Jurnal IPTEK-KOM (Jurnal Ilmu Pengetahuan dan Teknologi Komunikasi) eISSN 2527 - 4902
Vol. 22 No. 2, Desember 2020: 207 - 222

Manajemen Risiko Teknologi Informasi pada *e-Government*: Ulasan Literatur Sistematis

Information Technology Risk Management on e-Government: Systematic Literature Review

Alifiani Kurniati[1], Lukito Edi Nugroho[2], Muhammad Nur Rizal[3]
[1,2,3]Departemen Teknik Elektro dan Teknologi Informasi, Universitas Gadjah Mada
Jalan Grafika 2, Kampus UGM, Yogyakarta

[1]alifiani.kurniati@mail.ugm.ac.id, [2]lukito@ugm.ac.id, [3]mnrizal@ugm.ac.id

Naskah diterima: 17 Oktober 2020, direvisi: 18 November 2020, disetujui: 14 Desember 2020

Abstract

Risk management is used as a basic planning and decision making by management, optimizing the use of resources, and minimizing the risks which could harm the organization. The Implementation of risk management in e-government is used to minimize risks and reduce negative impact on e-government implementation. The aim of this study is to make a systematic literature review on the implementation of information technology risk management according to standards in e-government. From the content and descriptive analysis of the literature, it can be concluded that the implementation of risk management in non-profit organizations (government) is influenced by information technology resources planning, management, policy andregulations and also organizational performance. The risk management process in e-government adopts several standards issued by the International Standards Organization (ISO). Additionally, the implementation of the risk management process can be integrated according to the conditions and organizational needs.

Keywords: *literature review, risk management, e-government, International Standard Organization* (ISO)*.*

Abstrak

Manajemen Risiko digunakan sebagai dasar perencanaan dan pengambilan keputusan oleh pimpinan, mengoptimalkan pemanfaatan sumber daya yang dimiliki, serta meminimalisir terjadinya risiko yang dapat merugikan organisasi. Implementasi manajemen risiko pada e-government digunakan untuk meminimalisir risiko serta mengurangi dampak negatif terhadap implementasi e-government. Penelitian ini bermaksud melakukan tinjauan literatur sistematis mengenai implementasi manajemen risiko teknologi informasi yang sesuai standar dalam e-government. Dari hasil analisis konten dan deskriptif terhadap literatur, disimpulkan bahwa implementasi manajemen risiko pada organisasi non-profit (pemerintah) dipengaruhi oleh perencanaan sumber daya teknologi informasi, manajemen, kebijakan dan regulasi serta kinerja organisasi. Proses manajemen risiko pada e-

government mengadopsi beberapa standar yang dikeluarkan oleh International Standard Organization (ISO), dan implementasinya dapat diintegrasikan sesuai dengan kondisi dan kebutuhan organisasi.

Kata kunci: ulasan literatur, manajemen risiko, *e-government, International Standard Organization (ISO).*

PENDAHULUAN

Sistem digitalisasi penyelenggaraan pemerintah yang dikenal dengan *electronic government* atau *e-government* merupakan dampak positif dari kemajuan teknologi informasi dan komunikasi (TIK) di Indonesia. *E-government* digunakan sebagai media transformasi layanan publik yang diharapkan dapat meningkatkan efisiensi dan efektifitas kinerja pemerintah. Pada tahun 2019, Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi (KemenPAN-RB) telah melakukan evaluasi terhadap penyelenggaraan *e-government* yang dikenal dengan Sistem Pemerintahan Berbasis Elektronik (SPBE). Hasil evaluasi tingkat kematangan penyelenggaraan SPBE pada 637 Kementerian, lembaga, dan Pemerintah Daerah menunjukkan nilai 2,18 atau berpredikat 'cukup' (KemenPAN-RB 2020). Hasil ini meningkat dibandingkan dengan hasil evaluasi tahun 2018 sebesar 1,98 di mana masih dibawah target yaitu sebesar 2,6. Hal tersebut menunjukkan bahwa masih terdapat permasalahan dalam implementasi SPBE (Kementerian PAN RB 2020).

Permasalahan pertama yaitu tata kelola SPBE yang belum terpadu. Masih banyak instansi baik di tingkat pemerintah pusat maupun daerah yang memiliki aplikasi sejenis, contohnya aplikasi di bidang kepegawaian. Masing-masing instansi menganggarkan dan mengembangkan sendiri aplikasi tersebut, sehingga berdampak pada pemborosan dan duplikasi anggaran TIK (Kementerian PAN RB 2020). Permasalahan kedua yaitu layanan SPBE yang belum optimal. Layanan publik maupun layanan administrasi pemerintah masih menggunakan aplikasi yang berdiri sendiri sehingga mengakibatkan layanan SPBE belum efektif dan efisien (Kementerian PAN RB 2020). Permasalahan ketiga yaitu terbatasnya SDM yang memiliki pengetahuan tentang TIK. Minimnya SDM TIK yang mendukung penerapan SPBE dapat mengakibatkan terganggunya penyediaan layanan SPBE (Kementerian PAN RB 2020). Selain ketiga permasalahan tersebut, perkembangan TIK 4.0 juga merupakan faktor kunci keberhasilan implementasi SPBE. Beberapa tren TIK 4.0 seperti *artificial intelligence*, *big data analytics*, *internet of things*, dan *cloud computing* diharapkan mampu mendukung penerapan SPBE (Tupa, Simota, and Steiner 2017)

Beberapa permasalahan di atas serta perkembangan tren TIK 4.0 dapat menimbulkan beberapa risiko dalam implementasi *e-government* khususnya SPBE di Indonesia. Risiko-risiko yang timbul hendaknya dikelola melalui manajemen risiko untuk meningkatkan kemungkinan keberhasilan implementasi *e-government* (Kementerian PAN RB 2020). Implementasi manajemen risiko pada organisasi *non-profit* (pemerintah) dalam mengelola risiko memberikan beberapa keuntungan antara lain sebagai dasar perencanaan sumber daya teknologi informasi dan *decision support system* bagi pimpinan serta meningkatkan kinerja operasional dilihat dari *maturity level* proses manajemen risiko (Oliveira, Augusto, and Marins 2017; Callahan and Soileau 2017; Simota, Tupa*, and Steiner 2018). Keberhasilan implementasi manajemen risiko pada *e-government* dipengaruhi oleh beberapa faktor antara lain manajemen, kebijakan, regulasi pemerintah, serta

manajemen kinerja organisasi (Rampini, Takia, and Berssaneti 2019; Fraser and Simkins 2016). Dalam hal regulasi, Kementerian PAN-RB telah menyusun pedoman tentang manajemen risiko yang tertuang dalam Peraturan Menteri PAN-RB Nomor 5 Tahun 2020 sebagai dasar hukum bagi seluruh instansi dalam mengimplementasikan manajemen risiko. Beberapa standar implementasi manajemen risiko khususnya di organisasi pemerintah banyak diadopsi sesuai dengan kondisi organisasi seperti sumber daya TI yang dimiliki, manajemen, kebijakan dan regulasi (Barafort, Mesquida, and Mas 2018).

