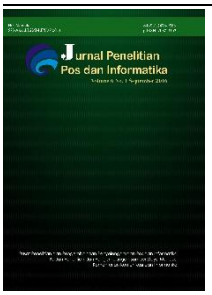
e-ISSN 2476-9266
p-ISSN: 2088-9402



JPPI Vol 7 No 1 (2017) 17-36
Jurnal Penelitian Pos dan Informatika

771/AU1/P2MI-LIPI/08/2017
32a/E/KPT/2017

DOI: 10.17933/jppi.2017.070102

MANAJEMEN RISIKO INFRASTRUKTUR *CLOUD* PEMERINTAH MENGGUNAKAN NIST *FRAMEWORK* STUDI KASUS LEMBAGA ILMU PENGETAHUAN INDONESIA (LIPI)

GOVERNMENT CLOUD INFRASTRUCTURE RISK MANAGEMENT USING NIST FRAMEWORK CASE STUDY IN INDONESIAN INSTITUTE OF SCIENCES (LIPI)

Wahyu S. Prabowo[1], Widyawan[2], Noor A. S, M[3]. Hanif Muslim[4], Yoga S. Utama[5]

Departemen Teknik Elektro dan Teknologi Informasi[123]
Fakultas Teknik Universitas Gadjah Mada[123]
Jl. Grafika No.2 Kampus UGM, Yogyakarta, Indonesia[123]
Biro Umum Lembaga Ilmu Pengetahuan Indonesi (LIPI)[45]
Jl. Jend. Gatot Subroto No. 10, Jakarta, Indonesia[45]
wahyu.cio14@mail.ugm.ac.id

Naskah Diterima: 12 April 2017; Direvisi : 23 Mei 2016; Disetujui : 15 Juni 2017

Abstrak

Lembaga Ilmu Pengetahuan Indonesia (LIPI) sejak tahun 2015 telah menggunakan teknologi *cloud computing* sebagai pengganti infrastruktur *data center* yang mengalami kerusakan. Setiap penerapan teknologi baru, organisasi dihadapkan berbagai peluang dan risiko yang dapat mempengaruhi kinerja organisasi tersebut. Terlebih *cloud computing* merupakan salah satu skema outsourcing TIK sehingga manajemen risiko yang tepat harus dilaksanakan. Tujuan penelitian ini adalah melakukan manajemen risiko terhadap penggunaan teknologi *cloud computing* menggunakan *framework* yang tepat sehingga manfaat dari teknologi tersebut dapat diperoleh secara maksimal. Penelitian ini menggunakan *framework* NIST SP800-37 *revision* 1 *Guide for Applying the Risk Management Framework to Federal Information Systems*. Pemilihan *framework* ini karena dari hasil analisis *framework* ini paling sesuai dengan kondisi LIPI. Selain itu *framework* ini telah diadaptasi untuk bisa menyesuaikan dengan lingkungan *cloud*. Hasil dari penelitian yang telah terlaksana sampai tahap ketiga adalah tersusunnya rencana keamanan yang merupakan bagian dari proses manajemen risiko. Diharapkan rencana keamanan yang berisi kategorisasi sistem informasi, tipe informasi, dan kontrol keamanan yang terpilih dapat diimplementasikan sehingga keamanan lingkungan *cloud* dapat terjamin.

Kata kunci: *cloud computing, manajemen* risiko, keamanan, NIST *framework*, LIPI

Abstract

Indonesian Institute of Sciences (LIPI) since 2015 has been using cloud computing technology as a substitute for damaged data center infrastructure. Every application of new technology, organizations are faced with various opportunities and risks that can affect the organization's performance. Moreover cloud computing is one of the ICT outsourcing schemes so that proper risk management must be implemented. The purpose of this research is to perform risk management on the use of cloud computing technology using the right framework so that the benefits of such technology can be obtained maximally. The study used the NIST SP800-37 revision 1 Guide for Applying the Risk Management Framework to Federal Information Systems. Selection of this framework because of the results of this framework analysis most in accordance with the conditions LIPI. In addition, this framework has been adapted to be able to adjust to the cloud environment. The result of the research that has been done until the third stage is the establishment of a security plan that is part of the risk management process. It is expected that a security plan containing the information system categorization, information type, and security controls selected can be implemented so that the security of the cloud circle can be guaranteed.

***Keywords**: cloud computing, risk management, security, NIST framework, LIPI*

PENDAHULUAN

Pemanfaatan Teknologi Informasi dan Komunikasi (TIK) yang dilaksanakan secara optimal akan membantu mempercepat proses transformasi e-government. Begitu penting peranan TIK bahkan pertumbuhan ekonomi suatu bangsa dapat didorong dengan lebih cepat oleh TIK (Meiningsih et al., 2013). Salah satu hal yang mendasar dalam survei pemeringkatan *e-government* yang dilakukan oleh waseda adalah *Network Preparedness/ Digital Infrastructure* (Obi, 2014, 2015). Infrastruktur yang memadai merupakan tulang punggung dalam pelaksanaan *e-government*.

Salah satu *key factor* dalam Indikator *Network Preparedness/Digital Infrastructure* salah satunya adalah *cloud computing*. Paradigma baru yang diusung oleh *cloud computing* terkait layanan TIK antara lain : reduksi biaya, fleksibilitas layanan yang tinggi, dan metode akses yang dapat dilakukan dimana saja, kapan saja, dan menggunakan perangkat apa saja (Avram, 2014; Frantsvog, Seymour, & John, 2012; Hsu, Ray, & Li-Hsieh, 2014; Tim Mell, 2009; Zissis & Lekkas, 2011). Hal tersebut dapat menjadi pendorong pemerintah untuk segera melakukan adopsi *cloud computing* (Zhang & Chen, 2010).

Lembaga Ilmu Pengetahuan Indonesia (LIPI) telah melakukan adopsi teknologi *cloud computing* sejak tahun 2015. Operasional TIK yang efektif dan efisien sangat dibutuhkan oleh LIPI yang terdiri dari 50 satuan kerja dengan lokasi yang tersebar di seluruh Indonesia. Migrasi *data center* tradisional menjadi *virtual private data center* yang baerbasis *cloud* merupakan hal baru bagi LIPI. Penerapan teknologi baru bagi organisasi memberikan berbagai peluang dan risiko yang dapat mempengaruhi kinerja organisasi tersebut baik positif maupun negatif (Samani, Honan, & Reavis, 2015), terlebih *cloud computing* adalah salah satu skema dari *outsourcing* TIK sehingga manajemen risiko yang tepat harus segera dilaksanakan (Paquette, Jaeger, & Wilson, 2010; Yaumi & Kridanto, 2012).

Manajemen risiko merupakan kegiatan yang kompleks dan melibatkan semua komponen dari organisasi (National Institute of Standards and Technology, 2011). Hubbard menyampaikan bahwa manajemen risiko merupakan kegiatan mengidentifikasi, melakukan penilaian, dan membuat prioritas terkait risiko, selanjutnya harus dilakukan minimalisasi, monitoring, dan kontrol terhadap kemungkinan maupun dampak dari kejadian yang tak terduga (Hubbard, 2009). Sampai saat ini layanan *cloud computing* yang telah diterapkan LIPI masih belum dilakukan reviu. Pengelolaan teknologi informasi masih berdasarkan insiden yang terjadi. Sehingga perlunya pengelolaan yang mengacu pada standar / kerangka kerja tertentu sangat dibutuhkan.

Cloud Security Alliance (CSA) telah merilis 9 ancaman/ risiko yang paling signifikan terhadap cloud computing antara lain : *Data Breaches, Data Loss, Account Hijacking, Insecure APIs, Denial of Service, Malicious Insiders, Abuse of Cloud Services, Insufficient Due Diligence, dan Shared Technology Issues* (*Cloud Security Alliance*, 2013). Manajemen risiko yang baik akan mengurangi dampak yang merugikan dan meningkatkan peluang manfaat yang menguntungkan dalam pemanfaatan TIK.

Susanto et al. telah membandingkan lima besar standar dalam keamanan informasi yaitu ISO27001, BS 7799, PCIDSS, ITIL, dan COBIT (Susanto,

Almunawar, & Tuan, 2011). Hasil penelitian ini merekomendasikan ISO27001 sebagai standar yang paling banyak digunakan terkait keamanan informasi. Perbandingan antara ISO27001 dengan framework NIST telah dilakukan oleh Kuligowski (Kuligowski, 2009), yang menghasilkan pemetaan antara keduanya, tetapi menurutnya NIST lebih berfokus pada sistem informasi.

