Model Manajemen Risiko Sistem Informasi Untuk Sistem Informasi Manajemen Kepegawaian

Information System of Risk Management Model for Personnel Management Information System

Eka Yulisuyanti[1*], Benfano Soewito[2]
[1,2]Computer Science Department, BINUS Graduate Program – Master of Computer Science, Bina Nusantara University, Jakarta 11480, Indonesia
Email: eka.yulisuyanti@binus.ac.id[1], bsoewito@binus.edu[2]

Abstrak

Sistem informasi dan aplikasi manajemen kepegawaian memiliki peran penting dalam menjaga kerahasiaan data pribadi karyawan, terutama di sektor pemerintahan di mana manajemen karier sangat bergantung pada informasi dari data Aparatur Sipil Negara (ASN) dalam sistem informasi kepegawaian. Selain sebagai sumber informasi, aplikasi ini juga berfungsi sebagai perantara pengguna dan database. Namun, seringkali aplikasi ini menjadi target serangan siber yang bertujuan mengakses data pribadi ASN. Tidak ada aplikasi yang dapat menjamin keamanan mutlak atau bebas dari serangan semacam itu. Oleh karena itu, diperlukan pengembangan manajemen risiko teknologi informasi yang dapat diimplementasikan saat terjadi serangan. Penerapan framework standar untuk manajemen risiko dalam sistem informasi tidaklah mudah, sehingga diperlukan pedoman yang komprehensif. Penelitian ini bertujuan membangun model manajemen risiko khusus untuk sistem informasi kepegawaian, mengadopsi panduan NIST 800-34 Rev 1 dan NIST 800-61 Rev 2, serta mengintegrasikan teori terkait dengan pengembangan manajemen risiko dan contingency plan yang ada. Metode penelitian melibatkan tinjauan literatur sebelumnya dan analisis panduan NIST terkait manajemen risiko teknologi informasi untuk mengidentifikasi tahapan yang signifikan pada model manajemen risiko dalam sistem informasi. Penelitian ini akan menghasilkan model manajemen risiko yang mencakup analisis dampak bisnis, rencana tanggap insiden, dan rencana pemulihan bencana, dirancang khusus untuk sistem informasi kepegawaian dalam konteks pemerintahan.

Kata kunci: Manajemen Risiko, Model Manajemen Risiko Sistem Informasi, Sistem Informasi Kepegawaian, Contingency Plan, NIST

Abstract

Information systems and personnel management applications play a vital role in safeguarding the privacy of employee personal data, particularly in the government sector where career progression relies heavily on information derived from the State Civil Apparatus (ASN) data within the personnel information system. Apart from serving as an information source, these applications also act as intermediaries between users and databases. Unfortunately, they frequently become targets of cyberattacks aimed at unauthorized access to ASN personal data. It is crucial to acknowledge that no application can provide absolute security or guarantee immunity from such attacks. Consequently, the development of information technology risk management measures becomes necessary, ready to be implemented in the event of an attack. The implementation of a standardized risk management framework within information systems poses challenges, necessitating the creation of comprehensive guidelines. This research endeavors to construct a tailored risk management model specifically designed for personnel information systems. The model will adopt the guidelines established in NIST 800-34 Rev 1 and NIST 800-61 Rev 2, while integrating relevant theories pertaining to the development of risk management and contingency plans. The research methodology encompasses a comprehensive review of existing literature and an in-depth analysis of NIST guidelines concerning information technology risk management. The aim is to identify significant stages within the risk

management model applicable to information systems. The outcome of this study will yield a comprehensive risk management model for personnel information systems. The model will incorporate business impact analysis, incident response plans, and disaster recovery plans, tailored to suit the specific needs of personnel information systems within a government context..

Keywords: *Risk Management, Information System Risk Management Model, Personnel Information System, Contingency Plan, NIST.*

1. PENDAHULUAN

Di era transformasi digital seperti saat ini, data dan informasi menjadi asset yang sangat berharga bagi organisasi atau perusahaan [1]. Salah satu jenis data yang sangat penting dan perlu mendapatkan perlindungan adalah data pribadi, terutama data pribadi individu yang tersimpan pada basis data suatu sistem informasi yang dapat diakses secara daring melalui Internet [2]. Salah satu sistem informasi yang berperan krusial dalam proses bisnis suatu organisasi adalah sistem informasi kepegawaian. Hal ini berlaku tidak hanya bagi sector swasta, namun juga pada sector publik atau pemerintah dalam pengelolaan data dan informasi Pegawai Negeri Sipil (PNS) sebagaimana tercantum pada Pasal 175 ayat (1) Peraturan Pemerintah nomor 11 tahun 2017 tentang Manajemen PNS [3].

Meningkatnya adopsi teknologi informasi dalam pengelolaan data ASN khususnya yang dilakukan melalui aplikasi berbasis web yang dapat diakses secara daring melalui internet, berpotensi untuk menjadi sasaran kejahatan siber. Pencurian data maupun pemerasan dalam bentuk enkripsi data yang disertai dengan ancaman peyebarluasan data yang bersifat rahasia jika tidak penuhi dengan nilai tebusan tertentu (*ransomware*) dapat terjadi kapan pun selama aplikasi dapat diakses secara daring oleh peretas [4]. Keamanan data pribadi ASN menjadi sangat penting untuk dijaga dan diatur secara baik untuk menghindari tindakan penyalahgunaan atau pelanggaran privasi yang dapat merugikan individu tersebut. Oleh karena itu, manajemen risiko keamanan data pribadi ASN pada sistem informasi kepegawaian menjadi sangat penting untuk diterapkan.