Beberapa penelitian mengenai standar implementasi manajemen risiko dalam *e-government* antara lain ISO 31000 pada manajemen risiko proyek TI (Olechowski et al. 2016), *software lifecycle* (Masso et al. 2020), ISO 27000 pada manajemen risiko keamanan informasi (Fikri et al. 2019; Brunner et al. 2020), *cloud computing* (Ali et al. 2020) serta COBIT sebagai *tools* perhitungan *maturity level* manajemen risiko *e-government* (Joshi et al. 2018). Implementasi manajemen risiko TI mengadopsi standar ISO 31000-*series* sebagai panduan manajemen risiko secara umum berdasarkan prinsip, kerangka kerja, dan proses. Manajemen risiko menjadi bagian dalam manajemen proyek TI sebagai alat untuk pengambilan keputusan yang sistematis berdasarkan sebelas prinsip manajemen risiko (Olechowski et al. 2016). Manajemen risiko juga diimplementasikan pada *software lifecycle* untuk menghasilkan pengawasan dan tanggung jawab yang tepat serta meningkatkan efektifitas dan efisiensi *software lifecycle* (Masso et al. 2020). Risiko yang berkaitan dengan keamanan informasi dapat timbul dalam implementasi *e-government*, salah satunya akuntabilitas dan transparansi pelaporan atau informasi (Kasma, Sutikno, and Surendro 2019). Langkah praktis pengelolaan risiko keamanan informasi adalah melalui manajemen risiko keamanan informasi yang bertujuan memberikan perlindungan terhadap informasi dan aset organisasi (Brunner et al. 2020). Penilaian risiko keamanan informasi mengadopsi beberapa standar keamanan informasi ISO 27000-*series,* National Institute of Standards and Technology (NIST) SP 800-301, dan disesuaikan dengan kondisi organisasi (Fikri et al. 2019). Di era industri 4.0, *cloud computing* telah banyak digunakan di sektor pemerintah, sehingga keamanannya turut menjadi bagian dalam manajemen risiko. Model keamanan *cloud computing* yang diusulkan antara lain keamanan data, penilaian risiko, peraturan dan kepatuhan, serta *requirement* (Ali et al. 2020).

Penelitian mengenai implementasi standar manajemen risiko pada *e-government* lebih berfokus pada integrasi standar manajemen risiko dalam proses penilaian risiko. Proses penilaian risiko menggunakan metode *Design Science Research Methodology* (DSRM) yang bertujuan untuk menciptakan model atau metode baru yang lebih inovatif dan mendukung tujuan organisasi (Barafort, Mesquida, and Mas 2018). Di sisi lain, banyaknya organisasi pemerintah yang telah berinvestasi terhadap pengamanan informasi dan aset TI menimbulkan beberapa tantangan dalam proses penilaian risiko keamanan informasi sehingga diperlukan taksonomi atau metode penilaian risiko yang tepat dan akurat (Shameli-Sendi, Aghababaei-Barzegar, and Cheriet 2016).

Ulasan literatur yang telah ada sebelumnya fokus pada implementasi standar manajemen risiko *e-government* atau teknik penilaian risikonya. Kajian literatur ini tidak hanya memberikan informasi mengenai implementasi standar manajemen risiko pada *e-government* maupun teknik penilaian risiko akan tetapi memberikan informasi mengenai keuntungan implementasi manajemen risiko serta faktor-faktor penentu keberhasilan implementasi manajemen risiko pada *e-government*. Dengan ulasan literatur ini, organisasi pemerintah dapat mengetahui pentingnya implementasi manajemen risiko dan menjadikannya sebagai langkah utama dalam meminimalisir risiko yang akan terjadi dalam implementasi *e-government*.

METODE

Metode yang digunakan pada kajian ini adalah ulasan literatur. Ulasan literatur akan mengidentifikasi, menganalisis dan menafsirkan penelitian yang relevan mengenai manajemen risiko teknologi informasi dan memiliki hubungan dengan pertanyaan penelitian (*research question*). Ulasan literatur sistematis terdiri dari tiga fase (Kitchenham and Charters 2007) yaitu:

1. *Planning the review*. Tujuan dari fase ini adalah untuk mengidentifikasi kebutuhan dari ulasan literatur, mendefinisikan pertanyaan penelitian (*research question*), serta mengembangkan aturan untuk ulasan literatur.
2. *Conducting the review.* Tujuan dari fase ini adalah mengidentifikasi artikel, menyeleksi artikel, menilai kualitas dari penelitian yang terpilih, mengekstraksi, dan mensintesis data.
3. *Reporting the review*. Tujuan dari fase ini adalah membuat dokumen yang memberikan penjelasan mengenai hasil dari ulasan literatur yang telah dilakukan.

Panduan dalam melakukan kajian ini adalah penelitian mengenai manajemen risiko teknologi informasi pada implementasi *e-government*. Untuk dapat menentukan penelitian yang relevan maka digunakan empat pertanyaan penelitian yang dapat menjawab pertanyaan penelitian tentang bagaimana implementasi manajemen risiko teknologi informasi pada *e-government* dan standar yang digunakan. Pertanyaan penelitian (*research question*) dan motivasi yang akan memandu dalam melakukan ulasan literatur dapat dilihat pada Tabel 1.

Tabel 1. Pertanyaan Penelitian (*Research Question*)

	Pertanyaan Penelitian	**Motivasi**
RQ1	Apa saja keuntungan implementasi manajemen risiko?	Menentukan keuntungan implementasi manajemen risiko dalam organisasi *non-profit* (pemerintah)
RQ2	Apa saja faktor yang mempengaruhi keberhasilan implementasi manajemen risiko?	Menentukan faktor-faktor yang dapat mempengaruhi implementasi manajemen risiko di sektor pemerintah
RQ3	Apa saja penelitian terkait standar implementasi manajemen risiko *e-government*?	Menentukan standar yang dapat digunakan dalam implementasi manajemen risiko
RQ4	Bagaimana implementasi standar dan *framework* tersebut dalam proses manajemen risiko *e-government*?	Mengetahui implementasi standar dalam proses manajemen risiko

Sumber: diadaptasi dari Kitchenham and Charters (2007)

Setelah mendefinisikan pertanyaan penelitian, langkah selanjutnya adalah mencari artikel ilmiah di *database* ScienceDirect dan IEEXplore tentang manajemen risiko teknologi informasi di organisasi *non-profit* (pemerintah) dengan rentang waktu antara tahun 2015 sampai dengan 2020. Strategi pencarian literatur menggunakan kata kunci "*risk management*" AND "*information technology*" AND "*e-government*". Setelah melakukan pencarian literatur pada *database* langkah selanjutnya adalah seleksi hasil penelitian yang dilakukan melalui:

1. Identifikasi penelitian melalui judul, abstrak, dan kata kunci
2. Penerapan *inclusion* dan *exclusion* kriteria
3. Penilaian kualitas dari jurnal terpilih

Inclusion criteria (IC) yang ditetapkan adalah:

IC1 : Artikel ditulis dalam bahasa inggris dan membahas mengenai manajemen risiko pada organisasi *non-profit* (pemerintah) yang menerapkan layanan teknologi informasi (*e-government*).