Sesuai dengan rekomendasi dari (Kundra, 2011) dan (Iorga & Karmel, 2015) penelitian ini akan menggunakan *framework* NIST untuk manajemen risiko pada *cloud computing* dengan beberapa pertimbangan antara lain: (a) *framework* NIST telah diadaptasi pada lingkungan *cloud*; (b) dukungan panduan dan katalog yang komprehensif; (c) framework ini disusun oleh NIST di bawah *Departement of Commerce* USA yang telah terbukti kematngan pengelolaan teknologi informasi dan menempati rangking teratas sesuai survei Waseda.

Besarnya manfaat *cloud computing* dan risiko yang dihadapi juga sangat berbahaya, serta belum adanya manajemen risiko pada LIPI terkait penggunaan *cloud computing*, maka penelitian ini bertujuan untuk memberikan rekomendasi manajemen risiko menggunakan kerangka kerja yang telah terstandar. Diharapkan hasil penelitian dapat diimplementasikan sehingga manfaat dari teknologi *cloud computing* dapat dirasakan optimal untuk mendukung kinerja organisasi.

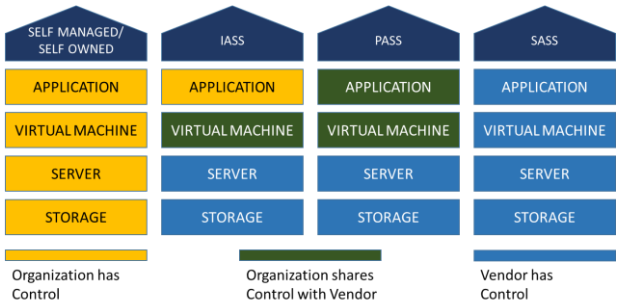
METODE

Penelitian ini menggunakan metodologi yang dikembangkan oleh Hevner et al., yang disebut dengan *Design Science In Information System Research* (Hevner, March, Park, & Ram, 2004; Khrisna & Harlili, 2014). Pemilihan metodologi ini karena DSIISR merupakan sebuah kerangka kerja penelitian yang secara esensial memecahkan masalah (*problem-solving*) pada area sistem informasi dengan tahapan sebagai berikut :

a. *Problem identification and research goals*
   Mendefinisikan latar belakang permasalahan yang dihadapi dan hasil yang ingin dicapai. Identifikasi ini menghasilkan permasalahan bahwa LIPI telah melakukan migrasi infrastrukturnya ke lingkungan *cloud*, sehingga manajemen risiko yang sesuai perlu diterapkan.
b. *Literature review*
   Studi literatur dilaksanakan dengan cara mengumpulkan referensi yang terkait dan mendukung penelitian. Referensi tersebut terdiri dari penelitian-penelitian yang pernah dilakukan, teori dasar pendukung, perundang-undangan, dokumen standar, buku, serta sumber lain dari internet.
c. *Analysis and design*
   Analisis terhadap referensi yang telah dikumpulkan pada tahap sebelumnya. Analisis ini terkait *framework* yang paling sesuai, langkah yang mungkin dilaksanakan.
d. *Implementation and evaluation*
   Melakukan implementasi kerangkan manajemen risiko pada *Virtual Private Cloud* LIPI berdasarkan tahap sebelumnya dan menggunakan alat yang telah disebutkan sebelumnya yaitu NIST SP 800-37 *Revision* 1, NIST SP 800-39, dan NIST SP 800-53, karena saling keterkaitan satu dengan yang lainnya.
e. *Conclusions*
   Kesimpulan dari kegiatan penelitian yang bisa dijadikan sebagai salah satu acuan untuk pengambilan keputusan bagi pengelolaan *Virtual Private Cloud* LIPI.

Penelitian Terdahulu

Adopsi teknologi *cloud* dapat diartikan bahwa sebuah organisasi menjadi tergantung terhadap penyedia layanan, tetapi dalam pengertian lain bahwa terdapat pembagian wewenang antara organisasi (pengguna) dengan penyedia layanan, hal ini lebih dikenal sebagai "*trust boundary*" pembatasan wewenang (Carstensen, Golden, & Morgenthal, 2012). Gambar 1 menunjukkan perbedaan *trust boundary* dari masing-masing model implementasi *cloud computing*. Pembagian wewenang tersebut disisi lain dapat juga dikatakan terdapat pembagian risiko "*risk-share*" antara kedua belah pihak.



Gambar 1. Pembagian wewenang dalam implementasi *cloud computing*
Sumber : (Chan, Leung, & Pili, 2012)

Alnuem et al. telah melakukan perbandingan beberapa kerangka kerja manajemen risiko pada lingkungan *cloud computing* (Alnuem, Alrumaih, & Al-Alshaikh, 2015). Terdapat 7 (tujuh) kerangka kerja yang dievaluasi, berdasarkan cakupannya terbagi menjadi 3 (tiga) jenis yaitu : *Cloud Environments Security Evaluation Frameworks, Cloud Environments Security Analysis Frameworks*, dan *Frameworks Based on Security Policies*. Kebijakan dalam manajemen risiko suatu organisasi harus mempertimbangkan aspek *confidentiality*, *integrity*, dan *availability*. Meskipun kerangka kerja yang telah ada tersebut telah mencakup semua model layanan maupun implementasi *cloud*, tetapi masih berfokus pada aspek layanan, sedangkan aspek keamanan masih kurang mendapatkan porsi yang cukup.

Khrisna dan Harlili telah mengintegrasikan COBIT 5 dengan salah satu *framework* untuk manajemen risiko untuk *cloud computing* oleh Xie et al. (Khrisna & Harlili, 2014)(Xie et al., 2012). Fungsi penanganan risiko pada COBIT 5 terdapat pada EDM03 : *Ensure Risk Optimization* dan APO12 *Risk Management*. Tata kelola terkait risiko yang baik akan mengoptimalkan keuntungan penggunaan *cloud*, sehingga kerangka kerja manajemen risiko oleh Xie et al. yang diintegrasikan dengan COBIT 5 akan lebih komprehensif dalam mengelola risiko yang ada pada *cloud computing*. Integrasi ini menghasilkan 2 tahapan yaitu *risk governance* dan *risk management*, setiap tahapan mempunyai proses utama dan pendukung. Proses utama terkait *risk optimization*, *risk identification*, *risk analisys*, dan *risk response*. Sedangkan untuk proses pendukung merupakan deskripsi bagaimana untuk melakukan kedua tahapan tersebut secara efektif dan efisien.

CSA juga menyediakan *Cloud Controls Matrix* (CCM) untuk pengguna layanan *cloud* terkait keamanan pada lingkungan *cloud computing*. CCM merupakan kerangka kerja yang dikembangkan berdasarkan beberapa standar antara lain : ISO 27001/27002, ISACA COBIT, PCI, NIST, Jericho Forum, dan NERC CIP (Cordero, 2016). Zhao (Zhao, 2012) dalam (Alnuem et al., 2015) telah mengembangkan kerangka kerja manajemen risiko yang berbasis pada beberapa standar dan CCM yang dapat digunakan untuk semua model *cloud computing*. Iorga (Iorga, 2015) menyampaikan bahwa pendekatan *Cloud-adapted Risk Management Framework* juga merupakan hasil

pemetaan dari CSA CCM.

Yaumi dan Kridanto dalam (Yaumi & Kridanto, 2012) menggunakan COSO *Enterprise Risk Management* (ERM) sebagai kerangka kerja manajemen risiko pada sebuah Perguruan Tinggi. Penilaian risiko menggunakan pendekatan metode *Failure Mode and Effects Analysis* (FMEA) yang proaktif, berbasis tim, dan sistematis. Identifikasi risiko terkait *cloud* menggunakan publikasi dari ENISA (Catteddu & Hogben, 2009) disesuaikan dengan objek penelitian Sistem Informasi Akademik dan *e-learning*. Beberapa risiko dengan kategori dampak yang tinggi antara lain: *lock-in*, *cloud service termination of failure*, dan *cloud provider acquisition*.

Pengukuran risiko *cloud computing* pada Perguruan Tinggi juga dilakukan oleh Andriyani et al. (Andriyani, Ulfa, & Cholil, 2013). Menggunakan kerangka kerja *The Operationally Critical Threat, Asset, and Vulnerability Evaluation for Small Organizations* (OCTAVE-S) yang merupakan turunan dari OCTAVE. Kerangka kerja ini memiliki beberapa tahapan yaitu: (1) Membuat profil ancaman berbasis aset; (2) Mengidentifikasi kelemahan infrastruktur; dan (3) Membuat perancangan dan strategi keamanan. Terdapat 10 (sepuluh) hal terkait penilaian risiko yaitu: *Security Policy*, *Organizational Security*, *Asset Clasification & Control*, *Personnel Security*, *Fhysical Environmental Security*, *Communication & Operations Management*, *Access Control*, *System Development & Maintenance*, *Business Continuity Management*, dan *Compliance*. Hasil penelitian menunjukkan bahwa pada tiap poin penilaian masih harus ditingkatkan.

