JAIIT (Journal of Advances in Information and Industrial Technology)
Vol. 5, No. 1 Mei 2023, ISSN 2716-1935, E-ISSN 2716-1927

Analisis Manajemen Risiko IT di Organisasi XYZ Berdasarkan ISO31000:2018

Sangaji Wicaksono[*1)], Yupit Sudianto[2)]
[1,2)]Sistem Informasi, Fakultas Teknologi Informasi dan Bisnis, Institut Teknologi Telkom Surabaya,
Jl. Ketintang No. 156, Kota Surabaya 60231 Indonesia
Email: sangajiw@student.ittelkom-sby.ac.id[1)], yupit@ittelkom-sby.ac.id[2)]

Abstrak

Untuk mewujudkan Good Corporate Governance (GCG) di organisasi XYZ melalui optimalisasi departemen Information and Communication Technology (ICT), diperlukan analisis manajemen risiko. Tujuannya adalah mengidentifikasi, mengklasifikasi, dan menganalisis risiko untuk mencapai transparansi, akuntabilitas, tanggung jawab, kemandirian, dan keadilan. Namun, permasalahan masih ditemukan di tiap departemen yang mengganggu proses bisnis. Untuk mengurangi risiko, diterapkan manajemen risiko berdasarkan kerangka kerja ISO31000:2018 yang didukung oleh UU RI No. 20 Tahun 2014 dan PP No. 34 Tahun 2018 melalui BSN. Hasil penilaian risiko menunjukkan bahwa departemen pertama memiliki sebelas risiko dengan lima risiko signifikan, departemen kedua memiliki sembilan risiko dengan dua risiko signifikan, dan departemen ketiga memiliki delapan risiko dengan satu risiko tidak signifikan. Tiga risiko dapat diterima dan tiga risiko dapat dibagikan dengan pihak terkait atau vendor.

Kata kunci: *Analisis Risiko, Evaluasi Risiko, Identifikasi Risiko, ISO31000:2018, Manajemen Risiko*

1. Pendahuluan (*Introduction*)

Sebagai bagian dari perubahan organisasi penerapan *Information and Communication Technology* (ICT) saat ini banyak di implementasikan dalam mendorong transformasi digital yang di bagi ke dalam empat dimensi utama yaitu infrastruktur digital, ekonomi digital, pemerintah digital dan masyarakat digital (Ditjen Aplikasi Informatika, 2022). Organisasi XYZ merupakan organisasi pemerintah nonprofit yang termasuk dalam bagian empat dimensi utama dalam menerapkan strategi inklusif dari pemerintah pusat dengan lima web aplikasi meliputi operasional, personalia, kewilayahan, logistik dan perencanaan serta *website* organisasi itu sendiri. Dalam organisasi XYZ terdiri dari beberapa departemen namun dari beberapa departemen tersebut yang menunjang dalam implementasi ICT terdapat tiga departemen yaitu departemen satu, dua dan tiga. Ketiga departemen tersebut berperan penting dalam merancang, mengawasi dan menjaga keamanan, keutuhan dan ketersediaan terhadap seluruh aset data dan informasi *Technology Information* (IT). Pada departemen satu berperan dalam mengelolah seluruh aset data dan informasi dalam aplikasi organisasi XYZ serta meng-*update* maupun meng-*upgrade* secara berkala sesuai dengan waktu yang sudah ditentukan. Departemen dua merupakan departemen yang berperan dalam menjaga dan mengamankan ruang siber baik dari sisi fisik, logis dan persona pada organisasi XYZ serta dalam kesehariannya juga melaksanakan tugas untuk patroli siber sebagai tindakan preventif terhadap kemungkinan terjadinya insiden siber. Dan departemen tiga sebagai departemen penyedia layanan konektivitas internet dan menghubungkan jaringan sesuai dengan topologi yang sudah ditentukan.