IC2 : Artikel diterbitkan dalam lima tahun terakhir (2015 sampai dengan 2020).

IC3 : Artikel yang menjelaskan mengenai keuntungan dan faktor yang mempengaruhi implementasi manajemen risiko TI pada organisasi *non-profit* (pemerintah).

Sedangkan *exclusion criteria* (EC) meliputi:

EC1 : Artikel yang berhubungan dengan manajemen risiko pada perusahaan swasta/bisnis dan perbankan.
EC2 : Artikel mengenai manajemen risiko diluar bidang teknologi informasi.
EC3 : Artikel yang tidak berkontribusi pada sektor pemerintah.

Langkah selanjutnya adalah menilai kualitas dari jurnal yang terseleksi dengan menetapkan kriteria kualitas (*quality criteria*). Sistem penilaian dibuat untuk setiap pertanyaan yang diterapkan pada semua artikel dengan menggunakan nilai antara 0 sampai dengan 3. Adapun *quality criteria*-nya sebagai berikut:

QC1 : Apakah artikel memuat deskripsi lengkap mengenai aktifitas yang didukung oleh manajemen risiko teknologi informasi? (Jika Ya nilai 1, jika Sebagian nilai 0.5, jika tidak nilai 0)
QC2 : Apakah artikel menjelaskan mengenai proses manajemen risiko teknologi informasi pada sektor pemerintah? (Jika Ya nilai 1, jika Sebagian nilai 0.5, jika tidak nilai 0)
QC3 : Apakah artikel dipublikasikan pada jurnal atau *conference* yang bereputasi? (Jika Ya nilai 1, jika tidak nilai 0)

HASIL DAN PEMBAHASAN

Dari pencarian literatur dengan menerapkan kata kunci pencarian yang telah ditetapkan, didapat 207 literatur. Literatur tersebut meliputi 75 litertaur bersumber dari ScienceDirect dan 132 literatur bersumber dari IEEEXplore. Literatur yang terpilih kemudian diseleksi kembali dengan menerapkan *inclusion* dan *exclusion criteria* sehingga diperoleh 20 artikel. Proses seleksi artikel dapat dilihat pada Tabel 2.

Tabel 2. Jumlah Literatur Primer

Sumber	Tahap 1	Tahap 2			Tahap 3
	kata kunci pencarian	EC1	EC2	EC3	Seleksi akhir
Sciencedirect	132	73	16	31	12
IEEE *Xplore*	75	35	5	28	8
Total	**207**				**20**

Sumber: Hasil olah data penelitian

Tahap terakhir dari pemilihan artikel adalah penilaian kualitas dengan menerapkan *quality criteria* (QC) pada masing-masing artikel. Proses ini tidak mengurangi artikel yang telah dipilih tetapi digunakan sebagai referensi dalam penelitian mendatang. Hasil penilaian kualitas disajikan pada Tabel 3.

Tabel 3. Penilaian Kualitas Artikel

No	Penulis	Judul	QC1	QC2	QC3	Nilai total
1	Akiyat et al. (2019)	*Modelling Risk Management Process According to ISO Standard*	1	1	1	3
2	Ali et al. (2020)	*Assessing Information Security Risks in the Cloud: A Case Study of Australian Local Government Authorities*	1	1	*1*	3
3	Alreemy et al. (2016)	*Critical Success Factors* (CSFs) *for Information Technology Governance* (ITG)	1	1	1	3
4	Barafort et al. (2018)	*Integrated Risk Management Process Assessment Model for IT Organizations Based on ISO 31000 in an ISO Multi-Standards Context*	0.5	0.5	1	2
5	Brunner et al. (2020)	*Risk Management Practices in Information Security*	0.5	0.5	1	2
6	Callahan et al. (2017)	*Does Enterprise Risk Management Enhance Operating Performance?*	1	1	1	3
7	Fazlida et al. (2015)	*Information Security: Risk, Governance and Implementation Setback*	0.5	0.5	1	2
8	Fikri et al. (2019)	*Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organization: Case Study of ZZZ Information System Application in ABC Agency*	0.5	1	1	2.5
9	Fraser et al. (2016)	*The Challenges of and Solutions for Implementing Enterprise Risk Management*	1	1	1	3
10	Joshi et al. (2018)	*Explaining IT Governance Disclosure through the Constructs of IT Governance Maturity and IT Strategic Role*	0.5	0.5	1	2
11	Kasma et al. (2019)	*Design of E-Government Security Governance System Using COBIT 2019: (Trial Implementation in Badan XYZ)*	0.5	1	1	2.5
12	Maingak et al. (2018)	*Information Security Assessment Using Iso / Iec 27001 : 2013 Standard*	0.5	0.5	1	2
13	Masso et al. (2020)	*Risk Management in the Software Life Cycle: A Systematic Literature Review*	1	0.5	1	2.5
14	Olechowski et al. (2016)	*The Professionalization of Risk Management: What Role Can the ISO 31000 Risk Management Principles Play?*	0.5	0.5	1	2
15	Oliveira et al. (2017)	*The ISO 31000 Standard in Supply Chain Risk Management*	0.5	0.5	1	2
16	Rampini et al. (2019)	*Critical Success Factors of Risk Management with the Advent of ISO 31000 2018 - Descriptive and Content Analyzes*	1	1	1	3
17	Shakibazad et al. (2020)	*New Method for Assets Sensitivity Calculation and Technical Risks Assessment in the Information Systems*	1	1	1	3
18	Shameli-sendi et al. (2016)	*Taxonomy of Information Security Risk Assessment (ISRA)*	1	0.5	1	2.5

No	Penulis	Judul	QC1	QC2	QC3	Nilai total
19	Simota et al. (2018)	*Risk Management to Enhance Performance in the Construction SME Sector; Theory and Case Study*	0.5	0.5	1	2
20	Tupa et al. (2017)	*Aspects of Risk Management Implementation for Industry 4.0*	1	0.5	1	2.5

Sumber: Hasil olah data penelitian

RQ1: Apa saja keuntungan implementasi manajemen risiko?

Tabel 4. Keuntungan Implementasi Manajemen Risiko

Penulis	Keuntungan Manajemen Risiko
Tupa et al. (2017)	Manajemen risiko digunakan sebagai prinsip dasar pengukuran kinerja dan mendukung efektivitas kinerja organisasi.
Simota et al. (2018)	Manajemen risiko yang terintegrasi dengan manajemen kinerja dapat meningkatkan kinerja organisasi.
Oliveira et al. (2017)	Manajemen risiko sebagai dasar penanganan risiko organisasi, perencanaan organisasi, dan *decision support system* oleh pimpinan.
Callahan et al. (2017)	Meningkatkan kinerja operasional dilihat dari tingkat kematangan (*maturity level*) proses dan layanan organisasi.