Penilaian risiko pada manajemen risiko *cloud* menggunakan *Risk Management Guide for Information Technology Systems* yang dikembangkan oleh NIST telah dilakukan Hidayat dalam penelitiannya di Pemerintah Daerah (Hidayat, 2013). Identifikasi risiko menggunakan CSA *Top Threat to Cloud Computing* V1.0 yang meliputi: *Abuse and Nefarious Use of Cloud Computing*, *Insecure Interface and* APIs, *Malicious Insiders*, *Shared Technology Issues*, *Data Loss or Leakage*, *Account or Service Hijacking*, dan *Unknown Risk Profile*. Beberapa aksi terkait risiko telah disampaikan, tetapi tidak ada hasil kuantifikasi dari penilaian risiko tersebut.

(Susanto et al., 2011) telah membandingkan lima besar standar dalam keamanan informasi yaitu ISO27001, BS 7799, PCIDSS, ITIL, dan COBIT. Beberapa hal yang menjadi perhatian antara lain : fokus, kekuatan, komponen pendukung, dan metodologi yang digunakan dalam mengimplementasi. Hasil penelitian ini merekomendasikan ISO27001 yang telah banyak diterima dan terimplementasi lebih dari 163 negara dan berfokus pada keamanan informasi. Sedangkan secara khusus perbandingan dan pemetaan antara ISO27001 dengan FISMA / NIST SP 800 *Family* telah dilakukan oleh Kuligowski (Kuligowski, 2009). Hasil penelitian ini secara umum mendefinisikan bahwa NIST *Framework* adalah untuk sebuah sistem, sedangkan ISO27001 merupakan standar untuk proses manajemen. NIST *Framework* lebih fokus mendefinisikan, menilai, implementasi, dan monitoring terhadap sebuah sistem.

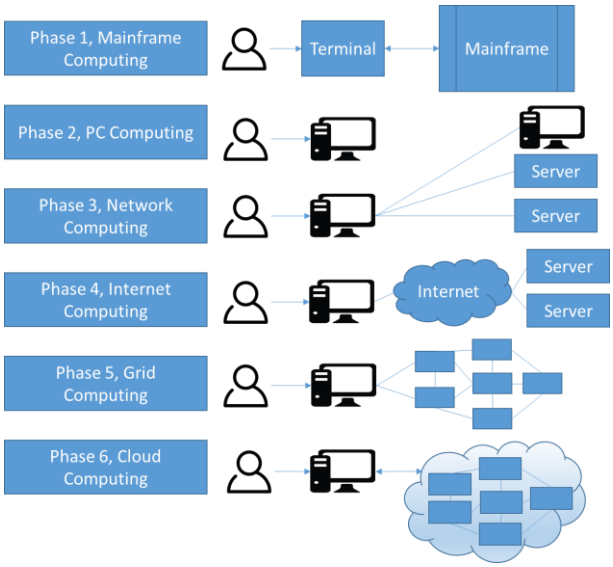
Konteks layanan TIK di LIPI yang berbasis *cloud computing* (*virtual private data center*), memungkinkan kapabilitas dari sisi pengguna dapat dikelola secara langsung (Iorga & Karmel, 2015).

Berdasarkan (Iorga & Karmel, 2015) dan (Kundra, 2011) kerangka kerja yang paling sesuai untuk menerapkan manajemen risiko adalah NIST SP 800-37 *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.* Beberapa alasan pemilihan kerangka kerja tersebut antara lain : (a) NIST Framework telah banyak digunakan dan merupakan pendekatan manajemen risiko yang dapat disesuaikan dengan lingkungan *cloud* (Iorga & Scarfone, 2016; Luna, Suri, Iorga, & Karmel, 2015); (b) organisasi yang mempublikasikan adalah lembaga pemerintah dengan tingkat maturitas TI yang sudah mapan sehingga sesama lembaga pemerintah dapat menyesuaikan dengan kebutuhan (Obi, 2016); (c) panduan yang komprehensif dari setiap tahapan dan dapat digunakan secara umum (NIST, 2010). Selain itu pemilihan untuk menggunakan standar keuntungan yang akan diperoleh organisasi adalah lebih terarah dalam implementasi, keterbaruan acuan akan tetap terjaga, transparan dan dapat diaudit, serta yang paling penting dengan menggunakan standar akan meminimalkan risiko (Spafford, 2003). Manajemen risiko yang dilakukan oleh penyedia layanan juga sangat dibutuhkan, karena model layanan yang digunakan adalah *Infrstructure as a Service* (IaaS).

Cloud Computing

Frost dan Sullivan dalam laporannya '*The New Language of Cloud Computing*' menyatakan terdapat empat faktor yang berpengaruh dalam pemanfaatan layanan cloud yaitu aplikasi, keputusan bisnis, pelanggan, dan keamanan (Frost & Sullivan, 2015). Sebanyak 91% enterprise di wilayah Asia Pasifik sedang dalam posisi merencanakan penerapan *cloud* pada perusahaan mereka dan sebagian sedang dalam tahap penerapan. Pengguna layanan *cloud* juga bervariasi mulai dari organisasi kecil maupun perorangan dapat menggunakan layanan berkelas dunia dengan biaya yang lebih terjangkau (Ardagna, 2015). Definisi terkait *cloud computing* sendiri telah banyak disampaikan oleh para praktisi, vendor, jurnalis, dll. Salah satu rujukan yang paling banyak digunakan adalah yang telah dirilis oleh *National Institute of Standards and Technology* (NIST) yang mendefinisikan *Cloud Computing* sebagai sebuah model yang memungkinkan untuk *ubiquitous* (dimanapun dan kapanpun), nyaman, *On demand* akses jaringan ke sumber daya komputasi (contoh: jaringan, *server*, *storage*, aplikasi, dan layanan) yang dapat dengan cepat dirilis atau ditambahkan (Tim Mell, 2009).

Gambar 2 menunjukkan 6 fase paradigma dalam komputasi (Furht, 2010) yang diadaptasi dari Voas dan Zhang. Fase 1 merupakan masa komputer *mainframe* yang sangat besar ukuran dan kapasitasnya, pengguna mengakses melalui *dummy terminal*. Fase 2 komputer personal mulai digunakan untuk memenuhi kebutuhan pengguna. Fase 3 komputer, laptop, dan server dapat terhubung dalam jaringan lokal. Fase 4 jaringan-jaringan internal membentuk jaringan global (internet). Fase 5 model komputasi *grid* merupakan sistem komputasi terdistribusi melalui jaringan internet untuk membagi *computing power* maupun *storage*. Fase 6 merupakan masa *cloud computing* dari *resource shared* yang dapat diakses dari jaringan internet dengan skalabilitas dan cara yang mudah.



Gambar 2. Fase Paradigma Komputasi
Sumber : (Furht, 2010)

Model layanan pada *cloud computing* lebih dikenal dengan "*as a Service* (aaS)", NIST (Tim Mell, 2009) telah menyampaikan tiga model layanan yang ditawarkan oleh *cloud computing* hal ini berdasarkan kemampuan yang disediakan: *Software as a Service* (SaaS), *Platform as a Service* (PaaS), dan *Infrastucture as a Service* (IaaS). Perkembangan kebutuhan pasar membuat model layanan yang semakin inovatif antara lain: *business process-as-a-service* (BPaaS), *cloud advertising-as-a-service* (CAaaS), *analytics-as-a-service* (DAaaS), *data storage-as-a-service* (DSaaS), *cloud management-as-a-service* (CMaaS), *backup-as-a-service* (BaaS), *database- as-a-service* (DaaS), bahkan *everything-as-a-service* (EaaS) (Hausman, Cook, & Sampaio, 2013; Kauffman, Ma, & Yu, 2014).

Risiko dan Manajemen Risiko

Definisi risiko dalam penelitian bidang sistem informasi masih memiliki banyak konsep yang berbeda-beda, dalam penelitiannya Ackerman (Ackermann, 2012) menyampaikan bahwa risiko berasal dari "*riscare*" yang berarti "berani terhadap sesuatu". Meskipun banyak juga definisi risiko yang dapat diterima dan digunakan oleh berbagai industri (Hardy, 2015), konsep paling umum terkait risiko dapat dilihat pada Tabel 1.