Untuk mengelola risiko keamanan data pribadi ASN pada sistem informasi kepegawaian, diperlukan sebuah *framework* atau kerangka kerja yang dapat dijadikan acuan. *Framework* standar yang dapat dijadikan acuan antara lain *framework NIST Cybersecurity Framework* [5], [6], *NIST Special Publication 800-30 Revision 1 Guide for Conducting Risk Assessments* [7], *NIST Special Publication 800-34 Rev 1 Contingency Planning Guide for Federal Information Systems* [8], *NIST Special Publication 800-53 revision 5 Security and Privacy Controls for Information System and Organization* [9], [10], *NIST Special Publication 800-37 revision 2 Risk Management Framework for Information System and Organization* [11], dan *NIST Special Publication 800-61 revision 2 Computer Security Incident Handling Guide* [12], [13].

Perlu diingat bahwa implementasi *framework* standar tersebut pada sistem informasi kepegawaian tidaklah mudah dan seringkali dihadapkan dengan banyak hambatan. Banyak organisasi yang mengalami kesulitan dalam menerapkan NIST, karena kompleksitas dari standar tersebut. Oleh karena itu dalam rangka membantu organisasi menerapkan NIST dengan benar, maka dibutuhkan sebuah model atau panduan yang dapat memudahkan pemahaman dan penerapan standar tersebut.

Di sisi lain, setiap organisasi memiliki proses bisnis yang berbeda dan memiliki asset yang berbeda, sehingga mempunyai ancaman yang berbeda pula. Oleh karena itu implementasi *framework risk management* akan berbeda pula antara satu organisasi dengan organisasi yang lain. Oleh karena itu, penting bagi setiap bisnis untuk melakukan evaluasi dan analisis yang cermat sebelum mengadopsi *framework* keamanan data tertentu[14], sehingga dapat memastikan bahwa implementasinya tepat dan efektif dalam menjaga keamanan data dan informasi pribadi mereka.

Framework standar yang ada mengatur manajemen risiko teknologi informasi untuk tingkat organisasi, tetapi untuk manajemen risiko tingkat aplikasi atau system informasi belum ada pembahasan yang lebih detail. Di dalam paper ini kami akan mengembangkan model bagaimana implementasi konsep manajemen risiko pada sebuah system informasi manajemen kepegawaian. Sebagai studi kasus yang kami lakukan pada system informasi manajemen kepegawaian e-HRM Kementerian Pekerjaan Umum dan Perumahan Rakyat di mana di dalamnya terdapat modul-modul yang penting seperti: data pribadi, kualifikasi, rekam jejak jabatan, kompetensi, riwayat pengembangan kompetensi, riwayat hasil penilaian kinerja, dan informasi kepegawaian lainnya. Selain data kepegawaian, system informasi manajemen kepegawaian juga memiliki modul yang mendukung manajemen PNS seperti kenaikan pangkat, pensiun, penghargaan, disiplin, absensi, serta integrasi data dengan system informasi lainnya. Model yang kami kembangkan ini dapat dijadikan arahan atau acuan bagi organisasi melakukan implementasi *framework* tersebut. Model ini dapat membantu organisasi untuk menyesuaikan *framework* standar dengan kebutuhan dan kondisi bisnis system informasi kepegawaian, serta membantu dalam mengidentifikasi, mengevaluasi, dan mengelola risiko keamanan data pribadi dengan lebih baik dan efektif. Dengan memiliki model yang tepat, pemerintah dapat memperoleh manfaat dari penerapan *framework* standar yang sesuai dengan kebutuhan dan kondisi bisnis, sehingga dapat menjaga keamanan data pribadi dan mencegah terjadinya pelanggaran privasi atau penyalahgunaan data yang merugikan.

Penelitian terdahulu memberikan pemahaman dan wawasan terkait dengan framework manajemen risiko dan *contingency plan*. Beberapa penelitian yang terdahulu sebagai berikut:

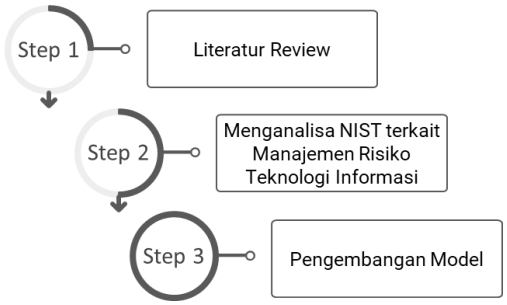
1. Shinde dan Kulkarni mengusulkan rancangan framework penanganan insiden berdasarkan hasil survey pada 17 organisasi yang berbeda. Framework yang diusulkan merupakan gabungan dari berbagai framework, termasuk NIST, ISO, dan SANS, yang digunakan oleh responden. Penelitian ini menyimpulkan bahwa framework yang tersedia sangat komprehensif dan bersifat umum agar bisa diterapkan di berbagai jenis organisasi. Namun, untuk mengadopsi framework dengan efektif dan efisien, perlu dilakukan penyesuaian dengan kondisi dan kebutuhan organisasi yang akan menggunakannya. [15].
2. Fernandes, Olivera, dkk dalam penelitiannya mengungkapkan meskipun telah terdapat berbagai framework dalam penanganan insiden namun kurangnya pengalaman yang memadai dan keragaman framework menjadi kendala bagi organisasi dalam merancang rencana respon insiden. Penelitian ini merumuskan strategi yang fleksibel untuk merancang IRP yang dapat disesuaikan dengan ruang lingkup dan tujuan organisasi mana pun. [16].
3. Pada penelitian Knight R dan Nurse J menyajikan penyesuaian-penyesuaian framework yang tidak disediakan pada framework-framework yang telah ada untuk meningkatkan efektivitas komunikasi pasca terjadinya insiden keamanan siber [17].
4. Pada penelitian yang lain yaitu He, Y., Maglaras, L., Aliyu, A., dan Luo, C menyampaikan penyesuaian framework terkait dengan tindakan proaktif dalam penanganan insiden (*proactive incident response*) yang tidak diakomodir pada framework NIST [18].