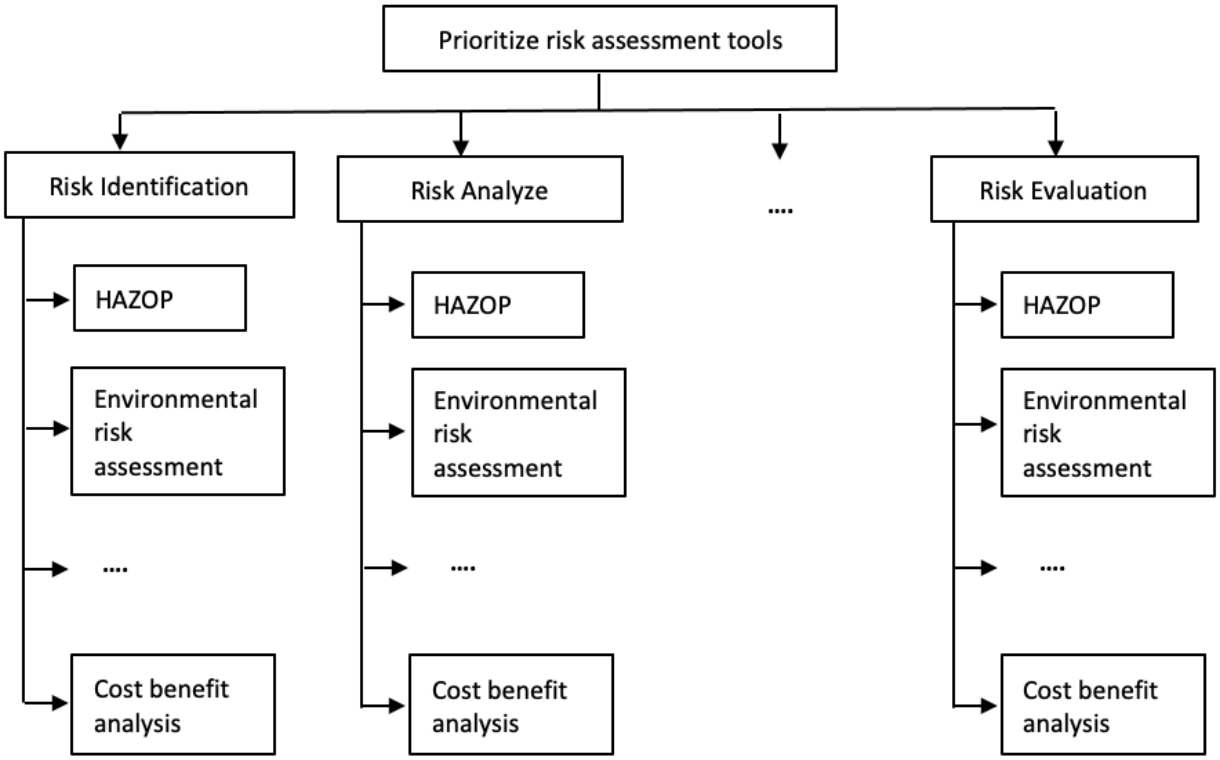
Sumber: Hasil olah data penelitian

Dari Tabel 4 dapat diketahui bahwa keuntungan implementasi manajemen risiko pada organisasi *non-profit* (pemerintah) meliputi sebagai dasar perencanaan sumber daya teknologi informasi, *decision support system* bagi pimpinan, serta meningkatkan kinerja operasional jika dilihat dari *maturity level* proses manajemen risiko.

Pengukuran kinerja merupakan hal yang sangat penting dalam organisasi untuk mengetahui kesenjangan kinerja saat ini dengan kinerja yang diinginkan untuk memberikan motivasi kepada organisasi dalam meningkatkan kinerjanya. Desain *framework* manajemen risiko yang tepat dapat membantu proses identifikasi *Key Performance Indicator* (KPI) dan *Key Risk Indicator* (KRI) serta menyusun langkah-langkah mitigasi risiko. Manajemen risiko diimplementasikan secara berkala dalam organisasi sebagai prinsip dasar pengukuran kinerja dan mendukung efektivitas kinerja organisasi (Tupa, Simota, and Steiner 2017).

Manajemen kinerja merupakan bagian penting dari organisasi yang disusun dalam rencana jangka panjang organisasi yang mencakup pengukuran dan pelaksanaan *Key Performance Indicator* (KPI), dukungan teknologi informasi, serta dukungan pengolahan data dan pelaporan. Manajemen risiko merupakan suatu proses pendekatan sistematis dalam penilaian dan mitigasi risiko untuk memastikan tujuan dari organisasi tercapai. Manajemen risiko yang efektif dan terintegrasi dengan manajemen kinerja dapat meningkatkan kinerja organisasi (Simota, Tupa*, and Steiner 2018).

Proses penilaian risiko merupakan hal yang sangat penting dalam menentukan *Key Risk Indicator* (KRI) organisasi. Metode yang dapat digunakan antara lain *Analytic Hierarchy Process* (AHP) di mana prioritas risiko diperoleh dari kriteria-kriteria yang dinilai atau dipilih oleh pemilik risiko. KRI yang telah disusun berperan besar dalam menentukan indikator kinerja organisasi (*Key Performance Indicator*, KPI). Hasil dari manajemen risiko berdasarkan prioritas risiko dapat digunakan oleh manajemen sebagai dasar penanganan risiko organisasi, perencanaan organisasi, dan pendukung keputusan sehingga segala keputusan yang diambil oleh pimpinan berdasarkan prioritas risiko (Oliveira, Augusto, and Marins 2017).



Gambar 1. Hierarki pemilihan prioritas risiko (Oliveira, Augusto, and Marins 2017)

Selain itu, proses manajemen risiko yang tepat (identifikasi, penilaian, serta respon terhadap risiko) sangat mempengaruhi tingkat kematangan (*maturity level*) implementasi manajemen risiko serta kinerja organisasi baik itu *Return of Asset* (ROA) maupun *Return of Equity* (ROE). Walaupun tidak semua risiko dapat diprediksi, akan tetapi implementasi manajemen risiko dapat meminimalisir terjadinya risiko yang dapat memberikan dampak merugikan terhadap organisasi serta mengelola respon terhadap risiko tersebut. Manajemen dan jajaran direksi memiliki peran terbesar dalam mengadopsi dan menerapkan proses manajemen risiko organisasi, hasil dari manajemen risiko dapat memberikan tambahan wawasan bagi manajemen dalam mengambil keputusan yang berkaitan dengan investasi organisasi (Callahan and Soileau 2017).

RQ2: Apa saja faktor yang mempengaruhi keberhasilan implementasi manajemen risiko?

Tabel 5. Faktor Yang Mempengaruhi Implementasi Manajemen Risiko

Penulis	Faktor-faktor
Rampini et al. (2019)	Manajemen kinerja, Kemitraan (kerjasama dengan swasta), Perencanaan sumber daya
Alreemy et al. (2016)	*Strategic alignment*, lingkungan eksternal, kondisi internal organisasi, manajemen kinerja, manajemen usmber daya.
Fraser et al. (2016)	Manajemen, kebijakan dan regulasi

Sumber: Hasil olah data penelitian

Dari Tabel 5 dapat diketahui faktor-faktor yang mempengaruhi implementasi manajemen risiko pada *e-government* antara lain manajemen, kebijakan dan regulasi, perencanaan sumber daya TI dan kinerja organisasi. Pengetahuan yang dimiliki manajemen mengenai perencanaan sumber daya dapat mempermudah pendelegasian tugas sesuai dengan kualifikasi pegawai serta menumbuhkan budaya organisasi. Hal tersebut menjadi faktor penentu bagi manajemen dalam

implementasi *e-government*. Selain itu, manajemen juga harus dapat melakukan komunikasi yang efektif dengan staf dalam membangun pemahaman terhadap organisasi melalui seminar, loka karya, wawancara, rapat staf, maupun dewan direksi. Akan tetapi, kebijakan dan regulasi tetap sebagai faktor utama yang dapat mempengaruhi bagaimana kinerja manajemen dan organisasi (Fraser and Simkins 2016).