Tabel 1. Definisi Risiko

Pengguna	Definisi Risiko	Manajemen Risiko	Sumber
Layanan Public (Kanada)	Risiko merupakan ketidakpastian terhadap peristiwa/hasil pada masa yang akan datang, tujuan yang akan dicapai oleh organisasi dipengaruhi oleh kemungkinan dan dampak dari suatu risiko	Pendekatan secara sistematik untuk mencari jalan terbaik dalam menghadapi ketidakpastian dengan beberapa tahapan : identifikasi, penilaian, memahami, reaksi dan komunikasi terhadap kemungkinan-kemungkinan risiko	*Integrated Risk Management Framework, Treasury Board of Canada Secretariat, April 2001*
Government Accountability Office (GAO) USA	Kejadian yang memiliki dampak negatif dan berpengaruh terhadap aset, aktivitas, dan operasional	Proses yang berkelanjutan dalam menilai risiko, meminimalisasi potensi yang mungkin dapat terjadi, dan mempersiapkan langkah-langkah apabila terjadi risiko terjadi.	*Government Accountability Office, Report #* GAO-06-91, *December 2005*
ISO 31000	Akibat yang ditimbulkan dari ketidakpastian terhadap suatu tujuan tertentu	Aktivitas yang terkoordinasi pada sebuah organisasi terkait tata kelola dan kontrol terhadap risiko	ANSI/ASSE Z690.2-2011 *Risk Management Principles and Guidelines*

Sumber : (Hardy, 2015)

Manajemen risiko memainkan peranan yang penting diberbagai bidang, misal statistik, ekonomi, analisis sistem, biologi, maupun operasional penelitian (Djemame, Armstrong, Guitart, & Macias, 2014). Manajemen risiko pada masa sebelumnya merupakan bagian dari proses keamanan, tetapi dengan berjalannya waktu pendekatan secara sistematis mulai dari yang bersifat transaksional dan fungsional sampai pada tingkat strategis (Hardy, 2015). Secara konsisten berbagai literatur menyatakan bahwa manajemen risiko merupakan sebuah proses berulang yang terdiri dari empat tahapan : identifikasi, kuantifikasi, penanganan, dan evaluasi risiko (Ackermann, 2012).

Definisi manajemen risiko sebelumnya telah disampaikan dari beberapa sumber. Hubbard dalam (Hubbard, 2009) menyampaikan bahwa manajemen risiko merupakan kegiatan mengidentifikasi, melakukan penilaian, dan membuat prioritas terkait risiko, selanjutnya harus dilakukan minimalisasi, monitoring, dan kontrol terhadap kemungkinan maupun dampak dari kejadian yang tak terduga. Secara umum telah banyak standar maupun kerangka kerja manajemen risiko antara lain ISO 31000:2009.

NIST Framework

Manajemen risiko merupakan aktivitas yang melibatkan setiap aspek dari organisasi. NIST menyampaikan bahwa manajemen risiko dapat diterapkan pada tiga tingkatan dalam organisasi, demikian pula kegiatan penilaian risiko, yaitu Tingkat 1 (level organisasi), Tingkat 2 (level proses bisnis), dan Tingkat 3 (level sistem informasi). Tingkatan/ hirarki ini akan menunjukkan perspektif risiko dari sisi strategis sampai teknis (NIST, 2010). Gambar 3 merupakan ilustrasi dari tingkatan manajemen risiko sesuai rekomendasi NIST. Secara umum manajemen risiko dan penilaian risiko biasanya hanya pada level sistem informasi, sehingga akan menghasilkan risiko hanya dari perspektif teknis. NIST menyarankan pengembangan penilaian sampai dengan sisi strategis berdasarkan ancaman yang ada pada sisi teknis.

Gambar 3. Tingkatan Manajemen Risiko
Sumber : NIST SP800-37r1

Kebutuhan terkait keamanan informasi dapat dilaksanakan dengan pengelolaan yang baik terkait manajemen, operasional, dan teknis kontrol keamanan yang dapat diambil dari NIST *Special Publication* 800-53. Kerangka kerja manajemen risiko berdasarkan NIST SP800-37 R1 merupakan pendekatan yang lebih efektif terkait pengelolaan risiko keamanan informasi. Terlebih lagi dalam lingkungan *cloud* yang melibatkan kompleksitas penyedia layanan dan ancaman *cyber* yang semakin meningkat.

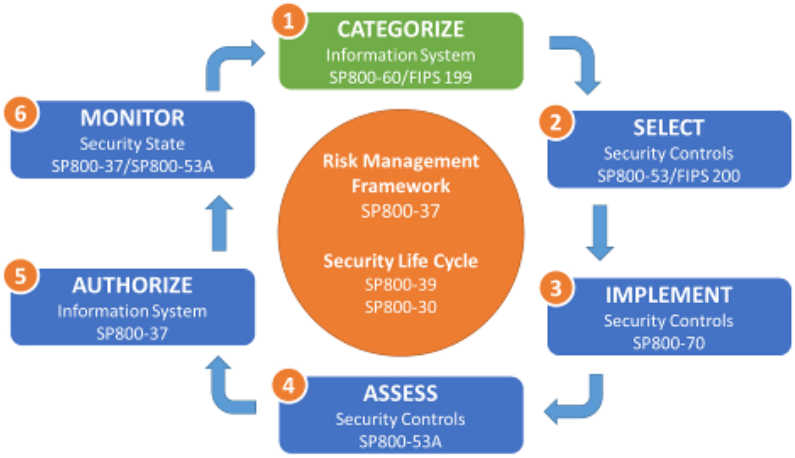
Kerangka kerja manajemen risiko NIST SP800-37 R1 merupakan proses yang terstruktur dan terintegrasi terkait aktivitas manajemen risiko keamanan informasi yang terbagi dalam beberapa tahapan (Gambar 4) yaitu :

a. *Categorize*, mengkategorisasikan sistem informasi dan informasi yang diproses, disimpan, dan dikirimkan oleh sistem tersebut

berdasarkan analisis dampak. Kategorisasi keamanan merupakan langkah yang sangat vital dalam mengintegrasikan pengelolaan keamanan (Stine, Kissel, Barker, Lee, & Fashlsing, 2008), identifikasi ini dimulai dari informasi terkait sistem dan keterkaitannya dengan terminologi keamanan dalam hal ini adalah *confidentiality*, *integrity*, dan *availability*.

b. *Select*, memilih *baseline* kontrol keamanan sistem informasi berdasarkan kategorisasi, standar kontrol keamanan, dan kondisi yang ada pada organisasi.
c. *Implement*, melakukan implementasi kontrol keamanan dan membuat deskripsi terkait operasional kontrol keamanan tersebut.
d. *Assess*, melakukan penilaian terhadap kontrol keamanan menggunakan prosedur penilaian untuk memperoleh informasi apakah kontrol keamanan telah diimplementasi dengan benar, dijalankan sesuai prosedur, dan memberikan dampak yang baik terhadap sistem informasi.
e. *Authorize*, otorisasi terkait operasional sistem informasi berdasarkan determinasi risiko yang dihasilkan maupun dari penetapan risiko yang dapat diterima oleh organisasi.
f. *Monitor*, memonitor kontrol keamanan sistem informasi yang telah berjalan baik itu terkait efektivitas, dokumentasi terhadap perubahan-perubahan yang terjadi, melakukan analisis dampak terkait perubahan tersebut, dan melaporkan semuanya kepada manajemen/ pimpinan organisasi.

Penelitian ini hanya dilaksanakan sampai dengan tahap III karena keterbatasan sumberdaya dan waktu yang ada.



Gambar 4. Proses Manajemen Risiko
Sumber : NISTSP800-37r1

Keamanan Informasi dan Sistem Informasi

Dimensi risiko keamanan informasi dan sistem informasi dapat diterapkan baik pada lingkungan teknologi informarmasi yang masih tradisional maupun yang telah beralih pada lingkungan berbasis *cloud* (Hausman et al., 2013). Tujuan utama dari keamanan informasi dan sistem informasi adalah untuk melindungi kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*avalability*) data dari suatu organisasi (Ravi & Sankar, 2015; Sendi & Cheriet, 2014). Konsep keamanan ini sering disebut sebagai *CIA Triad*.

Kerahasiaan (confidentiality)

Kerahasiaan dapat merujuk pada tingkat sensivitas data (Hausman et al., 2013), sehingga data yang mempunyai sifat rahasia harus dilindungi dari akses, penggunaan, penyebaran yang tidak terotorisasi (Erl, Mahmood, & Puttini, 2014). Kerahasiaan ini dalam lingkungan cloud berkenaan dengan pembatasan akses terhadap data ketika ditransit maupun disimpan.

