Assessment Penerapan Manajemen Risiko Teknologi Informasi Menggunakan ISO 31000

Didik Wahyu Setyadi dan Singgih Jatmiko

Jurusan Manajemen Sistem Informasi, Program Pascasarjana, Universitas Gunadarma
Jl. Margonda Raya No. 100 Pondok Cina Depok Jawa Barat
E-mail: didikwahyusetyadi@gmail.com, singgih@staff.gunadarma.ac.id

Abstrak

Pustik telah mengintegrasikan ISO 9001:2015, ISO/IEC 20000-1:2018 dan ISO/IEC 27001: 2013 ke dalam *Integrated Management System* (IMS). Sejak tahun 2013 telah menerapkan *Risk Management System* (RMS) dan telah diperkuat dengan Kebijakan Internal Lembaga tentang Manajemen Risiko yang terintegrasi dengan ISO/IEC 27001:2013. Adapun pengintegrasian RMS dengan ISO 9001:2015 dan ISO/IEC 20000-1:2018 belum ada pedoman khusus yang mengatur hal tersebut. Kondisi ini dapat menyebabkan isu yang menjadi perhatian dalam ISO 9001:2015 dan ISO/IEC 20000-1:2018 tidak terekam dengan baik dalam *Risk Register*. Untuk mengetahui kesenjangan antara RMS dengan ISO 31000:2018, perlu dilakukan *assessment* penerapan RMS sesuai standar ISO 31000:2018. Penelitian ini melakukan penilaian terhadap dokumentasi dan implementasi berdasarkan ISO 31000, sehingga diperoleh seberapa besar nilai kesesuaian dan ketidaksesuaian, serta rekomendasi perbaikan terhadap pengelolaan risiko dan peluang yang terintegrasi antara RMS dan IMS. Hasil penelitian terdapat penilaian RMS terhadap proses IMS saat ini adalah 75,93%, terdapat 4 klausul yang belum terpenuhi secara keseluruhan, dan 5 klausul yang hanya terpenuhi sebagian. Hasil penelitian ini dapat digunakan untuk menentukan langkah-langkah perbaikan, serta bisa digunakan untuk penyusunan pedoman manajemen risiko yang terintegrasi antara RMS dengan IMS.

Kata kunci : *Assessment,* Manajemen Risiko, Teknologi, Informasi, ISO 31000

Pendahuluan

Bertambahnya ketergantungan organisasi terhadap penggunaan sistem informasi dalam menunjang kegiatan organisasi sejalan dengan ancaman dan risiko yang timbul dari penggunaan sistem informasi tersebut[1]. Risiko adalah suatu kondisi terjadinya keadaan dimana dampak yang ditimbulkan bisa merugikan bagi organisasi[2][3]. Setiap kegiatan yang terjadi pada organisasi mempunyai dampak material atau konsekuensi yang signifikan bagi organisasi[4]. Sistem informasi memiliki risiko yang beragam seperti kegagalan kelistrikan karena faktor alam, human error, kebocoran data karena hacker, kerusakan sistem akibat terkena virus, kebakaran dan lainya[5][6]. Agar risiko bisa berkurang maka dibutuhkan sebuah tata kelola risiko yang baik dan benar[7]. Kemampuan untuk mengatasi risiko-risiko yang telah terjadi, meminimalkan risiko yang mungkin akan terjadi dan mengatur tata kelola risiko dengan baik dapat dilakukan dengan manajemen risiko[8][9]. Manajemen risiko merupakan sebuah proses yang didalamnya terdapat kegiatan seperti mengontrol risiko, mengidentifikasi risiko dan melakukan mitigasi risiko[10]. Selain itu manajemen risiko yang baik akan sangat berpengaruh pada manajemen kualitas, manajemen layanan teknologi informasi[11].

Dalam rangka meningkatkan efektivitas pelaksanaan tugas dan mutu pelayanan, serta mewujudkan tata kelola pemerintahan yang baik, saat ini Unit pengelola Teknologi Informasi pada lembaga keuangan pemerintah (Pustik) telah mengintegrasikan pengelolaan sistem manajemen ISO 9001:2015, ISO/IEC 20000-1:2018 dan ISO/IEC 27001:2013 ke dalam *Integrated Management System* (IMS). Sejak tahun 2013 Pustik telah menerapkan *Risk Management System* (RMS) yang diperkuat dalam Kebijakan Internal Lembaga tentang Manajemen Risiko di lingkungan Lembaga. Dalam pelaksanaan penerapan Manajemen Risiko, Pustik menetapkan Pedoman Pelaksanaan Manajemen Risiko Keamanan Informasi di lingkungan Pustik yang terbit sejak 21 Desember 2018 dengan mengintegrasikan RMS dan ISO/IEC 27001:2013. Adapun pengintegrasian RMS dengan ISO 9001:2015 dan ISO/IEC 20000-1:2018 belum ada pedoman khusus yang mengatur hal tersebut. Kondisi ini dapat menyebabkan beberapa isu

DOI : http://dx.doi.org/10.32409/jikstik.21.2.3061

yang menjadi perhatian dalam ISO 9001:2015 dan ISO/IEC 20000-1:2018 tidak terekam dengan baik dalam *Risk Register* Pustik.

