihood Determination)

Tahapan ini dilakukan untuk menentukan tingkat kemungkinan yang memiliki potensi kerentanan pada SIMPEG RRI.

Tabel 3 Tingkatan Kemungkinan *(Likelihood)*

Risiko	**Kemungkinan Terjadinya Ancaman**	**Kemungkinan Terjadinya Ancaman yang Menyebabkan Dampak Buruk**	**Kemungkinan Keseluruhan**
Kerusakan aset yang sudah menua	*Medium*	*High*	*Medium*
Server Down	*Medium*	*Medium*	*Medium*
Serangan dari luar yang menyebabkan gangguan jaringan	*Medium*	*Medium*	*Medium*
Terganggunya daya listrik pada jaringan	*Medium*	*Very High*	*High*
Kerusakan perangkat jaringan	*Low*	*Medium*	*Low*
Serangan DDoS	*Medium*	*High*	*Medium*
Password guessing	*Medium*	*Low*	*Low*
Penyimpanan data backup penuh	*High*	*Medium*	*Medium*
Pemanfaatan celah keamanan	*Medium*	*Medium*	*Medium*
Kesalahan penginputan data	*Medium*	*Low*	*Low*
Gagalnya sinkronisasi data karena jaringan terputus	*Medium*	*Low*	*Low*
Kegagalan sinkronisasi data karena kualitas data	*Medium*	*Low*	*Low*
Kegagalan backup data	*Medium*	*Very High*	*High*
Keterbatasan dalam mencari data dan informasi pegawai	*Medium*	*Medium*	*Medium*
Kesalahan pengoperasian sistem	*Medium*	*Medium*	*Medium*

Kelalaian penanganan data dan informasi	*Low*	*Medium*	*Low*

6. **Analisis Dampak (*Impact Analysis)***

Tahapan ini dilakukan untuk mengukur dampak negatif yang diakibatkan oleh ancaman yang mengeksploitasi kerentanan pada SIMPEG RRI.

Tabel 4 Tingkatan Dampak Negatif

Peristiwa Ancaman	**Dampak Kejadian Ancaman**	**Dampak**
Kerusakan aset yang sudah menua	High	Sistem rentan terhadap serangan
Server Down	High	Sistem tidak dapat diakses
Serangan dari luar yang menyebabkan gangguan jaringan	Moderate	Penurunan kinerja sistem yang dapat menghambat layanan yang dibutuhkan
Terganggunya daya listrik pada jaringan	Moderate	Perangkat yang terhubung dengan listrik tidak dapat digunakan
Kerusakan perangkat jaringan	Moderate	Tidak dapat terhubung ke internet
Serangan DDoS	Moderate	Layanan tidak dapat diakses oleh pengguna yang sah
Password guessing	Moderate	Penggunaan/pengakesesan akun dengan hak akses tidak sah
Penyimpanan data *backup* penuh	Moderate	Proses *backup* tidak berjalan dengan baik karena tidak ada ruang untuk menyimpan
Pemanfaatan celah keamanan	High	Data dan informasi *sensitive* dapat dicuri dan bocor oleh pihak yang tidak berwenang
Kesalahan penginputan data	Moderate	Informasi terkait data pegawai tidak akurat

Gagalnya sinkronisasi data karena jaringan terputus	Moderate	Keterlambatan proses sinkronisasi data pegawai dengan BKN
Kegagalan sinkronisasi data karena kualitas data	Moderate	Data dan Informasi yang dihasilkan tidak konsisten
Kegagalan *backup* data	Moderate	Data penting dan data sensitive hilang secara permanen
Keterbatasan dalam mencari data dan informasi pegawai	Moderate	Memperlambat proses kerja karena keterbatasan dalam mencari data dan informasi pegawai berdasarkan lokasi kerja
Kesalahan pengoperasian sistem	Moderate	*Crash system* karena kesalahan pembaruan sistem
Kelalaian penanganan data dan informasi	Moderate	Kebocoran data pegawai

7. **Penentuan Risiko (Risk *Determination*)**

Tahapan penentuan risiko dilakukan untuk menilai tingkatan risiko yang berdasarkan kemungkinan ancaman, tingkatan dampak dari kerentanan berdasarkan ancaman dan pengendalian yang telah ada.