Integritas (integrity)

Integritas dapat dirujuk pada kehandalan data tersebut (Hausman et al., 2013), dibutuhkan proteksi agar data tidak diubah oleh pihak yang tidak terotorisasi. Termasuk dalam integritas data adalah bagaimana data disimpan, diproses, dan diterima oleh layanan *cloud.*

Ketersediaan (availability)

Ketersediaan merujuk pada tingkat aksesibilitas dari data (Hausman et al., 2013), sehingga data harus proteksi dari gangguan agar tingkat aksesibilitasnya tinggi. Ketersediaan layanan dalam cloud merupakan tanggungjawab dari penyedia layanan *cloud* dan juga penyedia akses menuju layanan *cloud*.

Penilaian Dampak Keamanan

Dampak yang paling memungkinkan terjadi akibat pelanggaran keamanan ada tiga tingkatan (Stine et al., 2008). Kategorisasi keamanan akan berpengaruh baik pada informasi maupun sistem informasi, demikian juga informasi secara elektronik maupun non-elektronik. Tingkatan dampak dapat dilihat pada Tabel 2.

Tabel 2. Dampak Keamanan

Dampak	Definisi
Rendah (*low*)	Dampak dikatakan rendah apabila pelanggaran terhadap kerahasiaan, integritas, ataupun ketersediaan mempunyai efek samping yang terbatas baik terhadap operasional, aset, maupun individu dari organisasi.
Sedang (*moderate*)	Dampak dikatakan sedang apabila pelanggaran terhadap kerahasiaan, integritas, ataupun ketersediaan mempunyai efek samping yang serius baik terhadap operasional, aset, maupun individu dari organisasi.
Tinggi (*high*)	Dampak dikatakan tinggi apabila pelanggaran terhadap kerahasiaan, integritas, ataupun ketersediaan mempunyai efek samping yang parah baik terhadap operasional, aset, maupun individu dari organisasi.

Sumber : FIPS 199

HASIL DAN PEMBAHASAN

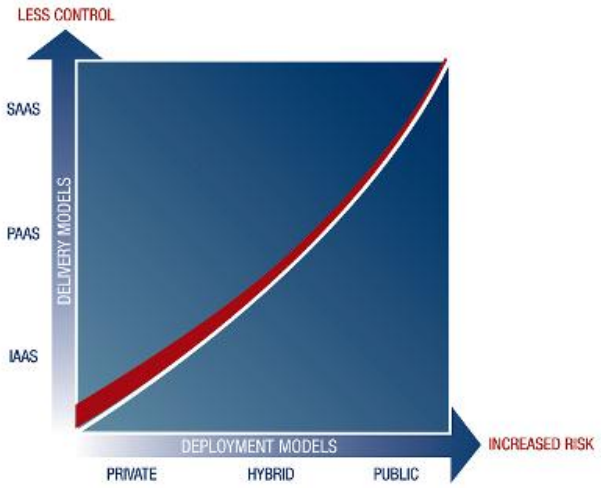
Virtual Private Data Center

Model layanan yang dipilih adalah *Infrastructure as a Service* (IaaS) (Prabowo, Muslim, & Iryanto, 2015), karena secara fundamental IaaS merupakan layanan virtual machine images yang secara fleksibel dapat dikelola oleh pengguna (Viega, 2009) hal ini secara teknis menggantikan fisik server, sumberdaya data center, peralatan jaringan, dan komponen fisik lainnya (Erl et al., 2014). Kelebihan lain model IaaS adalah pengguna layanan dapat dengan mudah mengubah (menambah atau mengurangi) jumlah maupun kapasitas virtual machine sesuai dengan kebutuhan (Erl et al., 2014; Tim Mell, 2009; Viega, 2009).

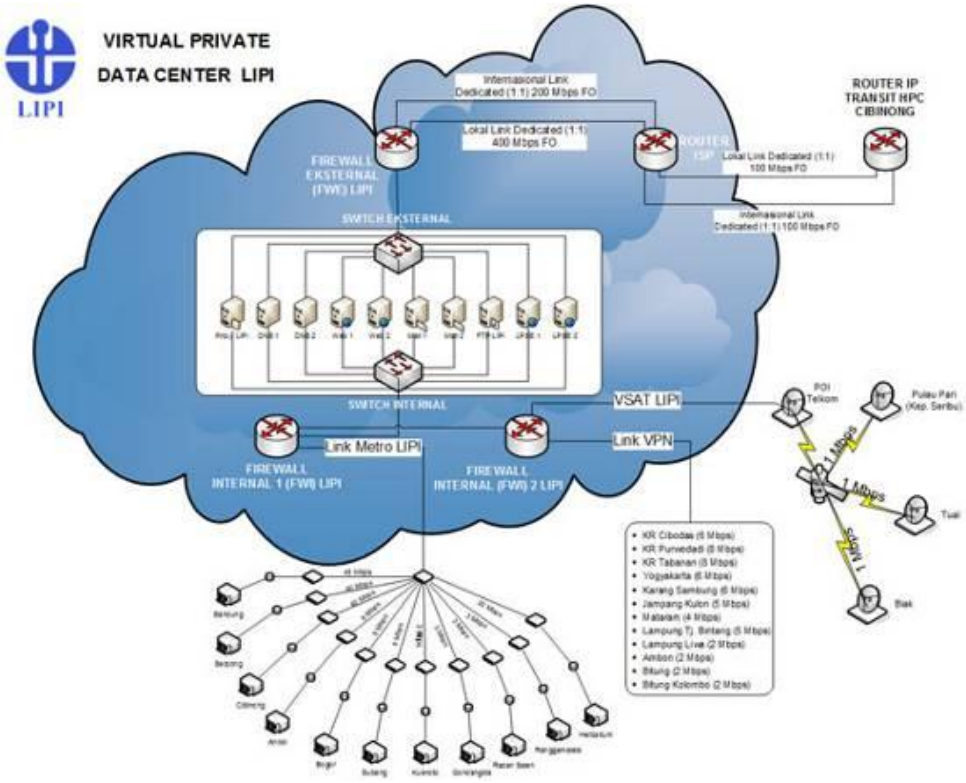
Level kontrol model IaaS lebih tinggi dibandingkan dengan model layanan yang lain Gambar 1. Model SaaS mempunyai level kontrol terhadap penggunaan dan konfigurasi terkait penggunaan, serta metode akses hanya melalui *front-end user interface*. Model PaaS memiliki level kontrol administrative tapi sangat terbatas, platform

yang terkait pengguna dapat dilakukan kontrol secara berbagi dengan penyedia (Erl et al., 2014). Sehingga penggabungan antara model implementasi *private cloud* dan model layanan IaaS akan meningkatkan level kontrol terhadap layanan dan meminimalkan tingkat resiko (Gambar 5).

Konfigurasi virtual *private data center* sama persis dengan kondisi eksisting (Prabowo et al., 2015), yaitu semua *server* (proxy, DNS1-2, Web1-2, mail1-2, FTP, LPSE1-2) dimigrasi menjadi *virtual machine*, tetapi untuk interkoneksi jaringan sudah tidak dibutuhkan lagi sewa *backhaul* yang menampung koneksi dari masing-masing satuan kerja (Gambar 6)



Gambar 5. Perbandingan Level Kontrol dan Tingkat Risiko
Sumber : (Chan et al., 2012)



Gambar 6. Virtual Private Data Center LIPI

Sumber : Biro Umum LIPI dalam (Prabowo et al., 2015)

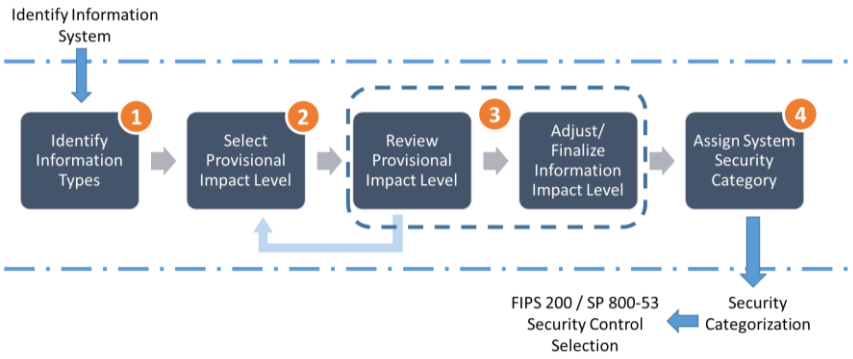
Kategorisasi Sistem Informasi (Tahap I)

Tahapan pertama dalam kerangka kerja manajemen risiko adalah melaksanakan kategorisasi sistem informasi. Dalam tahap ini terdapat 3 kegiatan yaitu :

a. Mengkategorisasikan sistem informasi dan membuat dokumentasi hasil kategorisasi keamanan dalam rencana keamanan;
b. Mendeskripsikan sistem informasi dan membuat dokumentasi hasil deskripsi dalam rencana keamanan;
c. Meregister sistem informasi untuk memudahkan kebutuhan organisasi dalam mengambil sebuah kebijakan;

Kategorisasi keamanan sistem informasi ini menggunakan panduan dari *Federal Information Processing Standards* (FIPS) 199 dan publikasi NIST SP800-60 *Guide for Mapping Types of Information and Information Systems to Security Categories.* Proses yang dilaksanakan ditunjukkan pada Gambar 7, terdapat tahapan masukan, proses dan keluaran.