Dengan pelaksanaan IMS di Pustik, pengintegrasian RMS dengan ISO 9001:2015 dan ISO/IEC 20000-1:2018 dan ISO/IEC 27001:2013 menjadi hal yang penting. Mengingat IMS di Pustik mengacu framework PAS 99:2012 dimana pada Annex B.6. disebutkan bahwa ISO 31000 menjadi standar proses manajemen risiko yang generic[12], ISO 31000:2018 dapat menjadi acuan dalam pengintegrasian RMS dengan IMS di Pustik. Untuk mengetahui seberapa besar kesenjangan antara RMS dengan ISO 31000:2018, perlu dilakukan *assessment* penerapan RMS sesuai standar ISO 31000:2018 dengan kondisi penerapan saat ini.

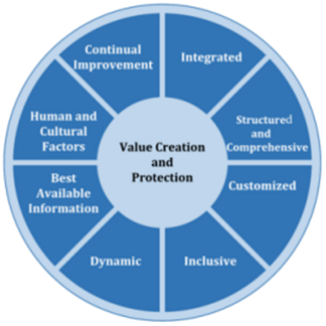
Masalah yang terjadi saat ini adalah belum terintegrasinya RMS dengan implementasi IMS di Pustik serta belum adanya pedoman khusus yang mengatur hal tersebut. Proses Manajemen Risiko untuk implementasi masing-masing ISO saat ini masih berjalan sendiri sehingga membutuhkan waktu serta alokasi *resource* baik sumber daya manusia ataupun dokumentasi teknis dalam hal pengelolaannya. Dalam penelitian ini, dilakukan analisis penerapan RMS di Pustik terhadap proses manajemen risiko pada ISO 20000:2018, ISO 27001:2013, dan ISO 9001:2015 yang sudah terintegrasi dengan IMS berdasarkan standar ISO 31000:2018 yang saat ini sudah diterapkan dan tertuang dalam Kebijakan Internal Lembaga tentang Manajemen Risiko.

Penelitian ini bertujuan untuk melakukan *assessment* seberapa besar nilai kesesuaian berdasarkan Klausul pada standar ISO 31000:2018 terhadap proses Manajemen Risiko di Pustik, dan memberikan rekomendasi perbaikan terhadap pengelolaan risiko dan peluang yang terintegrasi antara RMS dan IMS. Hasil penelitian ini dapat digunakan untuk menentukan langkah-langkah perbaikan yang harus dilakukan, agar efektivitas implementasi manajemen risiko dapat terus ditingkatkan sehingga penerapan RMS berjalan selaras dengan penerapan IMS serta dapat memberikan kontribusi kepada tata kelola organisasi yang baik (*good corporate governance*). Penelitian ini juga diharapkan bisa memberikan dampak positif terhadap peningkatan berkelanjutan pada proses pengelolaan Manajemen Risiko di lingkungan Pustik sesuai dengan aturan yang berlaku. Penelitian ini bisa digunakan untuk penyusunan Pedoman Manajemen Risiko yang terintegrasi antara RMS dengan IMS.

Penggunaan standar ISO 31000 berpotensi untuk menjadikan manajemen resiko yang lebih baik [13][14][15][16]. Dalam penelitian ini, standar ISO 31000:2018 digunakan untuk mengidentifikasi dan membandingkan klausul dengan implementasi beberapa Standar ISO yang terintegrasi dalam IMS. Penilaian dilakukan berdasarkan klausul ISO 31000:2018yang meliputi pemahaman organisasi dan konteksnya, kegiatan berbasis risiko, kepemimpinan dan komitmen, dan pendekatan proses *Plan Do Chenk Ack* (PDCA) yang sudah mengadopsi *High Level Structure* pada ISO yang sudah terintegrasi dengan IMS. Penelitian ini juga memberikan rekomendasi dalam penyusunan pedoman manajemen risiko yang bisa dijadikan acuan terhadap pengelolaan manajemen risiko yang terintegrasi.

IT Risk Management (Manajemen Risiko Teknologi Informasi) adalah suatu proses identifikasi kerentanan dan ancaman terhadap sumber daya informasi yang digunakan oleh sebuah organisasi dan dilakukan oleh manajer IT untuk mencapai tujuan bisnis, mengurangi risiko, dan menyeimbangkan pengeluaran dalam mencapai keuntungan dan melindungi IT. ISO 31000 adalah standar internasional untuk manajemen risiko yang disusun berdasarkan standar yang sudah ada terkait manajemen risiko yaitu AS/NZS 4360:2004. ISO 31000 dapat diaplikasikan dan diadopsi oleh berbagai organisasi terlepas dari ukuran, aktivitas, maupun sektornya. Berbeda dengan standar internasional lainnya, ISO 31000 tidak digunakan untuk tujuan sertifikasi, namun ISO 31000 menyediakan pedoman untuk program audit internal maupun eksternal. Suatu organisasi yang menerapkannya dapat membandingkan praktik manajemen risiko mereka dengan pedoman yang diakui secara internasional, memberikan kaidah yang baik untuk manajemen dan tata kelola organisasi yang efektif[17].