Namun dalam pelaksanaannya, beberapa aktivitas dalam proses bisnis pada organisasi XYZ di bidang IT tidak selalu berjalan dengan lancar terkadang memiliki kendala dan permasalahan. Seperti proses meng-*update* aplikasi pada departemen pertama tidak dapat berjalan optimal dikarenakan keterbatasan Sumber Daya Manusia (SDM), ketersediaan komputer *client* pada departemen dua masih belum sesuai dengan indeks kepemilikan personel. Serta keberagaman perangkat nirkabel yang membutuhkan waktu dan personel cukup lama dalam melaksanakan konfigurasi jaringan internet pada organisasi XYZ. Berbagai kendala dan permasalahan yang muncul hendaknya dapat dikelola dengan

baik melalui proses manajemen risiko guna meminimalkan dan meningkatkan kemampuan dalam mengoptimalisasikan implementasi ICT pada organisasi XYZ. Proses mengelola risiko sendiri terbagi menjadi empat tahapan dimulai dari identifikasi risiko, analisis risiko, evaluasi risiko, serta pelaksanaan tindakan manajemen risiko (Oliveira, Marins, Rocha, & Salomon, 2017). Manajemen risiko dapat dipahami juga sebagai proses yang terstruktur guna meminimalkan atau mengurangi dampak dari suatu risiko. Kemudian risiko tersebut dianalisis guna merencanakan tanggapan yang diperlukan untuk pemantauan dan pengendaliannya (Oliveira, Espindola, & Marins, 2017). Penerapan manajemen risiko sendiri juga berbeda beda antar organisasi satu dengan lainnya tergantung kepada sudut pandang dalam pengelolaan risiko perusahaan (Carolyn & Soileau, 2017). Kombinasi antara manajemen kinerja dengan manajemen kualitas, proses dan risiko merupakan salah satu cara yang efektif dalam mengelola risiko (Simota, Tupa, & Steiner, 2018). Salah satu langkah awal dalam mengelola berbagai kemungkinan risiko ini yakni melakukan upaya pengukuran terhadap risiko dan kemunculan risiko IT. Dilihat dari berbagai risiko IT yang sangat berpengaruh pada *performance* dan capaian nilai organisasi, penelitian ini bertujuan untuk menganalisis manajemen risiko IT di organisasi XYZ. Terdapat berbagai kerangka kerja untuk menganalisis manajemen risiko IT, pada penelitian ini peneliti mengelola risiko IT berdasarkan kerangka kerja ISO31000:2018 (Badan Standardisasi Nasional, 2018). Penggunaan ISO31000 tidak hanya untuk tujuan sertifikasi, artinya tidak/belum ada sertifikat ISO31000 untuk suatu organisasi, tetapi ISO31000 bisa digunakan untuk program audit/*assessment* manajemen risiko. Organisasi yang menerapkan standar ini dapat terbantu mewujudkan manajemen dan tata kelola yang efektif dan efisien dengan membandingkan praktik manajemen risikonya dengan organisasi lain (*benchmarking*) (Handayani, Sari, Irawan, & Afdi, 2017) yang menekankan kembali pengelolaan risiko pada penciptaan dan perlindungan nilai. Yang merupakan bagian tak terpisahkan dari kepemimpinan dan tata kelola dengan memperhatikan konteks penerapan serta faktor perilaku manusia dan budaya dalam organisasi. Penerapan ISO31000 yang merupakan penyesuaian standar internasional yang dirumuskan sesuai SNI berkaitan dengan perbedaan iklim, lingkungan, geologi, geografis, kemampuan teknologi, dan kondisi spesifik lain (Alijoyo, 2019) sehingga dapat membantu organisasi serta secara efektif mengalokasikan dan menggunakan sumber daya untuk menghadapi risiko.

2. Metode Penelitian (*Methods*)

Pada penelitian ini, peneliti menggunakan metodologi kualitatif eksploratif yang bertujuan untuk mengenali secara menyeluruh perihal sebab dan suatu dampak atau kejadian yang terjadi pada sebuah organisasi (Mudjiyanto, 2018). Untuk memahami permasalahan risiko pada aset IT di organisasi XYZ, peneliti mengumpulkan berbagai jurnal dan literatur ilmiah sebagai referensi maupun data awal. Dengan mengevaluasi ancaman aset IT dan kerentanan kritis proses bisnis melalui sesi wawancara atau *in-depth interview* serta studi literatur dan observasi pada setiap departemen penunjang IT pada organisasi XYZ. Sehingga dapat membantu dalam memahami perihal permasalahan kemunculan risiko menjadi lebih baik. Kemudian berbagai kemungkinan risiko yang muncul kemudian didokumentasikan lalu di analisis dengan menggunakan kerangka kerja manajemen risiko berdasarkan *International Organization for Standarzation* (ISO) 31000:2018. Serta menyingkronisasikan dengan pewawancara melalui *form risk register* guna memiliki kesinambungan terhadap risiko yang terdapat di lapangan dengan *user* sebagai pengguna maupun pengelola.