Hasil identifikasi sistem informasi (*virtual machine*/ server) yang ada pada layanan cloud LIPI adalah : server proxy, server dns, server web, server email, server FTP, server LPSE LIPI, sistem hosting, sistem arsip, sistem fisikanet, sistem NTP, IPSK, D-TERM, dan Sistem Telemetri Sumatran GPS Array (SUGAR). Sistem informasi terdiri dari program komputer dan informasi yang ada didalamnya. Kategorisasi keamanan sistem informasi juga termasuk kategorisasi tipe informasi yang terkandung dalam sistem tersebut. Sehingga hasil kategorisasi tipe informasi yang ada dapat mempengaruhi kategorisasi keamanan sistem informasi. Tidak semua sistem informasi yang ada pada data center dapat dikategorisasikan dalam pembahasan ini karena kepemilikan sistem tersebut tidak semua berada pada wewenang Biro Umum. Kategorisasi yang disampaikan disini adalah sistem informasi yang berada pada wewenang Biro Umum saja. Hasil kategorisasi sistem informasi disederhanakan sesuai Tabel 3 karena keterbatasan.



Gambar 7. Proses Kategorisasi Sistem Informasi
Sumber : NIST SP800-60

Tabel 3. Hasil Kategorisasi Sistem Informasi

No	Nama Sistem Informasi	Kategorisasi (FIPS-199 / NIST SP800-60)										
		Kerahasiaan			Integritas			Ketersediaan			Kategori Dampak	Tipe Informasi
		R	S	T	R	S	T	R	S	T		
1	Server Proxy			x			x		x		Tinggi	C.3.5 Information

No	Nama Sistem Informasi	Kategorisasi (FIPS-199 / NIST SP800-60)									Tipe Informasi
		Kerahasiaan			Integritas			Ketersediaan			Kategori Dampak	
		R	S	T	R	S	T	R	S	T		
												and Technology Management C.3.5
2	Server DNS		x			x		x			Sedang	Information and Technology Management C.3.5
3	Server Web			x			x		x		Tinggi	Information and Technology Management C.3.5
4	Server Email		x			x		x			Tinggi	Information and Technology Management C.3.5
5	Server LPSE-SPSE		x			x		x			Sedang	Information and Technology Management C.3.5
6	Sistem Hosting			x			x	x			Tinggi	Information and Technology Management C.3.5
7	Sistem NTP		x				x			x	Tinggi	Information and Technology Management

Selesi Kontrol Keamanan (Tahap II)

Tahapan kedua dalam kerangka kerja manajemen risiko adalah memilih kontrol keamanan. Dalam tahap ini terdapat 4 kegiatan yaitu :

a. Melakukan identifikasi terkait kontrol keamanan yang akan dijadikan oleh organisasi sebagai *common controls* untuk sistem informasi dan membuat dokumentasi dalam rencana keamanan;
b. Melakukan pemilihan kontrol keamanan untuk sistem informasi dan mendokumentasikan dalam rencana keamanan;
c. Membuat strategi terkait monitoring terhadap efektivitas kontrol keamanan dan perubahan-perubahan yang terjadi dalam operasional sistem informasi;
d. Melakukan telaah dan persetujuan terhadap rencana keamanan sistem informasi.

Seleksi kontrol keamanan sesuai dengan NIST RMF tahap kedua dengan menggunakan panduan *Federal Information Processing Standards* (FIPS) 200 dan NIST *Special Publication* 800-53 R4 *Security and Privacy Controls for Federal Information Systems and Organizations*. Kontrol keamanan secara terstruktur terbagi menjadi 18

rumpun (NIST, 2015), yang dapat dilihat Tabel 4.

Setiap rumpun kontrol keamanan memiliki beberapa turunan dan tambahan yang lebih detail.

Tabel 4. Rumpun Kontrol Keamanan

ID	Uraian	ID	Uraian
AC	*Access Control*	MP	*Media Protection*
AT	*Awareness and Training*	PE	*Physical and Environmental Protection*
AU	*Audit and Accountability*	PL	*Planning*
CA	*Security Assessment and Authorization*	PS	*Personnel Security*
CM	*Configuration Management*	RA	*Risk Assessment*
CP	*Contigency Planning*	SA	*System and Service Acquisition*
IA	*Identification and Authentication*	SC	*System and Communication Protection*
IR	*Incident Response*	SI	*System and Information Integrity*
MA	*Maintenance*	PM	*Program Management*

Sumber : NIST SP800-53

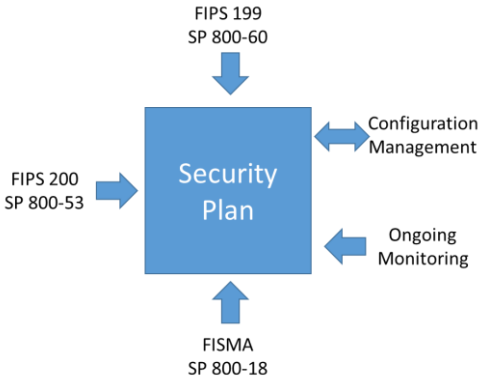
Proses pemilihan kontrol keamanan yang tepat dan sesuai dengan kebutuhan organisasi perlu didahului dengan proses identifikasi informasi dan kategorisasi sistem informasi yang merupakan tahap pertama dari RMF. Selanjutnya pemilihan kontrol keamanan dimulai dengan membuat kontrol awal (*baseline*), tetapi tidak semua kontrol keamanan secara baseline digunakan. Beberapa pertimbangan dalam pemilihan kontrol keamanan adalah : (a) perangkat yang terkait dalam sistem informasi, dalam hal ini ada perangkat yang merupakan tanggungjawab penyedia layanan (perangkat fisik, bangunan, keamanan, dll); (b) kebiasaan organisasi dalam operasional sistem informasi; (c) fungsionalitas sistem informasi; (d) tipe ancaman terhadap organisasi, visi misi organisasi, dan sistem informasi; (e) informasi yang terdapat dalam sistem informasi. Pertimbangan lain adalah kontrol keamanan tersebut dapat diimplementasikan pada organisasi. Sehingga dengan menggabungkan Lampiran D pada NIST SP800-53R4 dengan hasil dari kategorisasi sistem, hasil pemilihan kontrol keamanan dapat dilihat pada Tabel 5 (Karena keterbatasan hanya ditampilkan sebagian kontrol keamanan). Hasil ini masih dapat dilakukan penyesuaian lagi terhadap kebutuhan organisasi berdasarkan pertimbangan pemangku kepentingan yang ada pada organisasi.

Implementasi (Tahap III)

Tahapan ketiga dalam kerangka kerja manajemen risiko adalah mengimplementasi kontrol keamanan. Dalam tahap ini terdapat 2 kegiatan yaitu :

a. Melakukan implementasi kontrol keamanan sistem informasi sesuai rencana keamanan;
b. Mendokumentasikan implementasi kontrol keamanan dalam rencana keamanan dengan kelengkapan berupa deskripsi, fungsi, *input*, *output*, dll.

Lebih detail tahap implementasi kontrol keamanan menggunakan NIST *Special Publication* 800-160, *Systems Security Engineering*. Selain itu sebagai panduan dapat menggunakan NIST Special Publication 800-18 *Revision* 1, *Guide for Developing Security Plans for Federal Information Systems*. Berdasarkan NIST SP800-18R1 proses implementasi kategorisasi sistem informasi dan seleksi kontrol keamanan yang menghasilkan perencanaan keamanan dapat dilihat pada Gambar 8.



Gambar 8. Proses Perencanaan Keamanan
Sumber : NIST SP800-18

Langkah ini merupakan penggabungan antara tahap kesatu dan kedua yang mempertemukan antara sistem informasi yang telah terkategorisasi dengan kontrol keamanan yang telah dipilih. Rencana kontrol keamanan untuk sistem informasi dapat dilihat pada Tabel 6. Selanjutnya berdasarkan tabel tersebut organisasi dapat melakukan eksekusi terhadap kontrol keamanan pada sistem informasi. Tetapi pada penelitian ini langkah yang dapat dilaksanakan hanya sampai dengan tahap pemetaan yang merupakan keluaran dari NIST *Special Publication* 800-18 yaitu perencanaan keamanan yang merupakan bagian dari proses manajemen risiko.