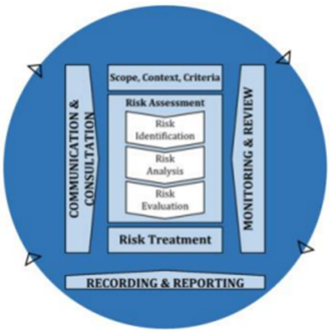
Pada ISO 31000:2018, terlihat pada Gambar 1., terdapat prinsip dalam penerapan manajemen risiko dan menjadi pertimbangan dalam mengembangkan kerangka kerja manajemen risiko suatu organisasi dan prosesnya. Prinsip ini memungkinkan organisasi mengelola dampak ketidakpastian dari sasaran dan tujuan organisasi. Prinsip tersebut merupakan dasar untuk pengelolaan risiko yang harus dipertimbangkan ketika menetapkan kerangka kerja dan proses manajemen risiko[18].



Gambar 1: Prinsip Manajemen Risiko ISO 31000:2018

Proses manajemen risiko pada Gambar 2, melibatkan penerapan kebijakan, prosedur, dan praktik yang sistematis untuk kegiatan berkomunikasi

dan konsultasi, membangun konteks dan menilai, memitigasi, pemantauan, peninjauan, pencatatan dan pelaporan risiko, sehingga proses manajemen risiko menjadi satu kesatuan yang utuh dan juga berkelanjutan dalam penerapan di suatu organisasi, dan dilakukan peninjauan secara terus-menerus.



Gambar 2: Proses Manajemen Risiko ISO 31000:2018

Menurut ISO 20000-1:2018[19], dalam konteks integrasi risiko bergantung pada pemahaman tentang struktur dan konteks organisasi, juga tujuan, sasaran, dan kompleksitas organisasi. Risiko dikelola di setiap bagian dari struktur organisasi. Setiap orang dalam suatu organisasi memiliki tanggung jawab untuk mengelola risiko. Dalam ISO 27001:2013[20] dan ISO 9001:2015[21] yang telah mengadopsi *High Level Structure*, dimana organisasi perlu menggunakan pendekatan berbasis risiko untuk mengatasi ancaman dan melihat peluang. Peluang dapat muncul sebagai akibat dari situasi yang menguntungkan untuk mencapai hasil yang diinginkan. Risiko adalah efek dari ketidakpastian dan setiap ketidakpastian tersebut dapat memiliki efek positif atau negatif. Penyimpangan positif yang timbul dari risiko dapat memberikan kesempatan, tapi tidak semua efek positif dari risiko dalam peluang.

Integrated Management System yang menggunakan standar PAS 99:2012 merupakan suatu standar umum yang mengadopsi *High Level Structure* untuk sistem manajemen yang digunakan sebagai dasar untuk membangun sistem manajemen yang terintegrasi. Dalam standar tersebut juga menyebutkan bahwa dalam aktivitas yang dilakukan, organisasi harus merencanakan tindakan untuk mengatasi risiko dan peluang.

Metode Penelitian

Agar penelitian ini berjalan secara sistematis, maka sebelumnya peneliti membuat perencanaan tentang langkah-langkah pemecahan masalah yang akan dilalui dalam bentuk metodologi penelitian sebagai berikut:

Tahap Pendahuluan

Pada tahapan ini terdiri dari penentuan objek penelitian serta melakukan studi lapangan dan pengumpulan data dengan wawancara, observasi dan reviu dokumen[22]. Penelitian dilakukan pada institusi pemerintah yang bergerak di bidang pengelolaan Teknologi Informasi. Secara tugas dan fungsi Pustik mempunyai tugas mengoordinasikan, menyusun dan melaksanakan kebijakan dan layanan teknologi informasi dan komunikasi, dan mengelola infrastruktur dan fasilitas pusat data, jaringan komunikasi data, aplikasi, basis data, keamanan informasi, dan jabatan fungsional pranata komputer. Dalam melaksanakan tugas sebagaimana dimaksud Pustik menyelenggarakan fungsi salah satunya terkait pelaksanaan manajemen risiko dan bina kepatuhan teknologi informasi dan komunikasi.

Diskusi dan wawancara ini dilakukan dengan Bidang Keamanan Informasi, khususnya dengan personil pada Sub bidang Manajemen Risiko dan Bina Kepatuhan sebagai pengelola dan admin Risiko pada Organisasi. Tujuan dari wawancara ini adalah menentukan masalah yang akan diangkat untuk diteliti dan dianalisis sehingga diperoleh hasil diskusi untuk mengangkat tema tentang pengelolaan Risiko dan metode yang digunakan oleh Pustik. Wawancara ini juga bertujuan untuk memperoleh informasi terkait implementasi Manajemen Risiko dalam bentuk pemenuhan dokumentasi atau Risiko-risiko terkait pengelolaan Teknologi Informasi dan Komunikasi (TIK) apa saja yang mungkin muncul berdasarkan suatu kejadian dan dampak yang ditimbulkan. Risiko-risiko yang dimaksud terkait kebijakan TIK, sumber daya manusia untuk mengelola layanan TIK, gangguan terhadap perangkat TIK yang terdiri dari perangkat keras dan perangkat lunak, kejadian terkait kegagalan keamanan sistem informasi yang akan mempengaruhi ketersediaan terhadap layanan. Risiko yang mungkin terjadi tersebut bisa menimbulkan dampak terhadap ketersediaan dan kelangsungan layanan TIK kepada pengguna layanan, sehingga dibutuhkan tindakan antisipasi untuk mencegah ataupun mengurangi Risiko tersebut.