Pada penelitian sebelumnya tersebut penyesuaian terhadap beberapa framework lebih terfokus pada adopsi ditingkat proses bisnis organisasi, namun belum membahas lebih lanjut apakah penyesuaian terhadap model *best practice* untuk dapat diadopsi/diterapkan pada tingkat layanan system informasi atau aplikasi kepegawaian. Untuk itu pembaharuan pada penelitian ini sebagai berikut:

1. *Business Impact Analysis* (BIA) yang umumnya dibuat untuk proses bisnis dan asset organisasi, pada penelitian ini, BIA di tingkat sistem informasi atau aplikasi.
2. Model Manajemen Risiko Sistem Informasi yang dapat diterapkan oleh organisasi khususnya untuk sistem informasi kepegawaian guna meningkatkan ketahanan terhadap serangan siber di tingkat aplikasi.
3. Model ini merupakan studi kasus pada sistem informasi manajemen kepegawaian e-HRM Kementerian Pekerjaan Umum dan Perumahan Rakyat.

2. METODE PENELITIAN

Metodologi penelitian ini dilakukan dengan mempelajari *framework* standar terkait manajemen risiko system informasi oleh NIST dan mempertimbangkan penelitian-penelitian yang telah dilakukan sebelumnya. Melakukan analisa *framework* standar NIST untuk melakukan adaptasi dan diterapkan dalam mengembangkan model manajemen risiko system informasi manajemen kepegawaian. Penyesuaian perlu dilakukan karena layanan system informasi memiliki karakteristik yang unik. Model yang dibangun harus dapat di implementasikan dan mendukung keberlangsungan system informasi manajemen kepegawaian. Tahapan penelitian sebagaimana disajikan pada Gambar 1 sebagai berikut:



Gambar 1 Metodologi Penelitian

Literatur review sudah di bahas sebelumnya pada *section* 1. Pendahuluan. Untuk itu selanjutnya ke step ke 2 yaitu menganalisa NIST terkait Manajemen Risiko Teknologi Informasi. Kami akan melakukan analisis terhadap berbagai *framework* standar NIST dengan tujuan dari analisis ini adalah untuk menemukan referensi yang tepat untuk mengembangkan model yang sesuai untuk penerapan manajemen risiko teknologi informasi untuk sistem informasi manajemen kepegawaian. Dalam analisa framework standar ini, kami akan mempertimbangkan setiap elemen atau domain dari setiap *framework* standar yang dipilih untuk menghasilkan model manajemen risiko sistem informasi manajemen kepegawaian yang komprehensif, terarah, efektif dan relevan. Selanjutnya step ke 3 Pengembangan model akan di bahas pada *section* 2.1 Pengembangan Model.

2.1. Pengembangan Model

Untuk mengembangkan model manajemen risiko sistem informasi kepegawaian, kami akan menggunakan *framework* NIST dan teori pendukung. Tujuan kami adalah memperoleh model yang tepat dan dapat diterapkan dengan baik. Dengan mengembangkan model ini, kami memastikan bahwa manajemen risiko dan *contingency plan* efektif dalam menghadapi risiko dan mengantisipasi kemungkinan yang terjadi. Model yang dikembangkan dimulai dengan *Business Impact Analysis* (BIA) sebagaimana pada Gambar 2 sebagai berikut.

Gambar 2 Skema Pengembangan Model

Business Impact Analysis (BIA) di lakukan untuk mengidentifikasi aset kritikal, pontensi ancaman, risiko dan pengendalian atau kontrol yang telah ada. Sisa risiko yang tidak dapat ditangani melalui pengendalian atau kontrol yang telah teridentifikasi pada proses BIA di tangani melalui prosedur IRP. Apabila prosedur IRP tidak dapat menyelesaikan event atau kejadian maka tim akan menjalankan prosedur DRP. Hal ini memungkinkan organisasi untuk merespons dan memulihkan sistem informasi dengan cepat dan efektif saat terjadi keadaan darurat. Dengan demikian, organisasi memiliki rencana komprehensif dan terintegrasi untuk mengatasi risiko dan *contingency plan* dalam sistem informasi kepegawaian.

Dalam paper ini, pengembangan Model Manajemen Risiko Teknologi Informasi didasarkan pada kerangka kerja (*framework based*) *NIST Special Publication* 800-34 Rev 1 *Contingency Planning Guide for Federal Information Systems dan NIST Special Publication* 800-61 revision 2 *Computer Security Incident Handling Guide*, yang telah kami pelajari sebelumnya. Kerangka standar tersebut akan menjadi pedoman utama dalam penyusunan Model Manajemen Risiko Sistem Informasi untuk Sistem Informasi Manajemen Kepegawaian dalam penelitian ini.

A. NIST Special Publication 800-34 Rev 1 Contingency Planning Guide for Federal Information Systems

Isi dari NIST SP 800-34 Rev 1 adalah petunjuk, rekomendasi, dan pertimbangan yang ditujukan untuk menyusun rencana keberlangsungan (*contingency plan*) suatu sistem informasi. Penekanan *contingency plan* yang tertuang dalam NIST SP 800-34 Rev 1 adalah panduan dan langkah-langkah yang disusun untuk memulihkan layanan sistem informasi setelah terjadinya insiden atau gangguan. Terdapat tujuh proses contingency planning yang tertuang dalam NIST SP 800-34 Rev 1 antara lain:

a) *Develop the contingency planning policy*, yaitu formalisasi kebijakan dan arahan terkait contingency planning oleh pimpinan atau top management dalam bentuk aturan atau regulasi yang selanjutnya menjadi pedoman dan pemberian wewenang dalam penyusunan contingency plan dan implementasinya;

b) *Conduct the business impact analysis (BIA), yaitu kegiatan yang dilakukan untuk mengidentifikasi* berbagai ancaman yang mungkin terjadi sekaligus hal-hal kritis yang menyangkut keberlangsungan proses bisnis organisasi yang harus menjadi prioritas dalam pencegahan gangguan dan pelaksanaan pemulihan;