Rekomendasi bagi LIPI

Penelitian ini hanya bisa dilaksanakan sampai dengan tahap III karena keterbatasan. Sistem informasi yang dievaluasi juga terbatas infrastruktur utama yang berada di bawah kewenangan Biro Umum LIPI. Perlu dilakukan implementasi kontrol keamanan sesuai dengan hasil tahap III agar keamanan sistem informasi lebih terjamin dan tindakan pengamanan sesuai dengan panduan. Selain itu agar hasil yang diperoleh lebih komprehensif disarankan untuk melakukan evaluasi keamanan sistem informasi sampai tingkat satuan kerja yang memanfaatkan fasilitas *virtual private cloud* LIPI.

Tabel 5. Seleksi Kontrol Keamanan

KODE	Uraian	*Baseline*			Kerahasiaan			Integritas			Ketersediaan			Kontrol Umum
NO.	Detail Kontrol Keamanan	R	S	T	R	S	T	R	S	T	R	S	T	
AC-1	Access Control Policy and Procedures	x	x	x	x	x	x	x	x	x	x	x	x	x
AC-2	Account Management	x	x	x	x	x	x	x	x	x				x
AC-2(1)	*account management | automated system account management*		x	x	x	x	x	x	x	x				
AC-2(2)	*account management | removal of temporary / emergency accounts*		x	x	x	x	x	x	x	x				
AC-2(3)	*account management | disable inactive accounts*		x	x	x	x	x	x	x	x				
AC-2(4)	*account management | automated audit actions*		x	x	x	x	x	x	x	x				
AC-2(5)	*account management | inactivity logout*			x										x
AC-2(6)	*account management | dynamic privilege management*													
AC-2(7)	*account management | role-based schemes*													
AC-2(8)	*account management | dynamic account creation*				x	x	x	x	x	x	x	x	x	x

Tabel 6. Contoh Rencana Kontrol Keamanan untuk Sistem Informasi

No	Nama Sistem Informasi	Kategorisasi (FIPS-199 / NIST SP800-60)									Kontrol Keamanan (FIPS 200 / NIST SP800-53)	
		Kerahasiaan			Integritas			Ketersediaan			Tipe Informasi	Internal	Eksternal (Penyedia *Cloud*)
		R	S	T	R	S	T	R	S	T			
1	Server Proxy			x			x		x		C.3.5 Information and Technology Management	**Access Control (AC) :** AC-1, AC-2, AC-3, AC-4, AC-5, AC-6, AC-7, AC-10, AC-11, AC-12, AC-17, AC-18, AC-19 **Awareness and Training (AT) :** AT-1, AT-2, AT-3, AT-4 **Security Assessment and Authorization (CA) :** CA-1, CA-2, CA-3, CA-5, CA-6, CA-7, CA-8, CA-9 **Configuration Management (CM) :** CM-1, CM-2, CM-4, CM-4, CM-5, CM-6 **Contingency Planning (CP) :** CP-1, CP-2, CP-3, CP-4, CP-8, CP-9, CP-10 **Identification And Authentication (IA) :** IA-1, IA-2, IA-3, IA-4, IA-5, IA-7, IA-8 **Incident Response (IR) :** IR-1, IR-2, IR-3, IR-4, IR-5, IR-6, IR-7, IR-8 **System Maintenance (MA) :** MA-1, MA-2, MA-3, MA-4 **Security Planning (PL) :** PL-1, PL-2, PL-4, PL-8 **Personnel Security (PS) :** PS-1, PS-2, PS-6, PS-7, PS-8 **Risk Assessment (RA) :** RA-1, RA-2, RA-3, RA-5 **System And Communications Protection (SC) :** SC-1, SC-2, SC-3, SC-4, SC-5, SC-12, SC-13, SC-15, SC-17, SC-23 **System And Information Integrity (SI) :** SI-1, SI-2, SI-3, SI-4, SI-5, SI-6, SI-7, SI-8, SI-10, SI-11, SI-12, SI-16	**Contingency Planning (CP) :** CP-1, CP-2, CP-3, CP-4, CP-8, CP-9, CP-10 **Incident Response (IR) :** IR-1, IR-2, IR-3, IR-4, IR-5, IR-6, IR-7, IR-8 **Media Protection (MP) :** MP-1, MP-2, MP-4, MP-5, MP-6 **Physical and Environmental Protection (PE) :** PE-1, PE-2, PE-3, PE-6, PE-8, PE-9, PE-10, PE-11, PE-12, PE-13, PE-14, PE-15, PE-16, PE-17, PE-18 **Personel Security (PS) :** PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8

PENUTUP

Pelaksanaan manajemen risiko pada penelitian ini menghasilkan beberapa kesimpulan antara lain :

• Berdasarkan evaluasi pada penelitian ini *framework* manajemen risiko yang paling sesuai dengan kondisi pada LIPI yaitu layanan *virtual private data center* berbasis *cloud* adalah NIST *Special Publication* 800-37 Revision 1.

• Sesuai dengan NIST *Framework* seharusnya terdapat enam tahapan yang dilaksanakan dalam proses manajemen risiko, tetapi karena keterbatasan sumberdaya dan waktu, penelitian ini hanya dapat dilaksanakan sampai sebagian tahap ketiga.

Meskipun hanya sampai dengan tahap ketiga, penelitian ini menghasilkan rekomendasi perencanaan keamanan khususnya dalam penggunaan teknologi *cloud computing* yang telah dilaksanakan pada Lembaga Ilmu Pengetahuan Indonesia. Perlu dilakukan tahapan selanjutnya dan implementasi rencana keamanan yang telah disusun agar kemanfaatan teknologi informasi yang berbasis *cloud computing* di LIPI dapat dioptimalkan. Kerangkan kerja NIST merupakan siklus proses manajemen risiko, sehingga tahapan selanjutnya mungkin saja akan berpengaruh terhadap proses yang sudah berjalan.

UCAPAN TERIMA KASIH

Peneliti mengucapkan terima kasih, kepada reviewer, Kepala LIPI, Kepala Balitbang SDM Kominfo, Mitra Bestari, redaksi, dan pihak-pihak yang telah membantu dalam menyelesaikan penelitian ini.

DAFTAR PUSTAKA

Ackermann, T. (2012). *IT Security Risk*.

Alnuem, M., Alrumaih, H., & Al-Alshaikh, H. (2015). A Comparison Study of Information Security Risk Management Frameworks in Cloud Computing. *International Journal On Advances in Software*, *6*, 103–109.

Andriyani, R., Ulfa, M., & Cholil, W. (2013). Pengukuran Risiko Pada Penerapan Cloud Computing Untuk Sistem Informasi (Studi Kasus Universitas Bina Darma). *Prosiding Seminar Nasional Teknologi Informasi Komunikasi Dan Manajemen*, *53*(9), 1689–1699. https://doi.org/10.1017/CBO9781107415324.004

Ardagna, D. (2015). Cloud and Multi-cloud Computing: Current Challenges and Future Applications. *2015 IEEE/ACM 7th International Workshop on Principles of Engineering Service-Oriented and Cloud Systems*, 1–2. https://doi.org/10.1109/PESOS.2015.8

Avram, M. G. (2014). Advantages and Challenges of Adopting Cloud Computing from an Enterprise Perspective. *Procedia Technology*, *12*, 529–534. https://doi.org/10.1016/j.protcy.2013.12.525

Carstensen, J., Golden, B., & Morgenthal, J. (2012). *Cloud Computing Assessing The Risk*. Cambridgeshire: IT Governance Publishing.

Catteddu, D., & Hogben, G. (2009). Cloud Computing: Benefit, Risk and Recommendations for Infomation Security. *ENISA*.

Chan, W., Leung, E., & Pili, H. (2012). Enterprise risk management for cloud computing. *Committee of Sponsoring Organizations of the Treadway Commission*, 4. Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:COSO+Enterprise+Risk+Management+for+Cloud+Computing#0

Cloud Security Alliance. (2013). The Notorious Nine. Cloud Computing Top Threats in 2013. *Security*, (February), 1–14. Retrieved from http://www.cloudsecurityalliance.org

Cordero, S. (2016). Cloud Controls Matrix Working Group. Retrieved April 22, 2016, from https://cloudsecurityalliance.org/group/cloud-controls-matrix/

Djemame, K., Armstrong, D., Guitart, J., & Macias, M. (2014). A Risk Assessment Framework for Cloud Computing. *IEEE Transactions on Cloud Computing*, *PP*(99), 1–1. https://doi.org/10.1109/TCC.2014.2344653

Erl, T., Mahmood, Z., & Puttini, R. (2014). *Cloud Computing : Concept, Technology, and Architecture* (Fourth). Massachusetts: Prentice Hall.