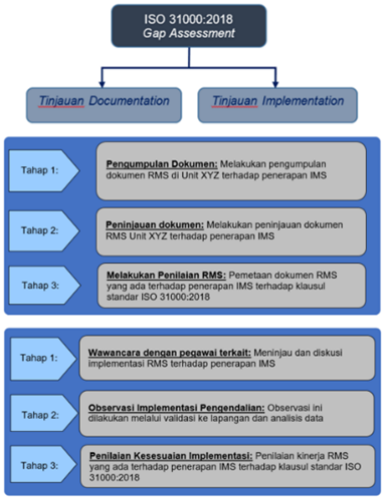
Tahap Assessment

Pada tahap ini dilakukan gap assessment proses manajemen risiko yang saat ini sudah diimplementasikan yaitu RMS yang sudah terintegrasi dengan ISO 27001:2013 namun perlu dilihat dengan IMS yang sudah dijalankan pada organisasi dan berdasarkan standar ISO 31000:2018 terkait manajemen risiko dengan klausul pada Tabel 1. sebagai berikut:

Tabel 1: Klausul ISO 31000:2018

Klausul	Keterangan
1. Lingkup	1. Merupakan klausul yang berisi tentang penjelasan dari Standar ISO 31000:2018.
2. Referensi normatif	
3. Istilah dan definisi	
4. Prinsip	2. Tidak masuk dalam klausul yang digunakan untuk *assessment*.
5. Kerangka kerja 5.1. Umum 5.2. Kepemimpinan dan komitmen 5.3. Integrasi 5.4. Desain 5.4.1.Pemahaman organisasi dan konteksnya 5.4.2.Penegasan komitmen manajemen risiko 5.4.3.Penetapan peran, kewenangan, tanggung jawab, dan akuntabilitas organisasional 5.4.4.Alokasi sumber daya 5.4.5.Penyiapan komunikasi dan konsultasi 5.5. Implementasi 5.6. Evaluasi 5.7. Perbaikan 5.7.1.Adaptasi 5.7.2.Perbaikan berkesinambungan	Merupakan klausul yang harus dilakukan implementasi dan masuk dalam kriteria *assessment*.
6. Proses 6.1. Umum 6.2. Komunikasi dan konsultasi 6.3. Lingkup, Konteks dan Kriteria 6.3.1.Umum 6.3.2.Penentuan lingkup 6.3.3.Konteks eksternal dan internal 6.3.4.Menentukan kriteria risiko 6.4. Penilaian risiko 6.4.1.Umum 6.4.2.Identifikasi risiko 6.4.3.Analisis risiko 6.4.4.Evaluasi risiko 6.5. Perlakuan risiko 6.5.1.Umum 6.5.2.Pemilihan opsi perlakuan risiko 6.5.3.Penyiapan dan penerapan rencana perlakuan risiko 6.6. Pemantauan dan tinjauan 6.7. Pencatatan dan pelaporan	

Pendekatan gap assessment yaitu dengan melakukan tinjauan pada dua aspek, dokumentasi dan implementasi, yang secara rinci dapat dilihat pada Gambar 3.



Gambar 3: Rincian Proses Tinjauan

Selanjutnya dilakukan penilaian terhadap hasil reviu terhadap dokumentasi dan proses implementasi. *Gap analysis* menggunakan acuan standar ISO 31000:2018 ini bertujuan untuk mengetahui sejauh mana pelaksanaan RMS yang sudah dilakukan di Pustik terkait ruang lingkup sertifikasi, sehingga dapat mengetahui proses mana yang masih memiliki kekurangan dan proses mana yang sudah cukup baik diterapkan. Selanjutnya Pustik dapat fokus kepada proses kritikal yang berpotensi menjadi hambatan dalam proses pelaksanaan standar RMS ini. Selain itu melalui penilaian dapat dilihat capaian kesesuaian secara kuantitatif. Kriteria yang digunakan dalam penilaian terhadap tingkat kesesuaian ditentukan dengan penjelasan seperti terlihat pada Tabel 2. yaitu kriteria penilaian berdasarkan hasil dari tahapan tinjauan aspek dokumentasi dan implementasi sesuai dengan klausul ISO 31000:2018.

Tabel 2: Kriteria Penilaian

Kategori Risk	Nilai	Keterangan
Low (Acceptable)	100	Dokumentasi sudah sesuai dengan standar ISO 31000:2018 dan Implementasi sudah terintegrasi secara total berjalan efektif dengan baik.
Medium (Not Acceptable)	50	Antara dokumentasi yang belum sesuai standar ISO 31000:2018 atau Implementasi belum terintegrasi dengan baik
High (Not Acceptable)	0	Dokumentasi belum sesuai standar ISO 31000:2018 dan Implementasi belum terintegrasi

Selanjutnya Penyusunan Pedoman Manajemen Risiko Pustik dilakukan berdasarkan hasil rekomendasi *assessment* yang mengacu pada standar ISO 31000:2018 yang sesuai juga dengan ketentuan yang ada pada Kebijakan Internal Lembaga tentang Manajemen Risiko. Pedoman ini bertujuan untuk memberikan acuan bagi pengelola risiko Pustik dalam menerapkan manajemen risiko dan peluang IMS di lingkungan Pustik, dengan Ruang lingkup pedoman ini terbatas pada pengelolaan risiko dan peluang dalam konteks IMS di lingkungan Pustik. Pedoman Manajemen Risiko ini terdiri dari beberapa bagian yaitu, Struktur Manajemen Risiko, Konsep dasar manajemen risiko, Strategi penerapan Manajemen Risiko, Proses manajemen Risiko.