Selain lingkungan eksternal organisasi (*stakeholder,* kebijakan dan regulasi*)*, kondisi internal organisasi juga mempengaruhi keberhasilan implementasi manajemen risiko. Kebijakan dan prinsip strategi TI organisasi mempengaruhi strategi penyelarasan bisnis dan TI. Oleh karena itu, manajemen perlu menetapkan secara jelas strategi dan tata kelola TI organisasi. Manajemen kinerja dan sumber daya TI yang efektif, kultur organisasi serta *capability* staf TI juga mempengaruhi implementasi manajemen risiko (Alreemy et al. 2016).

Manajemen sebagai penentu keberhasilan dalam implementasi manajemen risiko berperan untuk menyusun strategi manajemen kinerja sehingga selaras dengan tujuan organisasi. Manajemen bertugas untuk mendelegasikan tugas yang sesuai dengan kualifikasi pegawai, mengintegrasikan bidang atau sektor dalam organisasi, serta merumuskan tata kelola organisasi. Pemilihan mitra swasta dalam proyek juga mempengaruhi implementasi manajemen risiko organisasi, komunikasi yang terbuka menjadi kunci keberhasilan *Public Private Partnership* (PPP). Perencanaan sumber daya organisasi (*Enterprise Resources Planning*) diimplementasikan untuk meningkatkan nilai tambah dari organisasi serta mendukung pengambilan keputusan bagi manajemen (Rampini, Takia, and Berssaneti 2019).

RQ3: Apa saja penelitian terkait standar implementasi manajemen risiko e-government?

Tabel 6. Standar Manajemen Risiko

Penulis	Standar	Keterangan
Olechowski et al. (2016)	ISO 31000	Standar umum manajemen risiko (manajemen proyek, PMBOK)
Masso et al. (2020)	ISO 31000	Standar manajemen risiko *software lifecycle*
Fikri et al. (2019)	ISO 27005, NIST	Penilaian risiko keamanan informasi
Akkiyat et al. (2019)	ISO 31000, ISO 9001	Pemodelan proses manajemen risiko
Ali et al. (2020)	ISO 27002	Penilaian risiko keamanan informasi pada *cloud computing*
Kasma et al. (2019)	COBIT 2019	Tata kelola keamanan *e-government*
Joshi et al. (2018)	COBIT	Tools penilaian *maturity level* manajemen risiko *e-government*
Brunner et al. (2020)	ISO 27000, COBIT	Manajemen risiko keamanan informasi
Shameli-Sendi et al. (2016)	ISO 27000, NIST, octave	Penilaian risiko keamanan informasi

Sumber: Hasil olah data penelitian

Berdasarkan Tabel 6, standar implementasi manajemen risiko yang banyak digunakan adalah ISO 31000-*series* dan ISO 27000-*series*. ISO 31000-*series* sebagai panduan manajemen risiko secara umum yang berdasarkan prinsip, *framework*, dan proses yang mungkin secara penuh atau sebagian telah diterapkan dalam organisasi sehingga pengelolaan risiko perlu disesuaikan dengan kondisi organisasi agar menjadi lebih efektif, efisien, dan konsisten (ISO31000 2018). Hasil pengujian penelitian memperkuat gagasan bahwa manajemen risiko harus menjadi bagian inti dari manajemen proyek dan sebagai alat dalam pengambilan keputusan yang sistematis (Olechowski et al. 2016).

ISO 31000-*series* banyak digunakan dalam manajemen risiko proyek, di mana adopsi sebelas prinsip manajemen risiko menjadi faktor penting dalam pencapaian biaya, jadwal, target, dan *stakeholder* menjadi lebih baik. Sebelas prinsip manajemen risiko tersebut antara lain:

1. Menciptakan nilai tambah bagi organisasi
2. Merupakan bagian integral dari proses manajemen risiko organisasi
3. Merupakan bagian dari pengambilan keputusan
4. Membahas ketidakpastian secara eksplisit
5. Sistematis, terstruktur, dan tepat waktu
6. Berdasarkan ketersediaan informasi yang akurat
7. Manajemen risiko dapat disesuaikan
8. Memperhitungkan faktor sumber daya manusia dan budaya organisasi
9. Transparan dan inklusif
10. Bersifat dinamis, iteratif dan responsif terhadap perubahan
11. Mengakomodir peningkatan berkelanjutan (*continual improvement*)

ISO 31000 juga diimplementasikan dalam manajemen risiko *software lifecycle*, proses yang berhubungan dengan manajemen risiko antara lain perencanaan proyek, implementasi, *software requirement*, persyaratan dari *stakeholder*, dan evaluasi proyek. ISO 31000 merupakan standar yang dapat disesuaikan dengan kebutuhan organisasi, dapat diadaptasi dan dihubungkan dengan standar lainnya dalam proses penilaian dan penanganan risiko sehingga diharapkan dapat menghasilkan pengawasan dan tanggung jawab yang tepat serta membuat manajemen risiko *software lifecycle* menjadi lebih efektif dan efisien (Masso et al. 2020).

Manajemen risiko keamanan informasi adalah langkah praktis dalam mengelola risiko bidang keamanan informasi suatu organisasi dan bertujuan untuk memberikan perlindungan terhadap informasi dan aset organisasi. Aset organisasi yang berhubungan dengan teknologi informasi antara lain (Brunner et al. 2020):

1. Infrastruktur jaringan termasuk *server hardware*
2. Layanan TI, aplikasi
3. Bisnis proses TI, *workstation*
4. Ruangan
5. Unit organisasi TI, *supplier*
6. *Stakeholder*, *cloud services*
7. *Point of Sales*/*Point of Information* (POS/POI)
8. *Software design*
9. Aset TI lainnya

Tools untuk dokumentasi aset organisasi yang banyak digunakan antara lain *spreadsheets*, *Configuration Management Databas*e (CMDB), *Enterprise Architecture Modelling* (EAM), *schematic diagram*/*charts* (ISMS/ISRM *tools*), serta alat dokumentasi lainnya (Brunner et al. 2020).

Beberapa fitur dan taksonomi penilaian risiko keamanan informasi banyak diimplementasikan dalam mengarahkan penilaian risiko menjadi lebih baik (Shameli-Sendi, Aghababaei-Barzegar, and Cheriet 2016). Teknik kombinasi banyak diterapkan dalam proses penilaian risiko keamanan informasi, sebagai contoh kombinasi ISO 27005 dan National Institute of Standards and Technology (NIST) SP 800-301 (Fikri et al. 2019). Implementasi ISO 27002 juga diimplementasikan dalam proses penilaian risiko keamanan informasi pada *cloud computing*. Model keamanan *cloud computing* yang diusulkan antara lain keamanan data, penilaian risiko, peraturan dan kepatuhan, *requirement* dari segi bisnis dan teknis (Ali et al. 2020).