c) *Identify preventive controls*, yaitu aktivitas preventif yang dilakukan dengan melakukan identifikasi menyeluruh terhadap berbagai kontrol yang telah ada guna mengurangi dampak dari gangguan yang mungkint terjadi sehingga dapat meningkatkan ketersediaan layanan sistem informasi dan mengurangi pemborosan biaya pemulihan;

d) *Create contingency strategies*, yaitu perumusan strategi yang terkait dengan pemilihan berbagai metode pemulihan yang akan digunakan dan kapan metode tersebut digunakan untuk memastikan pemulihan sistem informasi dapat dilakukan secara cepat dan efektif setelah terjadi gangguan;

e) *Develop an information system contingency plan*, yaitu penyusunan petunjuk teknis dan prosedur-prosedur yang harus dilakukan oleh masing-masing personel dalam rangka pemulihan layanan sistem informasi;

f) *Ensure plan testing, training, and exercises*, yaitu kegiatan yang dilakukan untuk menguji dan memastikan bahwa rencana pemulihan dapat dieksekusi sesuai dengan target pemulihan yang diharapkan, peningkatan kapabilitas pemulihan, dan evaluasi terhadap hal-hal yang masih memerlukan perbaikan;

g) *Ensure plan maintenance*, yaitu kegiatan yang dilaksanakan untuk memastikan bahwa rencana yang telah disusun terus diperbarui agar senantiasa selaras dengan kondisi organisasi terkini.

B. NIST Special Publication 800-61 revision 2 Computer Security Incident Handling Guide

Isi dari NIST SP 800-61 Rev 2 adalah petunjuk, rekomendasi, dan pertimbangan yang ditujukan untuk menyusun rencana penanganan insiden (*incident response plan*). Beberapa hal yang harus ada dalam suatu dokumen IRP, diantaranya:

a) Mission;
b) Strategies and goals;
c) Senior management approval;
d) Organizational approach to incident response;
e) How the incident response team will communicate with the rest of the organization and with other organizations;
f) Metrics for measuring the incident response capability and its effectiveness;
g) Roadmap for maturing the incident response capability;
h) How the program fits into the overall organization.

3. HASIL DAN PEMBAHASAN

Berdasarkan metodologi penelitian yang tersaji pada Gambar 1 hasil dan pembahasan sebagai berikut:

3.1. Literatur Review Manajemen Risiko Keamanan Sistem Informasi

Pengembangan manajemen risiko sistem informasi dapat dibagi menjadi beberapa step yaitu *Business Impact Analysis* (BIA), *Incident Respon Plan* (IRP), dan *Disaster Recovery Plan* (DRP). Setelah semua komponen manajemen risiko ini selesai, maka dapat dijadikan pedoman yang disebut *contingency plan*.

Contingency plan merupakan suatu rencana yang disiapkan sebagai acuan untuk menanggapi kondisi bencana, pelaksanaan backup, dan pelaksanaan pemulihan pasca bencana dalam rangka memastikan ketersediaan layanan, akses terhadap sumberdaya penting, dan keberlangsungan operasional dalam situasi darurat [*NIST Special Publication 800-57 Part 1 Revision 5*] [19]. *Incident Response Plan* (IRP), dan *Disaster Recovery Plan* (DRP), sebagai bagian dari *Contingency Planning* dimana dalam penyusunan dari masing-masing rencana tersebut didahului dengan proses *Business Impact Analysis* (BIA) [20].

3.2. Menganalisa NIST terkait Manajemen Risiko Teknologi Informasi

Dari kelebihan *framework* standar yang telah di analisa dilakukan penyesuaian agar saling melengkapi untuk dijadikan tahapan dalam pembangunan Model Manajemen Risiko Sistem Informasi untuk system informasi manajemen kepegawaian. Terdapat 9 (sembilan) tahapan dalam melakukan pengembangan model manajemen risiko system informasi yaitu:

a) Pemahaman organisasi terkait isu internal dan eksternal. Hal ini penting karena aturan dan kebijakan terbaru berpengaruh terhadap kemampuan organisasi untuk mencapai tujuan pengembangan model manajemen risiko system informasi.
b) Wewenang dan kebijakan ditetapkan oleh Pimpinan organisasi yang merupakan permulaan siklus dan menjadi dasar hukum dan pedoman untuk membangun contingency plan.
c) Peran pimpinan/top management, dengan tujuan mendapatkan dukungan aktif dari pimpinan/top management agar semua program akan berjalan dengan baik.
d) Melakukan review/assessment terhadap system informasi manajemen kepegawaian dengan tujuan untuk membantu mengidentifikasi dan memprioritaskan aspek yang penting/kritikal.
e) Identifikasi pencegahan, kriteria ini untuk mencegah atau mengurangi pengaruh yang tidak diinginkan.
f) Menyediakan sumber daya yang dibutuhkan dalam pengembangan, implementasi, pemeliharaan dan peningkatan *contingency plan.*

g) Memilih strategi dan taktik contingency plan yang benar untuk mengidentifikasi dan memastikan proses pemulihan cepat dan efektif.