Hasil dan Pembahasan

Dilakukan *gap assessment* di Pustik untuk melihat implementasi RMS yang dibandingkan dengan persyaratan standar ISO 31000:2018. Metodologi yang digunakan adalah wawancara dengan PIC / pelaku proses, mempelajari dokumen yang tersedia (kebijakan, pedoman, prosedur) serta melakukan verifikasi terhadap rekaman dengan metode sampel.

Berdasarkan hasil assessment terdapat ketidaksesuaian secara keseluruhan terhadap 4 klausul ISO 31000:2018 dengan implementasi risiko pada

Pustik, yaitu klausul 5.3. Integrasi, 5.4.1. Pemahaman Organisasi dan Konteksnya, 6.3.2. Penentuan Ruang Lingkup, 6.3.3. Konteks Internal dan Eksternal dengan masuk dalam kategori Risk High. Secara detail hasil assessment pada Tabel 3. berikut.

Tabel 3: Ketidaksesuaian 100%

Klausul	Temuan	Rekomendasi
Klausul 5.3. Integrasi	Pedoman Pelaksanaan Manajemen Risiko untuk ISO/IEC 27001:2013 sudah ada namun untuk ISO 9001:2015 dan ISO/IEC 20000-1:2018 belum ada.	- Menyusun pedoman pengintegrasian Manajemen Risiko IMS yang mengacu ke ISO 31000:2018. - Melakukan identifikasi dan penetapan keterkaitan profil risiko dengan penerapan sistem manajemen terintegrasi yang ada.
Klausul 5.4.1. Pemahaman Organisasi dan Konteksnya	Belum mempertimbangkan isu internal dan eksternal dari sistem manajemen ISO 9001:2015 dan ISO/IEC 20000-1:2018	
Klausul 6.3.2. Penentuan Ruang Lingkup	Belum tersedia mekanisme untuk penetapan ruang lingkup sistem manajemen risiko dengan memperthatikan faktor: - Sasaran yang akan dicapai - Waktu, Lokasi - Sumberdaya yang diperlukan - Hubungan dengan proses, aktivitas lainnya, dll Pedoman Pelaksanaan Manajemen Risiko untuk ISO/IEC 27001:2013 sudah ada namun untuk ISO 9001:2015 dan ISO/IEC 20000-1:2018 belum ada.	
Klausul 6.3.3. Konteks Internal dan Eksternal	- Belum tersedia mekanisme untuk penetapan ruang lingkup sistem manajemen risiko dengan memperhatikan faktor internal dan eksternal - Pedoman Pelaksanaan Manajemen Risiko untuk ISO/IEC 27001:2013 sudah ada namun untuk ISO 9001:2015 dan ISO/IEC 20000-1:2018 belum ada.	

Kemudian terdapat ketidaksesuaian secara 50% terhadap 4 klausul ISO 31000:2018 dengan implementasi manajemen risiko pada Pustik, yaitu klausul 5.1. Umum, 5.4.2. Penegasan Komitmen Manajemen Risiko, 5.4.5. Penyiapan Komunikasi dan Konsultasi, 5.5 Implementasi, 6.3.1. Umum (Ruang Lingkup, Konteks, dan Kriteria) dengan kategori Risk Medium. Secara detail hasil assessment yang memuat temuan, risk level serta rekomendasi bisa dilihat pada Tabel 4. berikut.

Tabel 4: Ketidaksesuaian 50%

Klausul	Temuan	Rekomendasi
Klausul 5.1. Umum	- Tersedia komitmen dari Pimpinan Lembaga melalui Kebijakan Internal tentang Manajemen Risiko di lingkungan Lembaga. - Pedoman Pelaksanaan Manajemen Risiko untuk ISO/IEC 27001:2013 sudah ada namun untuk ISO 9001:2015 dan ISO/IEC 20000-1:2018 belum ada.	- Menyusun pedoman pengintegrasian Manajemen Risiko IMS yang mengacu ke ISO 31000:2018. - Melakukan identifikasi dan penetapan keterkaitan profil risiko dengan penerapan sistem manajemen terintegrasi yang ada.
Klausul 5.4.2. Penegasan Komitmen Manajemen Risiko	- Tersedia komitmen dari Pimpinan Lembaga melalui Kebijakan Internal tentang Manajemen Risiko di lingkungan Lembaga - Pedoman Pelaksanaan Manajemen Risiko untuk ISO/IEC 27001:2013 sudah ada namun untuk ISO 9001:2015 dan ISO/IEC 20000-1:2018 belum ada.	
Klausul 5.4.5. Penyiapan Komunikasi dan Konsultasi	- Sudah ditetapkan mekanisme komunikasi dan konsultasi pada sistem manajemen risiko antara lain: Rapat berkala, Rapat Insidental, *Focus Group Discussion* dan Forum Pengelola Risiko - Pedoman Pelaksanaan Manajemen Risiko untuk ISO/IEC 27001:2013 sudah ada namun untuk ISO 9001:2015 dan ISO/IEC 20000-1:2018 belum ada.	
Klausul 5.5. Implementasi	Sudah tersedia formulir - Formulir 1 - Konteks Manajemen Risiko Pustik - Formulir 2 - Profil Risiko Pustik - Formulir 3 - Penanganan Risiko Pustik - Manual IRU - Pedoman Pelaksanaan Manajemen Risiko untuk ISO/IEC 27001:2013 sudah ada namun untuk ISO 9001:2015 dan ISO/IEC 20000-1:2018 belum ada.	
Klausul 6.3.1. Umum (Ruang Lingkup, Konteks dan Kriteria)	- Sudah tersedia sistem dokumentasi untuk proses penentuan ruang lingkup, konteks dan kriteria sistem manajemen risiko. - Pedoman Pelaksanaan Manajemen Risiko untuk ISO/IEC 27001:2013 sudah ada namun untuk ISO 9001:2015 dan ISO/IEC 20000-1:2018 belum ada.	