Frantsvog, D., Seymour, T., & John, F. (2012). Cloud Computing. *International Journal of Management & Information Systems – Fourth Quarter*, *16*(4), 317–324. Retrieved from http://cgi.di.uoa.gr/~ad/MDE556/Papers/palis-ic10.pdf

Frost, & Sullivan. (2015). *The New Language of Cloud Computing*. Retrieved from https://dailysocial.net/wire/hasil-studi-f5-dan-frost-sullivan-merangkum-tren-serta-perkembangan-pemanfaatan-solusi-berbasis-cloud-di-asia-pasifik-dalam-kerangka-a-b-c-d

Furht, B. (2010). Cloud Computing Fundamentals. In *Handbook of Cloud Computing* (pp. 3–19). Boston, MA: Springer US. https://doi.org/10.1007/978-1-4419-6524-0_1

Hardy, K. (2015). *Enterprise Risk Management: A Guide for Government Professionals*.

Hausman, K., Cook, S. L., & Sampaio, T. (2013). *Cloud Essential*. Canada: SYBEX. https://doi.org/10.1073/pnas.0703993104

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research 1. *Design Science in IS Research MIS Quarterly*, *28*(1), 75–105. https://doi.org/10.2307/25148625

Hidayat, E. W. (2013). Risk Assessment pada Manajemen Resiko Penerapan Teknologi Cloud Computing bagi Pemerintah Daerah. *Jurnal LPKIA*, *2*(2).

Hsu, P.-F., Ray, S., & Li-Hsieh, Y.-Y. (2014). Examining cloud computing adoption intention, pricing mechanism, and deployment model. *International Journal of Information Management*, *34*(4), 474–488. https://doi.org/10.1016/j.ijinfomgt.2014.04.006

Hubbard, D. W. (2009). *The Failure of Risk Management: Why It's Broken and How to Fix It*. *Journal of Chemical Information and Modeling* (Vol. 53). New Jersey: Wiley - John Wiley & Sons, Inc. https://doi.org/10.1017/CBO9781107415324.004

Iorga, M. (2015). Cloudy with Showers of Business Opportunities adn a Good Chance of Security and Accountability.

Iorga, M., & Karmel, A. (2015). Managing Risk in a Cloud Ecosystem. *IEEE Cloud Computing*, *2*, 51–57.

Iorga, M., & Scarfone, K. (2016). Using a Capability-Oriented Methodology to Build Your Cloud Ecosystem. *IEEE Cloud Computing*, 58–63.

Kauffman, R. J., Ma, D., & Yu, M. (2014). A metrics suite for firm-level cloud computing adoption readiness. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *8914*, 19–35. https://doi.org/10.1007/978-3-319-14609-6_2

Khrisna, A., & Harlili. (2014). Risk Management Framework With COBIT 5 And Risk Management Framework for Cloud Computing Integration, 103–108.

Kuligowski, C. (2009). Comparison of IT Security Standards. *Masters of Science Information Security and Assurance*, 65. Retrieved from http://www.federalcybersecurity.org/CourseFiles/WhitePapers/ISOvNIST.pdf

Kundra, V. (2011). Federal Cloud Computing Strategy. Washington: U.S. Chief Information Officer.

Luna, J., Suri, N., Iorga, M., & Karmel, A. (2015). Leveraging the Potential of Cloud Security Service-Level Agreements through Standards. *IEEE Cloud Computing*, *2*(3), 32–40. https://doi.org/10.1109/MCC.2015.52

Meiningsih, S., Rianto, Y., Idris, H. M., Samekto, I., Sari, D., A, V. H., … Maharani, D. A. (2013). *Komunikasi dan Informatika Indonesia - Buku Putih 2013*.

National Institute of Standards and Technology. (2011). Managing Information Security Risk. *NIST Special Publication 800-39*, (March), 88. https://doi.org/10.6028/NIST.SP.800-39

NIST. (2010). Guide for Applying the Risk Management Framework to Federal Information Systems. *NIST Special Publication 800-37*, *Rev 1*(February), 93. https://doi.org/NIST Special Publication 800-37 R1

NIST. (2015). Security and privacy controls for federal information systems and organizations. *NIST Special Publication 800-53*, (800–53 revision 4). https://doi.org/http://dx.doi.org/10.6028/NIST.SP.800-53r4

Obi, T. (2014). *2014 WASEDA – IAC 10th International E-Government Ranking Survey*. Tokyo.

Obi, T. (2015). *2015 WASEDA – IAC International E-Government Ranking Survey*. Tokyo.

Obi, T. (2016). *2016 WASEDA – IAC INTERNATIONAL E-GOVERNMENT RANKING SURVEY*.

Paquette, S., Jaeger, P. T., & Wilson, S. C. (2010). Identifying the security risks associated with governmental use of cloud computing. *Government Information Quarterly*, *27*(3), 245–253. https://doi.org/10.1016/j.giq.2010.01.002

Prabowo, W. S., Muslim, M. H., & Iryanto, S. B. (2015). Government Virtual Private Data Center based on Cloud Computing (Empirical Study on Indonesian Institute of Sciences - LIPI). *Jurnal Penelitian Dan Pengembangan Komunikasi Dan Informatika2*, *6*(2), 1–14.

Ravi, T. N., & Sankar, S. (2015). Measuring the Security Compliance Using Cloud Control Matrix. *Middle-East Journal of Scientific Research*, *23*(8), 1797–1803. https://doi.org/10.5829/idosi.mejsr.2015.23.08.22482

Samani, R., Honan, B., & Reavis, J. (2015). *CSA Guide to Cloud Computing*. *CSA Guide to Cloud Computing*. https://doi.org/10.1016/B978-0-12-420125-5.00008-X

Sendi, A. S., & Cheriet, M. (2014). Cloud Computing: A Risk Assessment Model. *2014 IEEE Int. Conf. Cloud Eng.*, 147–152. https://doi.org/10.1109/IC2E.2014.17

Spafford, G. (2003). The benefits of standard IT governance frameworks. *IT Management. April*, 11–12. Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:The+Benefits+of+Standard+IT+Governance+Frameworks#0

Stine, K., Kissel, R., Barker, W. C., Lee, A., & Fashlsing, J. (2008). SP 800-60 Volume I : Guide for Mapping Types of Information and Information Systems to Security Categories. *National Institute of Standards and Technology*, *II*(August).

Susanto, H., Almunawar, M., & Tuan, Y. (2011). Information security management system standards: A comparative study of the big five. *International Journal of Electrical Computer Sciences IJECS-IJENS*, *11*(5), 23–29.

Tim Mell, P. G. (2009). Draft NIST Working Definition of Cloud Computing. *National Institute of Standards and Technology*, *53*, 50. https://doi.org/10.1136/emj.2010.096966

Viega, J. (2009). Cloud computing and the common man. *Computer*, *42*(8), 106–108. https://doi.org/10.1109/MC.2009.252

Xie, F., Peng, Y., Zhao, W., Chen, D., Wang, X., & Huo, X. (2012). A risk management framework for cloud computing. *2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems*, 476–480. https://doi.org/10.1109/CCIS.2012.6664451

Yaumi, N., & Kridanto, S. (2012). Risiko pada Penerapan Cloud Computing untuk Sistem Informasi di Perguruan Tinggi Menggunakan Framework COSO ERM dan FMEA (studi kasus: ITB. *ITB*, *1*(2), 1–6. Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Model+Manajemen+Risiko+pada+Penerapan+Cloud+Computing+untuk+Sistem+Informasi+di+Perguruan+Tinggi+Menggunakan+Framework+COSO+ERM+dan+FMEA+(+studi+kasus+:+ITB+)#0

Zhang, W., & Chen, Q. (2010). From E-government to C-government via Cloud Computing. *2010 International Conference on E-Business and E-Government*, 679–682. https://doi.org/10.1109/ICEE.2010.177

Zhao, G. (2012). Holistic framework of security management for cloud service providers. *IEEE 10th International Conference on Industrial Informatics*, 852–856. https://doi.org/10.1109/INDIN.2012.6301237

Zissis, D., & Lekkas, D. (2011). Securing e-Government and e-Voting with an open cloud computing architecture. *Government Information Quarterly*, *28*(2), 239–251. https://doi.org/10.1016/j.giq.2010.05.010