ISO31000:2018 merupakan standar internasional penerapan manajemen risiko atau di Indonesia SNI ISO31000:2018 melalui Badan Standarisasi Nasional (BSN) serta ketetapan dasar hukum PP No. 34 Tahun 2018 tentang Sistem Standardisasi dan Penilaian Kesesuaian Nasional (Pemerintah Pusat Indonesia, 2018). Implementasi ISO31000:2018 pada organisasi XYZ sesuai dengan Peraturan Pemerintah Nomor 60 Tahun 2008 tentang Sistem Pengendalian Intern Pemerintah (SPIP) (Pemerintah Pusat Indonesia, 2008). Sebagai fondasi dalam mengelola risiko maka proses manajemen risiko ISO31000 bersifat berkelanjutan dan berulang sesuai dengan ketentuan waktu yang sudah ditetapkan dalam sebuah organisasi sehingga menghasilkan sebuah informasi guna menetapkan strategi dan

 DOI: https://doi.org/10.52435/jaiit.v5i1.216

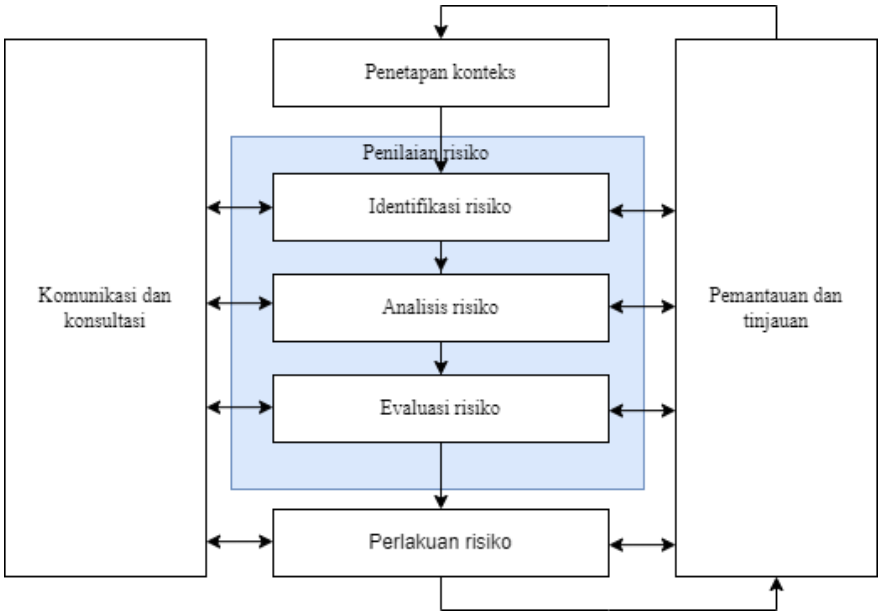
mengambil keputusan atau kebijakan untuk mencapai target. Proses manajemen risiko ISO31000 secara garis besar didasarkan pada prinsip, kerangka kerja dan proses dalam mengelola risiko pada suatu organisasi.

3. Hasil dan Pembahasan (*Results and Discussions*)

Seperti yang telah dijelaskan pada latar belakang permasalahan pada organisasi XYZ maka peneliti menentukan *scope context criteria* dalam organisasi. Penentuan tersebut diperoleh dengan mencari data dan informasi yang diperlukan oleh peneliti agar permasalahan yang terjadi menjadi lebih jelas kedudukannya. Penetapan *scope context criteria* pada penelitian ini sebagai batasan dan acuan atau parameter baik internal maupun eksternal yang dijadikan kajian pertimbangan dalam mengelola risiko, menentukan risiko, kriteria risiko meliputi manusia, teknologi dan hubungan antara manusia dan teknologi (Ross, Beath, & Goodhue, 1996). Kemudian melaksanakan observasi dan penilaian terkait manajemen risiko IT sehingga pendekatan kerangka kerja ISO31000:2018 mendapatkan hasil yang maksimal, akurat dan presisi untuk mengelola risiko pada organisasi XYZ.