Kemudian terdapat 18 Klausul yang secara ke-

seluruhan sesuai dengan implementasi manajemen risiko pada Pustik, dalam hal ini rekomendasi yang diberikan adalah terkait melakukan pemantauan terhadap pelaksanaan manajemen risiko secara berkala. Klausul tersebut antara lain terlihat pada Tabel 5. berikut.

Tabel 5: Ketidaksesuaian 0%

No	Klausul	Rekomendasi
1.	5.2. Kepemimpinan dan Komitmen	Melakukan pemantauan pelaksanaan secara berkala untuk proses yang sudah sesuai
2.	5.4.3. Penetapan Peran, Tanggung Jawab dan Akuntabilitas Organisasi	
3.	5.4.4. Alokasi Sumber Daya	
4.	5.6. Evaluasi	
5.	5.7.1. Adaptasi	
6.	5.7.2. Perbaikan Sinambung	
7.	6.1. Umum (Proses)	
8.	6.2. Komunikasi dan Konsultasi	
9.	6.3.4. Pendefinisian Kriteria Risiko	
10.	6.4.1. Umum (Penilaian Risiko)	
11.	6.4.2. Identifikasi Risiko	
12.	6.4.3. Analisis Risiko	
13.	6.4.4. Evaluasi Risiko	
14.	6.5.1. Umum (Perlakuan Risiko)	
15.	6.5.2. Pemilihan Opsi Perlakukan Risiko	
16.	6.5.3. Penyiapan dan Penerapan Rencana Perlakukan Risiko	
17	Klausul 6.6. Pemantauan dan Tinjauan	
18	Klausul 6.7. Pencatatan dan Pelaporan	

Berdasarkan hasil gap assessment yang dilakukan didapatkan persentase kesesuaian (conformance percentage) sebesar 75,93 %. Hasil tersebut diperoleh dari nilai 4 klausul yang belum terpenuhi secara keseluruhan, 5 klausul yang hanya terpenuhi sebagian, dan 18 klausul yang secara keseluruhan sudah terpenuhi, yang dipetakan sesuai Tabel 2. Kriteria Penilaian. Nilai yang diperoleh adalah sebesar 2050 dari total nilai secara keseluruhan yaitu 2700, sehingga diperoleh persentase kesesuaian sebesar 75,93%. Berdasarkan hasil assessment terdapat rekomendasi tindak lanjut yang perlu segera diperbaiki karena bersifat kritis, daftar rekomendasi disajikan dalam Tabel 6. berikut.

Tabel 6: Ketidaksesuaian 50%

Rekomendasi Tindak Lanjut	Tujuan	Dokumen Terkait
1.1 Menyusun pedoman pengintegrasian Manajemen Risiko IMS yang mengacu ke ISO 31000:2018. 1.2 Melakukan identifikasi dan penetapan keterkaitan profil risiko dengan penerapan sistem manajemen terintegrasi yang ada	- Agar mengacu kepada standar ISO 31000:2018 - Agar implementasi sistem manajemen risiko memiliki lingkup dan konteks IMS	Pedoman Pelaksanaan Manajemen Risiko (PDM-002/IT/2018)
2. Menambahkan kolom pada Form-2 Profil Risiko yang menjelaskan tentang keterkaitan profil risiko dengan penerapan sistem manajemen ISO 9001:2015; ISO/IEC 20000-1:2018; ISO 27001:2013 + Annex terkait; Kebijakan Organisasi.	Agar terlihat keterkaitan risiko yang dikendalikan dengan implementasi IMS dan klausul terkait	Formulir 2 Profil Risiko
3. Melakukan identifikasi semua isu yang timbul dari pihak berkepentingan pada saat melakukan komunikasi dan konsultasi, kemudian menganalisis apakah isu-isu tersebut adalah potensi risiko baru, dampak dari proses mitigasi risiko yang ada, keluhan atau hanya isu. Kemudian mencatat hasil identifikasi di atas ke dalam notulen komunikasi dan konsultasi.	Agar terlihat bahwa organisasi telah melakukan identifikasi semua isu yang ada dan direkam didalam notulen komunikasi dan konsultasi	Notulen Komunikasi dan Konsultasi
4. Pada saat melakukan komunikasi dan konsultasi sebaiknya juga dilakukan pemberian informasi tentang keberhasilan menangani risiko yang ada	Agar tercipta proses komunikasi keberhasilan proses penanganan risiko sehingga dapat menjadi masukan bagi bidang lain yang mungkin memiliki risiko yang sama atau mitigasi yang sama	Notulen Komunikasi dan Konsultasi / Laporan Triwulan atau Laporan Tahunan
5. Menambah informasi mengenai penanggung jawab rekaman dan masa simpan rekaman sistem manajemen risiko ke dalam Pedoman Pelaksanaan Manajemen Risiko di Pustik	Agar mengacu kepada standar ISO 31000:2018	Pedoman Pelaksanaan Manajemen Risiko (PDM-002/IT/2018)