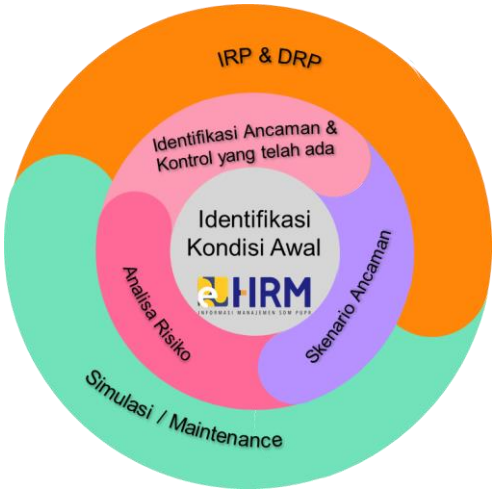
h) Penyusunan panduan/prosedur incident respon plan dan disaster recovery plan.

i) Validasi, evaluasi dan pengembangan. Tahapan ini merupakan tahap akhir siklus yang melakukan validasi, testing, evaluasi dan penigkatan *contingency planning.*

3.3. Pengembangan Model

Berdasarkan hasil analisa yang dilakukan pada tahapan sebelumnya, selanjutnya akan dikembangkan Model Manajemen Risiko Sistem Informasi untuk Sistem Informasi Majamenen Kepegawaian. Model yang akan kembangkan dimulai dengan *conduct bisnis impact analysis*, *incident respon plan* dan *disater recovery plan*. Hal ini bertujuan agar tahapan-tahapan *contingency plan* dapat fokus kepada penanggulangan insiden *cyber-attack* terhadap layanan system informasi manajemen kepegawaian. Model Manajemen Risiko Sistem Informasi untuk Sistem Informasi Majamenen Kepegawaian ditunjukkan pada

Gambar *3* sebagai berikut:



Gambar 3 Kontingensi Sistem Informasi Model (KOSIM)

A. *Preparation*

Penelitian ini menjawab permasalahan bagaimana menyusun model manajemen risiko system informasi untuk system informasi manajemen kepegawaian sesuai

Gambar *3*. Berdasarkan model manajemen risiko system informasi yang telah dihasilkan maka langkah-langkah perancangan model manajemen risiko dan contingency plan system informasi dapat diuraikan sebagai berikut:

a) Pemahaman organisasi, yaitu pemahaman yang mendalam yang membentuk konteks tentang organisasi (visi misi, tujuan, struktur, proses bisnis, sistem informasi kritikal, faktor internal, dan eksternal organisasi);

b) Penyusunan mandat *contingency plan* oleh top management yang mengamanatkan kebutuhan adanya *contingency plan* dan tim *contingency plan*, penyediaan kewenangan, dan panduan;

c) Pembentukan Tim *Contingency Planning* yang terdiri dari tim keskretariatan, tim respon insiden, dan tim pemulihan bencana;

d) Pelaksanaan analisa dampak bisnis yang terdiri dari proses identifikasi ancaman, indentifikasi kerentanan, identifikasi control, penilaian risiko berdasarkan kriteria kemungkinan dan dampak dengan mempertimbangkan control yang telah ada;

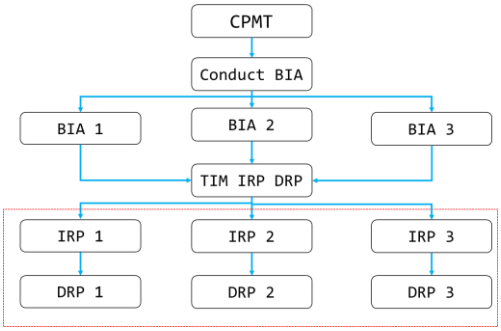
e) Penyusunan kebijakan contingency plan system informasi kritikal;

f) Penyusunan IRP dan DRP;

g) Pelaksanaan simulasi dan maintenance untuk memastikan keandalan IRP dan DRP serta contingency plan yang selaras dengan kondisi aktual organisasi.

Sebelum melakukan *bisnis impact analysis* dibentuk tim yang bertujuan untuk menyusun pernyataan kebijakan rencana kontingensi (*contingency planning policy statement*). *Contingency planning policy statement* merupakan suatu kebijakan formal yang menyatakan bahwa organisasi harus menyusun rencana kontingensi (*contingency plan*) termasuk didalamnya pejelasan peran dan kewenangan berbagai pihak yang terlibat dalam penyusunannya yang berperan sebagai *Contingency Planning Management Team* (CPMT) serta panduan yang diperlukan dalam penyusunan *contingency plan* yang efektif.

CPMT adalah tim yang di bentuk untuk menyusun *contingency planning* dengan beranggotakan perwakilan dari seluruh stakeholder, pengelola aplikasi, user, pengembang, pihak ke 3 (tiga) atau vendor dan komunitas/expert. Setelah CPMT menyelsaikan setiap komponen *Business Impact Analysis* (BIA) selanjutnya mulai membuat *Insiden Respon Plan* (IRP) dan *Disaster Recovery Plan* (DRP) yang dapat digambarkan pada Gambar 4 sebagai berikut:



Gambar 4 *Preparation Contingency Plan*

B. *Business Impact Analysis*

Business impact analysis (BIA) dilakukan terhadap sistem informasi kritikal yang telah dipilih untuk mendapatkan masukan dalam perancangan *contingency plan* yang akan disusun. Berdasarkan Gambar 4, BIA dilakukan dengan tahapan identifikasi kondisi awal, identifikasi ancaman dan kontrol yang telah ada, skenario ancaman, dan analisa risiko. Penjelasan dari tahapan BIA sebagai berikut:

a) Identifikasi kondisi awal

Dilakukan untuk mengetahui apakah dalam penerapan sistem informasi sudah sesuai dengan proses bisnis organisasi dan telah didukung dengan kondisi atau lingkungan yang mengoptimalkan keamaman sistem informasi. Hal ini dapat dilakukan melalui pendataan gambaran proses layanan Sistem Informasi yang meliputi: Peta Proses Bisnis Organisasi Level 0, Regulasi yang terkait dengan proses bisnis, Arsitektur Sistem Infomasi, Aset IT Sistem Infomasi, Daftar Layanan Sistem Infomasi, Daftar Pengguna Sistem Infomasi, Daftar Role/Hak Akses Sistem Infomasi, dan Metode Akses Sistem Infomasi yang disediakan.