Peristiwa Ancaman	**Tingkatan Kemungkinan**	**Tingkatan Dampak**	**Tingkatan Risiko**
Kerusakan aset yang sudah menua	*Medium*	*High*	*Medium*
Server Down	*Medium*	*High*	*Medium*
Serangan dari luar yang menyebabkan gangguan jaringan	*Medium*	*Medium*	*Medium*
Terganggunya daya listrik pada jaringan	*High*	*Medium*	*Medium*
Kerusakan perangkat jaringan	*Low*	*Medium*	*Low*
Serangan DDoS	*Medium*	*Medium*	*Medium*
Password guessing	*Low*	*Medium*	*Low*
Penyimpanan data *backup* penuh	*Medium*	*Medium*	*Medium*
Pemanfaatan celah keamanan	*Medium*	*High*	*Medium*

Kesalahan penginputan data	*Low*	*Medium*	*Low*
Gagalnya sinkronisasi data karena jaringan terputus	*Low*	*Medium*	*Low*
Kegagalan sinkronisasi data karena kualitas data	*Low*	*Medium*	*Low*
Kegagalan *backup* data	*High*	*Medium*	*Medium*
Keterbatasan dalam mencari data dan informasi pegawai	*Medium*	*Medium*	*Medium*
Kesalahan pengoperasian sistem	*Medium*	*Medium*	*Medium*
Kelalaian penanganan data dan informasi	*Low*	*Medium*	*Low*

8. **Rekomendasi Pengendalian (*Control Recommendation*)**

   Tahapan rekomendasi pengendalian dilakukan untuk mengurangi tingkat risiko terhadap sistem. Rekomendasi ini menjadi hasil dari proses penilaian risiko pada SIMPEG RRI. Terdapat rekomendasi kontrol risiko tingkatan medium pada SIMPEG RRI sebanyak 12 kelompok kontrol berdasarkan NIST SP 800-53 Rev 5. Rekomendasi kontrol risiko tingkatan low pada SIMPEG RRI sebanyak 6 kelompok control berdasarkan NIST SP 800-53 Rev 5.

9. **Dokumentasi Hasil (*Result Documentation*)**

   Tahapan ini merupakan dokumentasi penilaian risiko yang disajikan dengan pendekatan sistematis dan analitis sehingga pihak manajemen dapat memahaminya.

4. KESIMPULAN

Dari penelitian yang telah dilakukan pada SIMPEG RRI diketahui bahwa SIMPEG RRI belum melakukan manjamen risiko dan terdapat beberapa permasalahan selama sistem beroperasi. Oleh karena itu, untuk menghindari adanya permasalahan yang dapat memberikan kerugian yang lebih besar bagi organisasi maka dilakukan analisis manajemen risiko pada SIMPEG RRI menggunakan metode NIST SP 800-30 sebagai panduan melakukan penilaian risiko dan NIST SP 800-53 Rev 5 sebagai pedoman menyusun rekomendasi control untuk pengendalian sistem. Setelah dilakukan analisis penilaian risiko

pada SIMPEG RRI diketahui bahwa terdapat risiko dengan tingkatan Medium sebanyak 12 risiko dan risiko dengan tingkatan Low sebanyak 6 risiko. Kelompok rekomendasi control risiko dengan tingkatan Medium diantaranya Kelompok Pemeliharaan (Maintenance), Kelompok Perencanaan Kontingensi (Contingency Planning), Kelompok Kontrol Akses (Access Control), Kelompok Audit dan Akuntabilitas (Audit And Accountability), Kelompok Manajemen Konfigurasi (Configuration Management), Kelompok Tanggapan Terhadap Insiden (Incident Response), Kelompok Perlindungan Fisik Dan Lingkungan (Physical And Environmental Protection), Kelompok Penilaian Risiko (Risk Assessment), Kelompok Akuisisi Sistem Dan Layanan (System And Services Acquisition), Kelompok Perlindungan Sistem Dan Komunikasi (System And Communications Protection) dan Kelompok Integritas Sistem Dan Informasi (System And Information Integrity).