Penutup

Berdasarkan hasil gap assessment yang dilakukan didapatkan persentase kesesuaian (*conformance percentage*) sebesar 75,93 %, terdapat 4 klausul yang belum terpenuhi secara keseluruhan, dan 5 klausul yang hanya terpenuhi sebagian, dan 18 klausul yang secara keseluruhan sudah terpenuhi. Hasil *assessment* berupa rekomendasi dapat menghasilkan Pedoman Manajemen Risiko yang su-

dah mengintegrasikan RMS dengan IMS yang sudah diimplementasikan pada Pustik dan mengacu kepada standar ISO 31000:2018, dengan penyesuaian terhadap *Form* pada Profil Risiko yang menjelaskan keterkaitan penerapan sistem manajemen ISO 9001:2015; ISO/IEC 20000-1:2018; ISO 27001:2013 + Annex terkait; Agar terlihat keterkaitan risiko yang dikendalikan dengan implementasi IMS dan klausul terkait.

Untuk internal Pustik, hasil penelitian ini dapat digunakan untuk menentukan langkah-langkah perbaikan apa saja yang harus dilakukan, agar efektivitas implementasi manajemen risiko dapat terus ditingkatkan sehingga penerapan RMS berjalan selaras dengan penerapan IMS yang diterapkan di Pustik serta dapat memberikan kontribusi kepada organisasi yang baik (*good corporate governance*). Panduan manajemen risiko bisa digunakan secara rutin sebagai acuan untuk pengelolaan Manajemen Risiko dan Peluang yang terintegrasi antara RMS dan IMS yang diimplementasikan. Panduan tersebut juga bisa diperbaharui secara berkala disesuaikan dengan aturan atau kebijakan yang berlaku baik internal maupun eksternal.

Hasil assessment ini juga bisa dijadikan acuan organisasi untuk menghadapi penilaian yang bersifat eksternal. Hasil penelitian ini bisa digunakan untuk proses identifikasi Isu Internal dan Eksternal dalam Profil Risiko, sehingga risiko terkait pengelolaan layanan dan keamanan informasi bisa teridentifikasi lebih detail, dimitigasi dengan baik, dan pada akhir masa pemantauan level risiko bisa diturunkan sesuai dengan harapan, serta mendapatkan keuntungan yaitu dalam bentuk manfaat peluang dari mitigasi yang sudah dilaksanakan.

Untuk pengembangan penelitian selanjutnya diharapkan bisa melihat dan atau melakukan penilaian terhadap efektivitas penerapan manajemen risiko sesuai panduan yang telah disusun.

Ucapan Terimakasih

Terimakasih saya ucapkan kepada Pimpinan pada Pustik dan pengelola Manajemen Risiko terkait, dan semua pihak yang telah membantu dalam penelitian ini.

Daftar Pustaka

[1] A. Rahmawati and A. F. Wijaya, "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 Pada Aplikasi ITOP", J. SITECH Sist. Inf. dan Teknol., vol. 2, no. 1, pp. 13–20, 2019, doi: 10.24176/sitech.v2i1.3122.

[2] E. G. Monica and P. Pangeran, "The Integration of Balanced Scorecard and ISO 31.000 Based Enterprise Risk Management Process to Mitigate Supply Chain Risk: Case Study at PT Anugerah ", Int. J. Multicult, pp. 616–628, 2020.

[3] I. Sulistyowati and R. V. H. Ginardi, "Information Security Risk Management with Octave Method and ISO/EIC 27001: 2013 (Case Study: Airlangga University)", IPTEK J. Proc. Ser., vol. 0, no. 1, pp. 32–38, 2019, doi: 10.12962/j23546026.y2019i1.5103.

[4] Z. Putra, S. Chan, and M. IHA, "Design of Risk Management Based on Iso 31000 in PDAM Tirta Meulaboh", AFEBI Manag. Bus. Rev., vol. 2, no. 01, p. 21, 2017, doi: 10.47312/ambr.v2i01.55.

[5] Y. E. Patabang, S. Suprayitno, E. Sahiri, and I. M. J. A, "Operational Risk Management Of Surabaya Main Naval Base V Repair And Maintenance Facility Based On ISO 31000 Framework", Int. J. ASRO, vol. 10, no. 03, pp. 111–123, 2019.

[6] D. E. Anggraini and S. R. Rahayu, "Higeia Journal of Public Health", Higeia J. Public Heal. Res. Dev., vol. 1, no. 3, pp. 84–94, 2017.