Dalam melakukan identifikasi awal langkah-langkah yang dilakukan sebagai berikut:

- Melakukan wawancara kepada pemilik proses bisnis apakah sudah ada peraturan dan kebijakan terkait dengan *contingency plan* system informasi dan menunjukkan *blueprint* system informasi yang akan menjadi target perancangan *contingency plan*;
- Melakukan identifikasi proses yang dilakukan oleh system informasi dari sisi hak akses dan layanan system informasi untuk selanjutnya dapat di buat kelompok layanan system informasi berdasarkan hak akses dan proses layanan tersebut, selanjutnya akan disebut cluster layanan system informasi.

b) Identifikasi ancaman dan kontrol yang telah ada

Setelah diperoleh data daftar aset dan layanan Sistem Informasi pada tahapan pertama langkah selanjutnya dilakukan identifikasi sumber-sumber ancaman yang berpotensi mengganggu ketersediaan aset maupun keberlangsungan layanan system informasi, dilakukan dengan tahapan:

- Menentukan sumber ancaman dengan melakukan *vulnerability assessment* (VA) untuk mengetahui tingkat kerentanan yang dapat terjadi pada system informasi;
- VA dilakukan dengan standar owasp top 10;
- Nilai dari VA tersebut menjadi nilai tingkat kemungkinan terjadi.

Setelah daftar ancaman teridentifikasi selanjutnya dilakukan identifikasi kontrol yang telah ada terhadap ancaman tersebut. Identifikasi kontrol digunakan untuk menganalisis kontrol yang telah tersedia maupun yang sedang direncanakan untuk diimplementasikan oleh organisasi. Untuk mengetahui kontrol yang sudah ada dengan melakukan beberapa step sebagai berikut:

- Dengan mengetahui hasil VA terdapat rekomendasi perbaikan yang disarankan oleh OWASP;
- Melakukan uji coba source code terkait dengan kerentanan terhadap source code;
- Membuat flowcart ancaman dan kontrol untuk mempermudah pehaman terhadap posisi ancaman dan kontrol yang telah ada pada system informasi.

c) Skenario Ancaman

Setelah potensi ancaman dan kontrol yang telah ada terindentifikasi, selanjutnya dilakukan identifikasi skenario ancaman (*threat scenario*) dengan memberikan gambaran secara rinci mengenai properti dari suatu ancaman antara lain *actor, means, motives, outcome*, dan *security* untuk setiap ancaman.

d) Analisa Risiko

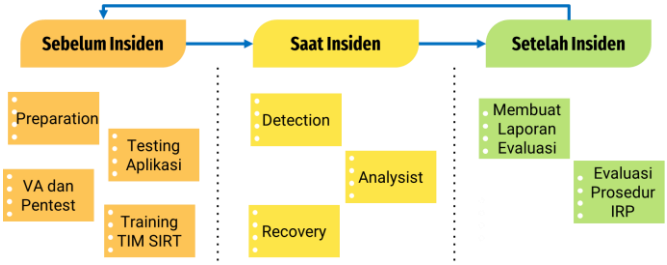
Setelah skenario ancaman teridentifikasi selanjutnya dilakukan analisis risiko dengan cara menentukan level kemungkinan dan level dampak terjadinya risiko berdasarkan kriteria risiko setelah mempertimbangkan keandalan pengendaliannya. Hasil dari proses analisis risiko adalah daftar risiko yang selanjutnya akan dilakukan perancangan terkait bagaimana penyusunan dokumen contingency plan nya yang terdiri dari *Incident Respon Plan* dan *Disaster Recovery Plan*.

Pada tahapan analisa risiko beberapa hal yang perlu diperhatikan yaitu:

- Untuk mempermudah melakukan perhitungan rumus risiko, sebelumnya di tentukan komponen dari rumus risiko tersebut.
- Pembobotan untuk menentukan nilai asset pada penelitian ini terbagi menjadi 2 (dua) yaitu nilai sensitifitas dan nilai prioritas.
  - Nilai prioritas adalah nilai berdasarkan jumlah akses setiap layanan dalam waktu 1 (satu) tahun yang diperoleh dari log *database*;
  - Nilai sensitifitas adalah nilai berdasarkan berapa banyak data yang digunakan untuk melakukan proses dari layanan tersebut.
- Nilai Aset adalah nilai dari penggabungan antara nilai prioritas dan nilai sensitifitas yang telah dikelompokkan dalam cluster dengan rumus sebagai berikut
  Nilai asset = 70% nilai prioritas + 30% nilai sensitifitas
- Rumus Risiko
  Risiko = (likelihood x nilai aset) + dampak
- Setelah melakukan perhitungan nilai risiko, selanjutnya mengurutkan hasil perhitungan risiko tersebut untuk mengetahun nilai ancaman tertinggi di setiap cluster layanan system informasi.

C. Perancangan *Incident Respon Plan*

Penyusunan IRP dari hasil skenario ancaman dan analisa risiko yang dilakukan pada tahapan BIA. Penyusunan IRP juga sekaligus membentuk tim untuk menjalankan prosedur IRP. Hal-hal yang perlu di perhatikan dalam perancangan IRP sebagai berikut:



Gambar 5 Perancangan *Incident Respon Plan*

Penjelasan dari perancangan incident respon plan pada Gambar 5 adalah sebagai berikut:

a) Sebelum Insiden

Pada tahapan ini melakukan 4 (empat) step yaitu preparation, testing aplikasi, vulnerability assessment atau penetration test, dan training tim SIRT dalam melakukan prosedur IRP yang telah dibuatkan sebelumnya.

b) Saat Insiden

Pada tahapan saat insiden melakukan detection dan analysist terkait cyber attack apa yang sedang terjadi. Setelah mengetahui jenis dan lokasi pada layanan apa cyber attack tersebut terjadi, selanjutnya melakukan *recovery*.

c) Setelah Insiden

Pada tahapan setelah insiden melakukan step *post-incident activity* yaitu membuat laporan evaluasi pasca terjadinya insiden. Hasil dari laporan tersebut juga dapat dijadikan bahan evaluasi untuk perbaikan prosedur IRP.