5. DAFTAR PUSTAKA

Budiono, N. J., Cahyono, A. D., & Tanaem, P. F. (2021). Evaluasi Manajemen Risiko Teknologi Informasi Pada Perusahaan Daerah Air Minum Kota Salatiga Menggunakan Framework Cobit 5.0. *Sebatik*, *25*(1), 82–91. https://doi.org/10.46984/sebatik.v25i1.1174

Dewi, F. R., Ariesmansyah, A., Ariffin, R. H. B., & Vaughan, R. (2022). Implementation E-Government in Employment Management Information Systemin the Regional Office of the Ministry of Law and …. *International Journal of Social Science (IJSS)*, *1*(5), 533–540.

Fahrudin, N. fitrianti, Nugraha S, A., & Ramadhan Putra, K. (2022). Penilaian Risiko Keamanan Data Karyawan Pada Sistem Informasi Dengan Menggunakan Framework Nist Sp 800-30 pada PT. ABC. *Jurnal Ilmiah Teknologi Infomasi Terapan*, *8*(3). https://doi.org/10.33197/jitter.vol8.iss3.2022.900

Gary Stoneburner, Alice Goguen, and A. F. (2002). Risk Management Guide for Information Technology Systems (NIST SP 800 - 30). In *Teaching of Psychology* (Vol. 29, Number 1).

Izatri, D. I., Rohmah, N. I., & Dewi, R. S. (2020). Identifikasi Risiko pada Perpustakaan Daerah Gresik dengan NIST SP 800-30. *JURIKOM (Jurnal Riset Komputer)*, *7*(1), 50. https://doi.org/10.30865/jurikom.v7i1.1756

Juliasari, Y., & Zulfikar, D. H. (2022). Analisis Manajemen Risiko Sistem Informasi Pendidik Dan Tenaga Kependidikan (SIMPATIKA) Menggunakan Framework NIST SP 800-30. *Seminar Nasional Riset &Inovasi …*, 63–72.

Manurung, L., & Julaeha, S. (2023). *Analisis Implementasi Kebijakan Sistem Informasi Manajemen Kepegawaian (SIMPEG) Pada Sekretariat Dewan Perwakilan Rakyat Daerah*. *11*(1), 52–59. https://doi.org/https://doi.org/10.31289/publika.v11i1.9521 Jurnal

Rido, F., Butar, B., Saputra, E., Marsal, A., & Hamzah, M. L. (2023). *Analisis Manajemen Risiko Keamanan Sistem Pengolahan Data Accurate Menggunakan Metode*. *7*(September), 675–685.

Sartika, I. F. N., & Bisma, R. (2021). Perancangan Sistem Informasi Manajemen Risiko berdasarkan ISO 27001: 2013 (Sistem Manajemen Keamanan Informasi). *Journal of Emerging Information …*, *02*(03), 81–86. https://ejournal.unesa.ac.id/index.php/JEISBI/article/view/41723/35905

Security and Privacy Controls for Information Systems and Organizations. (2020). https://doi.org/10.6028/NIST.SP.800-53r5

Syahrial Sidik, S. S., & Wahyuari, W. (2023). Manajemen Risiko Sistem Informasi Ujian Secara Daring Di Sekolah Tinggi Manajemen Asuransi Trisakti. *Jurnal Green Growth Dan Manajemen Lingkungan*, *12*(1), 84–97. https://doi.org/10.21009/10.21009/jgg.v12i1.06

Theresia Meiriati, A. S. S. N. M. (2020). Tata Kelola Manajemen Aset Ti Menggunakan Framework Cobit 5 Dan Itam. *Coding Jurnal Komputer Dan Aplikasi*, *8*(2). https://doi.org/10.26418/coding.v8i2.41264