Dalam tata kelola *e-government*, keamanan *e-government* menjadi hal yang sangat penting dalam pengendalian keamanan informasi. Tata kelola keamanan *e-government* mengadopsi 28 model COBIT 2019 yang diambil dari *critical success factor* dan risiko organisasi. Manajemen kinerja dari tata kelola ini terdiri dari kapabilitas dan *maturity* level yang dievaluasi oleh Kementerian Pendayagunaan Aparatur Negara-Reformasi Birokrasi (KemenPAN-RB) (Kasma, Sutikno, and Surendro 2019). Berdasarkan hasil analisis laporan tahunan dan survei mengenai *maturity* proses COBIT, disimpulkan bahwa *framework* tata kelola TI khususnya keamanan informasi sangat berperan dalam menstimulasi akuntabilitas dan transparansi pelaporan informasi yang berkaitan dengan teknologi informasi kepada *stakeholder* (Joshi et al. 2018).

RQ4: Bagaimana implementasi standar dan framework tersebut dalam proses manajemen risiko *e-government*?

Tabel 7. Integrasi Standar Manajemen Risiko

Penulis	Standar	Keterangan
Fikri et al. (2019)	Kombinasi ISO 27005 and NIST	Pemetaan ISO 27005 dan NIST SP 800-30 rev 1 fokus pada penilaian risiko keamanan informasi dengan menerapkan metode CBA (*Cost and Benefit Analysis*)
Barafort et al. (2018)	Kombinasi ISO 31000 dengan ISO 9001, 21500, 20000, 27000	Integrasi penilaian risiko dengan ISO 31000 dan ISO multi standar lainnya.
Fazlida et al. (2015)	ISO 27001 dan COBIT	ISO 27001 dan COBIT dapat digunakan organisasi dalam implementasi tata kelola keamanan informasi
Akkiyat et al. (2019)	ISO 31000, ISO 9001	Pemodelan proses manajemen risiko
Shakibazad et al. (2020)	NIST, ISO 27005, CRAMM (*Central Computing and Telecommunication Agency Risk Analysis and Management Method*)	Metode perhitungan sensitivitas aset dan teknik penilaian risiko pada sistem informasi
Shameli-Sendi et al. (2016)	ISO 27000, NIST, Octave	Taxonomi penilaian risiko keamanan informasi

Sumber: Hasil olah data penelitian

Secara umum, manajemen risiko berfungsi untuk menilai risiko dari seluruh kegiatan yang ada dalam organisasi, kemudian memilah berdasarkan prioritas serta menentukan tindakan penanganan risiko berdasarkan prioritasnya (ERM 2004). Masing-masing standar manajemen risiko memiliki prinsip dan *framework* sebagai acuan dalam penilaian risiko kegiatan dalam organisasi (ISO31000 2018). Sebagai standar umum manajemen risiko, ISO 31000 dapat diterapkan dengan mengintegrasikan standar lainnya, serta disesuaikan dengan kondisi dan kebutuhan masing-masing organisasi misalnya sumber daya TI yang dimiliki, manajemen, kebijakan dan regulasi (Barafort, Mesquida, and Mas 2018).

ISO 31000-*series* dapat diterapkan dalam segala jenis kegiatan termasuk pengambilan keputusan (Oliveira, Augusto, and Marins 2017). Proses manajemen risiko diawali dengan penentuan kriteria risiko, penilaian risiko, penanganan risiko, monitoring dan review, serta pencatatan dan pelaporan (ISO31000 2018).

ISO 27000-*series* diterapkan dalam mengembangkan manajemen keamanan informasi. Standar ini mengacu pada siklus PDCA (*Plan*, *Do*, *Check*, *Act*) yang memuat *information*

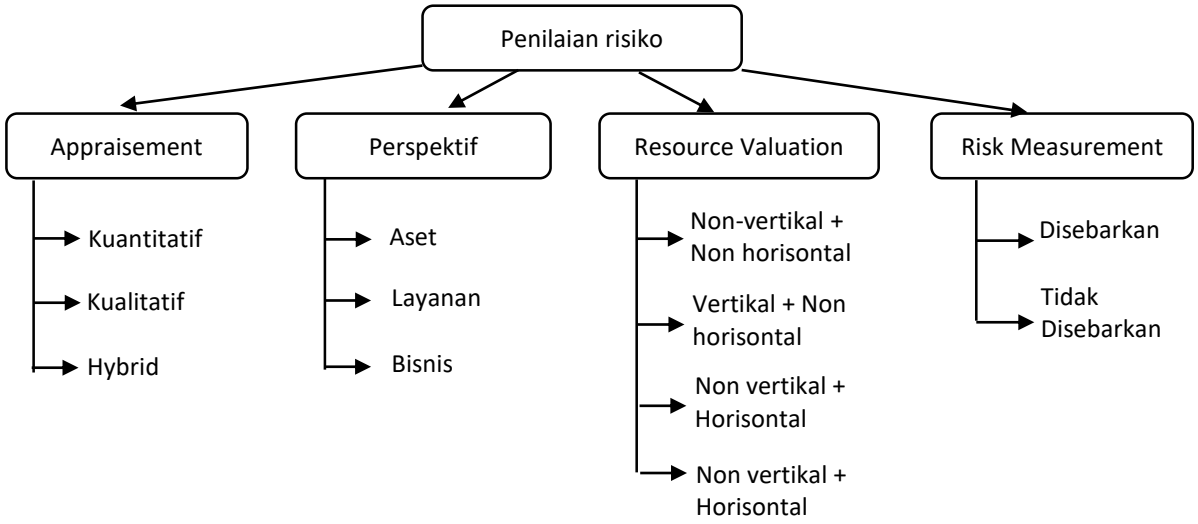
technology, *security technique*, dan *information security management system* (ISO/IEC 2016). Standar ini dapat diintegrasikan dengan standar lainnya seperti NIST (Fikri et al. 2019), COBIT (Fazlida and Said 2015), maupun ISO 31000 (Barafort, Mesquida, and Mas 2018). COBIT diterapkan dalam proses manajemen risiko dan perhitungan *maturity level* untuk menghitung sejauh mana tingkat kematangan implementasi *e-government* di suatu organisasi (Kasma, Sutikno, and Surendro 2019; Joshi et al. 2018).

Berdasarkan Tabel 7, *Integrated Standard* banyak diimplementasikan dalam proses manajemen risiko organisasi. Hal ini dianggap lebih fleksibel karena adopsi standar disesuaikan dengan kondisi dan kebutuhan dari organisasi serta dapat dimodifikasi oleh manajemen (Fikri et al. 2019; Fazlida and Said 2015; Barafort, Mesquida, and Mas 2018; Akkiyat and Souissi 2019; Shakibazad and Rashidi 2020). *Integrated Standard* menekankan pada proses penilaian risiko (*assessment*) dengan metode *Design Science Research Methodology* (DSRM). Tujuan dari implementasi DSRM ini adalah membuat hal yang dapat mendukung tujuan kemudian menciptakan sebuah model atau metode baru yang lebih inovatif.