Elemen IRP minimal yang ada pada system informasi sebagai berikut:

a) Tujuan
b) Ruang Lingkup dan Definisi
c) Lembar Persetujuan dan Pengesahan
d) Pembentukan Tim Penanganan Insiden
e) Respon Penanganan Insiden
f) Metode dan Alur Komunikasi
g) Evaluasi dan Respon Insiden
h) Evaluasi Dokumen IRP.

D. Perancangan *Disaster Recovery Plan*

Perancangan DRP ini akan fokus kepada disaster yang diakibatkan oleh cyber attack. Hal-hal yang perlu diperhatikan dalam membangun perancangan DRP terhadap system informasi sebagai berikut:

a) Prosedur DRP akan dijalankan jika IRP tidak bisa menyelsaikan seatu insiden;
b) Prosedur backup, restore dan lokasi data center akan di buatkan prosedur terpisah dari penelitian ini;
c) Dibuatkan aturan tentang anggota tim DRP dengan tugas dan tanggung jawab;
d) Terdapat jalur komunikasi kepada tim DRP untuk melakukan penangulangan disaster cyber attack;
e) Selain tim DRP, daftar kontak pihak lain juga perlu di persiapkan seperti stakeholder, programmer atau pengembang dan penyedia layanan.

Elemen minimal yang harus ada pada dokumen DRP untuk system infromasi sebagai berikut:

a) *Policy;*
b) Pembentukan TIM DRP;

c) Komunikasi dan Aktivasi;
d) Pada saat *Disaster*;
e) Setelah *Disaster*.

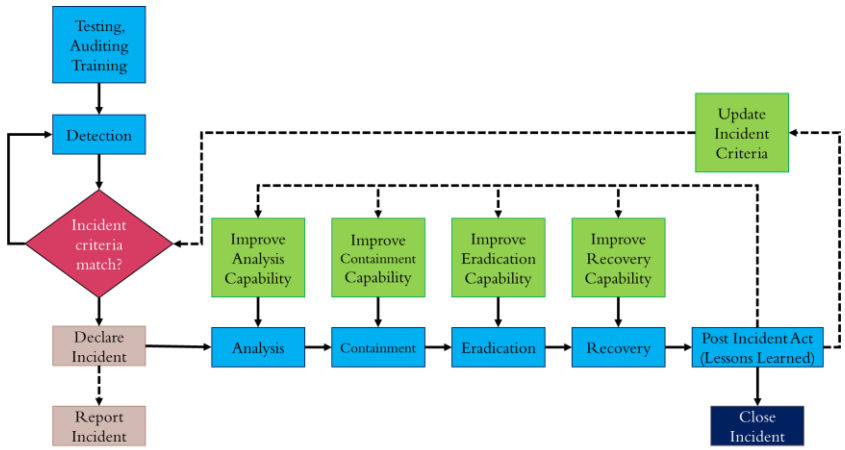
E. Simulasi *(Maintenance)*

Simulasi/ *maintenance* memiliki peran untuk memastikan keandalan *contingency plan* yang telah disusun. Proses simulasi dilakukan untuk menguji apakah seluruh personel, tahapan, instrumen, dan prosedur yang tercantum dalam *contingency plan* dapat dieksekusi dalam waktu tanggap (*response time*) yang diharapkan dan apakah dalam pelaksanaannya terdapat kelemahan-kelemahan (*flaws*) yang perlu untuk dikoreksi. Beberapa hal yang perlu di perhatikan yaitu:

a) Dalam melakukan simulasi dan maintenance terdapat target layanan apa yang akan dilakukan simulasi dan *maintenance*;
b) Dipersiapkan strategi simulasi dan *maintenance;*
c) Komunikasi;
d) Pelaporan simulasi dan *maintenance*.

F. Evaluasi

Tahapan evaluasi dilakukan untuk memperbaiki setiap prosedur yang telah dibuat sebelumnya. Skema evaluasi dapat dilihat pada Gambar 6 sebagai berikut:



Gambar 6 Evaluasi Prosedur IRP

Evaluasi ini juga dilakukan pada prosedur DRP untuk meningkatkan keamanan dan memperbaiki prosedur yang telah dibuat sebelumnya.

4. KESIMPULAN

Penerapan model manajemen risiko system informasi studi kasus pada system informasi manajemen kepegawaian memerlukan adaptasi dari *framework* standar yang ada karena sifatnya yang unik. Fokus dari penelitian ini adalah pada pengembangan model manajemen risiko system informasi manajemen kepegawaian. Untuk mencapai hal ini, studi menggunakan kerangka kerja berdasarkan NIST 800-34 Rev 1, dan NIST 800-61 Rev 2 dan menghasilkan sebuah model manajemen risiko system informasi yang dapat di aplikasikan pada system informasi manajemen kepegawaian.

Kontingensi Sistem Informasi *Model (KOSIM)* pada

Gambar *3* memberikan model referensi dalam mengembangkan *contingency plan* untuk layanan informasi. terdiri dari 6 komponen yaitu Identifikasi Kondisi Awal, Identifikasi Ancaman dan Kontrol yang telah ada, Skenario Ancaman, Analisa Risiko, *Incidect Respon Plan* dan *Disaster Recovery Plan*, dan Simulasi-Maintenance. Pelaksanaan pengembangan KOSIM ini mengacu pada Sistem Informasi Manajemen Kepegawaian di Kementerian Pekerjaan Umum

dan Perumahan Rakyat yang disebut *Electronic Human Resourse Management* (eHRM) yang memiliki service atau layanan data pegawai, kenaikan pangkat, pensiun, penghargaan, disiplin, baperjakat, cuti, kartu istri (karis) dan kartu suami (karsu), kenaikan gaji berkala, KPPI dan ujian dinas, jabatan fungsional, monitoring dan API ke aplikasi lain yang memerlukan data kepegawaian Kementerian PUPR baik itu internal maupun eksternal. Namun KOSIM ini tidak menutup kemungkinan untuk di terapkan pada aplikasi lain, karena pada pelaksanaan implementasinya sangat mudah.