[7] I. Setiawan, R. Waluyo, and W. A. Pambudi, "Perancangan Business Continuity Plan dan Disaster Recovery Plan Teknologi dan Sistem Informasi Menggunakan ISO 22301", J. RESTI (Rekayasa Sist. dan Teknol. Informasi), vol. 3, no. 2, pp. 148–155, 2019, doi: 10.29207/resti.v3i2.911.

[8] J. S. Suroso and M. A. Fakhrozi, "Assessment of Information System Risk Management with Octave Allegro at Education Institution", Procedia Comput. Sci., vol. 135, no. March, pp. 202–213, 2018, doi: 10.1016/j.procs.2018.08.167.

[9] D. K. Sari, D. Sakethi, R. Prabowo, "Pengembangan Sistem Pencarian Pada Tujuh Kitab Hadis Menggunakan Algoritma Knuth-Morris-Pratt", Jurnal Komputasi, vol. 7, no. 1, pp. 27–34, 2019.

[10] A. Syihabuddin, Y. Suryanto, and M. Salman, "Risk Management in Data Centers Using ISO 31000 Case Study : XYZ Agency", 1st STEEEM 2019, vol. 1, no. 1, pp. 341–352, 2019.

[11] W. S. Prabowo, . W., N. A Setiawan, M. H. Muslim, and Y. S. Utama, "Manajemen Risiko Infrastruktur Cloud Pemerintah Menggunakan Nist Framework Studi Kasus Lembaga Ilmu Pengetahuan Indonesia (LIPI)", J. Penelit. Pos dan Inform., vol. 7, no. 1, p. 17, 2017, doi: 10.17933/jppi.2017.0701002.

[12] G. Suprayitno and A. P. Stendel, "Integration management system design", Management and Entrepreneurship: Trends Of Development, vol. 3, no. 13, pp. 35–56, 2020, doi: 10.26661/2522-1566/2020-3/13-04.

[13] A. De and S. P. Dias, "Alcina de Sena Portugal Dias. ISO Standards Applicability and a Case Study About ISO 31000 in a Portuguese Municipality", Am. J. Theor. Appl. Bus., vol. 4, no. 4, pp. 102–111, 2018, doi: 10.11648/j.ajtab.20180404.11.

[14] Angraini and I. D. Pertiwi, "Analisa Pengelolaan Risiko Penerapan Teknologi Informasi Menggunakan Iso 31000", J. Ilm. Rekayasa dan Manaj. Sist. Inf., vol. Vol. 3, no. 2, pp. 70–76, 2017.

[15] B. Barafort, A. Mesquida, and A. Mas, "Integrating Risk Management in IT settings from ISO Standards and Management Systems Perspectives", Comput. Stand. Interfaces, vol. 54, Nov. 2016, doi: 10.1016/j.csi.2016.11.010.

[16] Hurin Iin, "Manajemen Risiko Teknologi Informasi Pada Proyek Perusahaan XYZ Melalui Kombinasi COBIT, PMBOOK, dan ISO 31000", Institut Teknologi Sepuluh Nopember, 2017.

[17] I. P. A. E. Pratama and M. T. S. Pratika, "Manajemen Risiko Teknologi Informasi Terkait Manipulasi dan Peretasan Sistem pada Bank XYZ Tahun 2020 Menggunakan ISO 31000:2018", J. Telemat., vol. 15, no. 2, pp. 63–70, 2020.

[18] K. B. Mahardika, A. F. Wijaya, and A. D. Cahyono, "Manajemen Risiko Teknologi Informasi Menggunakan Iso 31000 : 2018 (Studi Kasus: Cv. Xy)", Sebatik, vol. 23, no. 1, pp. 277–284, 2019, doi: 10.46984/sebatik.v23i1.572.

[19] B. Al Faruq, H. Herlianto, S. Simbolon, D. Utama, and A. Wibowo, "Integration of ITIL V3, ISO 20000 & ISO 27001: 2013 for IT Services and Security Management System", Int. J. Adv. Trends Comput. Sci. Eng., vol. 9, pp. 3514–3531, Jun. 2020, doi: 10.30534/ijatcse/2020/157932020.

[20] A. Fathurohman and R. W. Witjaksono, "Analysis and Design of Information Security Management System Based on ISO 27001: 2013 Using ANNEX Control (Case Study: District of Government of Bandung City)", Bull. Comput. Sci. Electr. Eng., vol. 1, no. 1, pp. 1–11, 2020, doi: 10.25008/bcsee.v1i1.2.

[21] A. Purwanto, P. Budi Santoso, and M. Asbari, "Effect Of Integrated ManagementaSystem Of ISO 9001:2015 And Iso 22000:2018 Implementation To Packaging Industries Quality Performance In Banten", J. Ilm. MEA (Manajemen, Ekon. dan Akuntansi), vol. 4, no. 1, pp. 17–29, 2020, doi: https://doi.org/10.31955/mea.vol4.iss1.pp17-31.

[22] Z. A. Hasibuan, "Metodologi Penelitian pada Bidang Ilmu Komputer dan Teknologi Informasi", 2007. diakses daring pada http://mhs.uks.ac.id/Referensi Kuliah/BUKUMETODE-PENELITIAN-PADA-BIDANG-IKOM-TI-ZAINAL-A-HASIBUAN1.pdf