Proses yang pertama DSRM adalah identifikasi risiko yang bertujuan untuk menemukan dan mendefinisikan risiko yang mungkin terjadi sehingga dapat membantu untuk mencegah risiko tersebut terjadi dan mendukung pencapaian tujuan organisasi. Faktor penentu kesuksesan identifikasi risiko antara lain informasi yang tepat dan akurat, teknik identifikasi risiko yang digunakan, serta identifikasi risiko berdasarkan faktor penyebabnya. Proses kedua adalah mendefinisikan objektif untuk pemecahan masalah. Kegiatan ini bertujuan untuk menyimpulkan sebuah solusi yang mungkin dari suatu identifikasi permasalahan. Proses ketiga adalah desain dan pengembangan. Kegiatan desain dan pengembangan bertujuan untuk membuat model/metode atau teknik manajemen risiko. Proses keempat adalah ujicoba yang bertujuan untuk menguji coba penggunaan model atau metode untuk memecahkan permasalahan dengan suatu eksperimen. Proses kelima adalah observasi. Kegiatan ini bertujuan untuk mengamati bagaimana implementasi model atau metode dalam memecahkan permasalahan dan membandingkan solusi-solusi yang ada dengan hasil eksperimen. Proses yang terakhir adalah komunikasi, yang bertujuan untuk mengkomunikasikan bagaimana keefektifan dan efisiensi penggunaan model penilaian risiko yang nantinya digunakan sebagai dasar perbaikan proses dalam organisasi tersebut (Barafort, Mesquida, and Mas 2018).

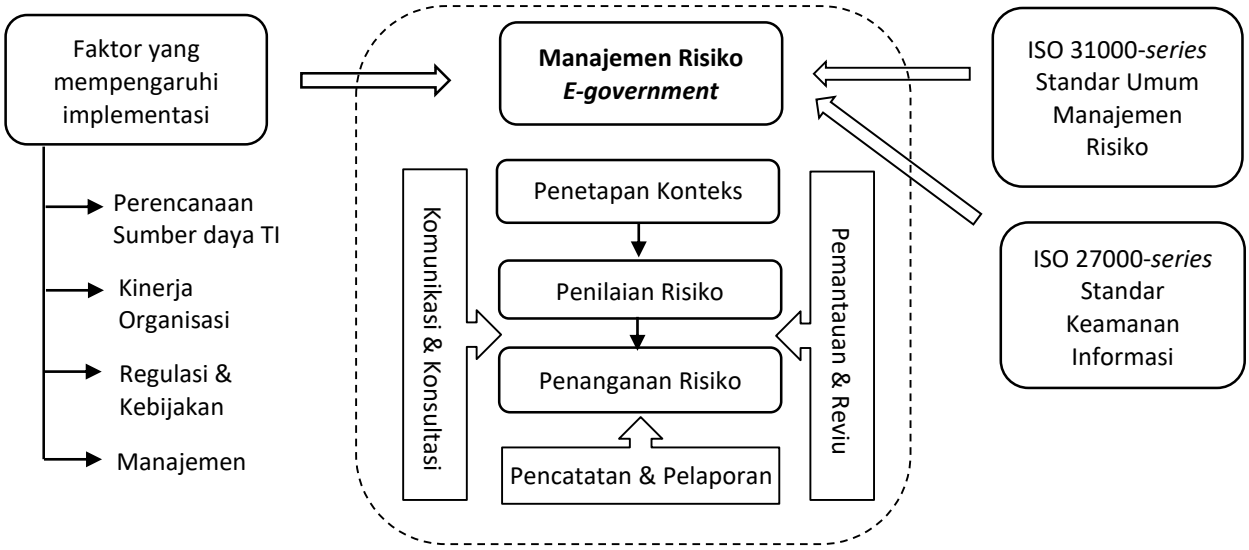
Banyak organisasi yang berinvestasi terhadap Sistem Manajemen Keamanan Informasi (SMKI) untuk mengidentifikasi dan mengurangi risiko keamanan dan memilih metode pengamanan yang terbaik. Dalam penilaian risiko, hal penting yang harus dilakukan adalah mengenali sumber daya penting dan kritis serta risikonya dalam organisasi. Sedangkan tantangan dalam proses penilaian risiko yaitu jumlah sumber daya non-kritis meningkat, perhitungan efek ancaman yang tidak akurat, sulitnya mendeteksi risiko yang signifikan, serta evaluasi risiko yang kurang tepat. Taksonomi keamanan informasi yang diusulkan kali ini diharapkan mampu membantu organisasi dalam memiliki pemahaman yang baik mengenai keamanan informasi (Shameli-Sendi, Aghababaei-Barzegar, and Cheriet 2016).

eISSN 2527 - 4902



Gambar 2. Taksonomi Penilaian Risiko Keamanan Informasi
(Shameli-Sendi, Aghababaei-Barzegar, and Cheriet 2016)

Secara garis besar implementasi manajemen risiko pada *e-government* dapat diilustrasikan seperti berikut:



Gambar 3. Ilustrasi manajemen risiko pada *e-government* (Sumber: Hasil olah data penelitian)

KESIMPULAN

Artikel ini menyajikan tinjauan literatur secara sistematis tentang manajemen risiko yang bertujuan untuk mengidentifikasi dan menganalisis implementasi standar manajemen risiko dalam *e-government*. Dari hasil analisis terhadap literatur dapat disimpulkan bahwa implementasi manajemen risiko pada *e-government* dapat meminimalisir terjadinya risiko yang dapat memberikan dampak merugikan bagi organisasi *non-profit* (pemerintah). Keberhasilan implementasi manajemen risiko dipengaruhi oleh faktor-faktor antara lain manajemen, regulasi dan kebijakan, kondisi sumber daya TI yang dimiliki, kemitraan, serta manajemen kinerja. Proses manajemen risiko yang baik harus berpedoman pada standar yang telah dikeluarkan oleh ISO. ISO

31000-*series* digunakan sebagai pedoman implementasi manajemen risiko secara umum seperti manajemen risiko proyek, *software lifecycle.* Sedangkan ISO 27000-*series* digunakan sebagai pedoman manajemen risiko keamanan informasi, perhitungan *maturity level* pada proses penilaian risiko menggunakan rujukan COBIT. Penggunaan standar tersebut dapat diintegrasikan (gabungan dua standar atau lebih) disesuaikan dengan kondisi dan kebutuhan organisasi masing-masing. Proses penilaian risiko sangat ditekankan ketika menggunakan metode integrasi.

Kajian ini dapat digunakan sebagai referensi bagi peneliti selanjutnya dalam melakukan penelitian terhadap manajemen risiko teknologi informasi pada *e-government*. Hingga saat ini belum ada penelitian yang bersifat kuantitatif yang mengkorelasikan antara implementasi manajemen risiko teknologi informasi dengan kinerja *e-government*. Untuk itu, ke depan perlu ada penelitian yang membahas mengenai hal tersebut.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Kementerian Komunikasi dan Informatika RI yang telah memberikan kesempatan untuk menempuh pendidikan pada Magister Teknologi Informasi Universitas Gadjah Mada.