Keluaran dari penelitian ini adalah sebuah model rancangan untuk mengelola sistem informasi kepegawaian (eHRM) Kementerian Pekerjaan Umum dan Perumahan Rakyat. Di dalam *framework* tersebut simulasi dan *maintenance* yang mencakup validasi juga di bahas dalam *framework* ini.

DAFTAR PUSTAKA

[1] J. M. Cavanillas, E. Curry, and W. Wahlster, "The Big Data Value Opportunity," in *New Horizons for a Data-Driven Economy*, Cham: Springer International Publishing, 2016, pp. 3–11. doi: 10.1007/978-3-319-21569-3_1.

[2] Z. Ke and L. Yongzhen, "Research on Internet data security and privacy protection," *J Phys Conf Ser*, vol. 2005, no. 1, p. 012004, Aug. 2021, doi: 10.1088/1742-6596/2005/1/012004.

[3] Republik Indonesia, *Peraturan Pemerintah RI No. 11 Tahun 2017 tentang Manajemen Pegawai Negeri Sipil*. Republik Indonesia, 2017.

[4] R. Aswandi, P. Muchsin, and M. Sultan, "Perlindungan Data dan Informasi Pribadi melalui Indonesia Data Protection System (IDPS)," *Jurnal Legislatif, Fakultas Hukum, Universitas Hasanudin*, vol. 3, no. 2, pp. 167–190, Jun. 2020.

[5] A. Ibrahim, C. Valli, I. McAteer, and J. Chaudhry, "A security review of local government using NIST CSF: a case study," *J Supercomput*, vol. 74, no. 10, pp. 5171–5186, Oct. 2018, doi: 10.1007/s11227-018-2479-2.

[6] M. Frayssinet Delgado, D. Esenarro, F. F. Juárez Regalado, and M. Díaz Reátegui, "Methodology based on the NIST cybersecurity framework as a proposal for cybersecurity management in government organizations," *3C TIC: Cuadernos de desarrollo aplicados a las TIC*, vol. 10, no. 2, pp. 123–141, Jun. 2021, doi: 10.17993/3ctic.2021.102.123-141.

[7] S. Salnyk, P. Sydorkin, S. Nesterenko, A. Zaytcev, and M. Konotopetc, "Comparative analysis of the us ISO and NIST standards on assessing the risk of information leakage in communication systems," *Journal of Scientific Papers "Social development and Security,"* vol. 10, no. 6, pp. 29–39, Dec. 2020, doi: 10.33445/sds.2020.10.6.4.

[8] A. Setyawan, Y. Giri Sucahyo, and A. Gandhi, "Design of Disaster Recovery Plan: State University in Indonesia," in *2020 Fifth International Conference on Informatics and Computing (ICIC)*, IEEE, Nov. 2020, pp. 1–5. doi: 10.1109/ICIC50835.2020.9288543.

[9] Yevhenii Kurii and Ivan Opirskyy, "Analysis and Comparison of the NIST SP 800-53 and ISO/IEC 27001:2013," *Cybersecurity Providing in Information and Telecommunication Systems, , Kyiv, Ukraine*, Oct. 2022.

[10] C. S. Puteho, A. Gamundani, and I. Nhamu, "Applying the NIST cybersecurity framework in developing a digital forensic incident response roadmap for the security sector in Namibia," *SSRN Electronic Journal*, 2023, doi: 10.2139/ssrn.4332936.

[11] National Institute of Standards and Technology, "Risk management framework for information systems and organizations:," Gaithersburg, MD, Dec. 2018. doi: 10.6028/NIST.SP.800-37r2.

[12] L. Tello-Oquendo *et al.*, "A Structured Approach to Guide the Development of Incident Management Capability for Security and Privacy," in *Proceedings of the 21st International Conference on Enterprise Information Systems*, SCITEPRESS - Science and Technology Publications, 2019, pp. 328–336. doi: 10.5220/0007753503280336.

[13] A. Rabello, J. Goulart, M. Karam, M. Pitanga, R. Filho, and R. Ricioni, "Proposed Incident Response Methodology for Data Leakage," *ICSEA 2021 : The Sixteenth International Conference on Software Engineering Advances*, pp. 50–55, 2021.

[14] D. Mahima, "Cyber Threat in Public Sector: Modeling an Incident Response Framework," in

2021 International Conference on Innovative Practices in Technology and Management (ICIPTM), IEEE, Feb. 2021, pp. 55–60. doi: 10.1109/ICIPTM52218.2021.9388333.

[15] N. Shinde and P. Kulkarni, "Cyber incident response and planning: a flexible approach," *Computer Fraud & Security*, vol. 2021, no. 1, pp. 14–19, Jan. 2021, doi: 10.1016/S1361-3723(21)00009-9.

[16] A. O. L. S. and C. R. Alexandre Fernandes, "A Strategy for Implementing an Incident Response Plan," in *Proceedings of the European Conference on Information Warfare and Security*, Academic Conferences International Ltd, 2021. doi: 10.34190/EWS.21.080.

[17] R. Knight and J. R. C. Nurse, "A framework for effective corporate communication after cyber security incidents," *Comput Secur*, vol. 99, p. 102036, Dec. 2020, doi: 10.1016/j.cose.2020.102036.

[18] Y. He, L. Maglaras, A. Aliyu, and C. Luo, "Healthcare Security Incident Response Strategy - A Proactive Incident Response (IR) Procedure," *Security and Communication Networks*, vol. 2022, pp. 1–10, Feb. 2022, doi: 10.1155/2022/2775249.

[19] National Institute of Standards and Technology, "NIST Special Publication 800-57 Part 1 Revision 5," Gaithersburg, MD, May 2020. doi: 10.6028/NIST.SP.800-57pt1r5.

[20] Michael E. Whitman; Herbert J. Mattord, *Principles of Incident Response & Disaster Recovery 3rd Edition* . 2022.