DAFTAR PUSTAKA

Akkiyat, Ikram, and Nissrine Souissi. 2019. "Modelling Risk Management Process According to ISO Standard." International Journal of Recent Technology and Engineering (IJRTE) Volume 8 No 2: 5830–35. https://doi.org/10.35940/ijrte.B3751.078219.

Ali, Omar, Anup Shrestha, Akemi Chatfield, and Peter Murray. 2020. "Assessing Information Security Risks in the Cloud: A Case Study of Australian Local Government Authorities." *Government Information Quarterly* 37(1). https://doi.org/10.1016/j.giq.2019.101419.

Alreemy, Zyad, Victor Chang, Robert Walters, and Gary Wills. 2016. "Critical Success Factors (CSFs) for Information Technology Governance (ITG)." *International Journal of Information Management* 36 (6): 907–16. https://doi.org/10.1016/j.ijinfomgt.2016.05.017.

Barafort, Béatrix, Antoni Lluís Mesquida, and Antònia Mas. 2018. "Integrated Risk Management Process Assessment Model for IT Organizations Based on ISO 31000 in an ISO Multi-Standards Context." *Computer Standards and Interfaces* 60 (February): 57–66. https://doi.org/10.1016/j.csi.2018.04.010.

Brunner, Michael, Clemens Sauerwein, Michael Felderer, and Ruth Breu. 2020. "Risk Management Practices in Information Security: Exploring the Status Quo in the DACH Region." *Computers and Security*. https://doi.org/10.1016/j.cose.2020.101776.

Callahan, Carolyn, and Jared Soileau. 2017. "Does Enterprise Risk Management Enhance Operating Performance?" *Advances in Accounting* 37: 122-139. https://doi.org/10.1016/j.adiac.2017.01.001.

ERM. 2004. COSO - *Enterprise Risk Management – Integrated Framework*. USA: John Willey & Sons, Inc.

Fazlida, M.R., and Jamaliah Said. 2015. "Information Security: Risk, Governance and Implementation Setback." *Procedia Economics and Finance* 28 (April): 243–48. https://doi.org/10.1016/s2212-5671(15)01106-5.

Fikri, Muhamad Al, Fandi Aditya Putra, Yohan Suryanto, and Kalamullah Ramli. 2019. "Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organization: Case Study of ZZZ Information System Application in ABC Agency." *Procedia Computer Science* 161: 1206–15. https://doi.org/10.1016/j.procs.2019.11.234.

Fraser, John R.S., and Betty J. Simkins. 2016. "The Challenges of and Solutions for Implementing Enterprise Risk Management." *Business Horizons* 59 (6): 689–98. https://doi.org/10.1016/j.bushor.2016.06.007.

ISO. 2016. "ISO/IEC 27000:2016(E) Information Technology — Security Techniques — Information Security Management Systems — Overview and Vocabulary." *www.iso.org*.

ISO. 2018. *BS ISO 31000 : 2018. Risk Management — Guidelines.* BSI Standards Publication.

Joshi, Anant, Laury Bollen, Harold Hassink, Steven De Haes, and Wim Van Grembergen. 2018. "Explaining IT Governance Disclosure through the Constructs of IT Governance Maturity and IT Strategic Role." *Information and Management* Vol 55 Issue 3: 368-380. https://doi.org/10.1016/j.im.2017.09.003.

Kasma, Vira Septiyana, Sarwono Sutikno, and Kridanto Surendro. 2019. "Design of E-Government Security Governance System Using COBIT 2019: (Trial Implementation in Badan XYZ)." In *Proceeding - 2019 International Conference on ICT for Smart Society: Innovation and Transformation Toward Smart Region, ICISS 2019*. https://doi.org/10.1109/ICISS48059.2019.8969808.

Kementerian PAN RB. 2020. *Pedoman Manajemen Risiko SPBE*.

Kementerian PAN RB. 2020. "Tim Koordinasi SPBE Nasional Sampaikan Capaian 2019 Dan Rencana 2020." Accessed October 4, 2020. http://spbe.go.id/blog/tim-koordinasi-spbe-nasional-sampaikan-capaian-2019-dan-rencana-2020.

Kitchenham, Barbara, and Stuart Charters. 2007. Guidelines for Performing Systematic Literature Reviews in Software Engineering. UK: Keele University and Durham University Joint Report.

Maingak, Akmal Zaifullah, and Listyo Dwi Harsono. 2018. "Information Security Assessment Using Iso / Iec 27001 : 2013 Standard." *Trikonomika* 17 (1): 28–37. http://journal.unpas.ac.id/index.php/trikonomika/article/view/1138/618.

Masso, Jhon, Francisco J. Pino, César Pardo, Félix García, and Mario Piattini. 2020. "Risk Management in the Software Life Cycle: A Systematic Literature Review." *Computer Standards and Interfaces* 71 (March 2019): 103431. https://doi.org/10.1016/j.csi.2020.103431.

Olechowski, A., J. Oehmen, W. Seering, and M. Ben-Daya. 2016. "The Professionalization of Risk Management: What Role Can the ISO 31000 Risk Management Principles Play?" *International Journal of Project Management* 34 (8): 1568–78. https://doi.org/10.1016/j.ijproman.2016.08.002.

Oliveira, De, Fernando Augusto, and Silva Marins. 2017. "The ISO 31000 Standard in Supply Chain Risk Management" *Journal of Cleaner Production* 151: 616-633. https://doi.org/10.1016/j.jclepro.2017.03.054.

Rampini, Gabriel Henrique Silva, Harmi Takia, and Fernando Tobal Berssaneti. 2019. "Critical Success Factors of Risk Management with the Advent of ISO 31000 2018 - Descriptive and Content Analyzes." *Procedia Manufacturing* 39: 894–903. https://doi.org/10.1016/j.promfg.2020.01.400.

Shakibazad, Mohammad, and Ali Jabbar Rashidi. 2020. "New Method for Assets Sensitivity Calculation and Technical Risks Assessment in the Information Systems." *IET Information Security* 14 (1): 133–45. https://doi.org/10.1049/iet-ifs.2018.5390.

Shameli-Sendi, Alireza, Rouzbeh Aghababaei-Barzegar, and Mohamed Cheriet. 2016. "Taxonomy of Information Security Risk Assessment (ISRA)." *Computers and Security* 57. https://doi.org/10.1016/j.cose.2015.11.001.

Simota, Jan, Jiri Tupa*, and Frantisek Steiner. 2018. "Risk Management to Enhance Performance in the Construction SME Sector; Theory and Case Study." In *Risk Management Treatise for Engineering Practitioners*. https://doi.org/10.5772/intechopen.68798.

Tupa, Jiri, Jan Simota, and Frantisek Steiner. 2017. "Aspects of Risk Management Implementation for Industry 4.0." *Procedia Manufacturing* 11 (December): 1223–30. https://doi.org/10.1016/j.promfg.2017.07.248.