3.1. Penilaian Risiko

Proses penilaian risiko digambarkan ke dalam rangkaian aktivitas dalam proses manajemen risiko pada Gambar 1 sesuai dengan ISO31000. Proses ini menyediakan pemahaman risiko lebih baik yang dapat mempengaruhi pencapaian sasaran, dan kecukupan beserta efektivitas pengendalian yang sudah tersedia. Sehingga dapat menjadi dasar dalam pengambilan keputusan tentang bagaimana pendekatan yang terbaik untuk mengelola kemungkinan risiko tersebut muncul. Keluaran dari penilaian risiko merupakan masukan untuk proses pengambilan keputusan dalam manajemen risiko organisasi.



Gambar 1. Penilaian Risiko pada Proses Manajemen Risiko Berdasarkan ISO31000:2018

a. Identifikasi Risiko

Identifikasi risiko merupakan tahapan awal guna mengidentifikasi risiko-risiko yang akan terjadi selama kegiatan dalam proyek IT atau proses bisnis. Pada tahap ini risiko diidentifikasi berdasarkan sumber kemunculan risiko yang dibagi menjadi dua bagian yaitu sumber risiko internal yang mencakup keterbatasan dana operasional, SDM yang tidak kompeten, peralatan yang tidak memadai, kebijakan dan prosedur yang tidak jelas, suasana kerja tidak kondusif serta sumber risiko eksternal yang mencakup peraturan perundang-undangan baru, perkembangan teknologi, bencana alam, gangguan keamanan dan vendor mengacu pada hasil studi literatur dengan identifikasi melalui hasil wawancara yang dilakukan dengan narasumber dari ketiga departemen organisasi XYZ serta penetapan konteks yang sudah

ditetapkan sebagai batasan dan acuan atau parameter baik internal maupun eksternal. Tabel 1 merupakan daftar risiko IT pada ketiga departemen organisasi XYZ.

Tabel 1. Risiko IT pada Organisasi XYZ

No.	Risiko	Dampak
S.1	Ketidaksesuaian domain organisasi	Mendapat sanksi dari pimpinan pusat
S.2	Jumlah SDM yang kurang	Profesionalitas dan regenerasi personel tidak berjalan
S.3	Pemerataan *skill* IT	Kompetensi personel kurang maksimal di bidang IT
S.4	Penggunaan *software* yang tidak resmi	Kerentanan data terhadap serangan virus, *malware* dan data *corruot*
S.5	Transfer *knowledge* dengan pihak ketiga tidak ada	Pengembangan aplikasi tidak terlaksana
S.6	Persetujuan dari departemen pusat	Aplikasi tertentu tidak dapat terintegrasi
S.7	*Overhead* pada server	Server dapat *shutdown* secara tiba-tiba
S.8	Komputer *client* tidak mendukung operasional	Tugas pokok menjadi kurang maksimal
S.9	Tidak memiliki antivirus tambahan	Data pada komputer *client* menjadi tidak dapat dibuka bahkan hilang.
S.10	Profesional personel	Lalai dalam melaksanakan tugas
S.11	Arus listrik yang berlebihan	Terjadi korsleting arus listrik
D.12	Jumlah SDM yang kurang	Beban kerja yang bertambah
D.13	Rekrutmen personel tidak sesuai dengan ketentuan	Kinerja personel kurang optimal
D.14	Jumlah komputer *client* belum sesuai	Kerahasiaan yang tidak terjaga dan terjamin
D.15	Server *Security Operations Center* (SOC) belum tersedia	Tidak dapat memonitor aplikasi, *website* dan lalu lintas jaringan internet
D.16	Ketersediaan *software* pengecekan aplikasi dan jaringan	Tidak dapat mengetahui keamanan secara *real time*
D.17	Ketersediaan *software* yang belum lengkap	Tugas pokok tidak dapat berjalan
D.18	Jaringan komunikasi sering terputus	Pelaksanaan proses bisnis menjadi terhambat
D.19	Integritas personel	Keamanan dan kerahasiaan tidak terjaga
D.20	*Overhead* pada hardware	Masa pakai yang tidak bertahan lama
T.21	Penataan SDM yang tidak merata	Ketidaksesuaian *jobdesk*
T.22	Kaderisasi yang tidak berjalan	Tugas pokok menjadi terhambat
T.23	Kendala pada *Internet Service Provider* (ISP) pertama	Koneksi jaringan terputus
T.24	Kendala pada ISP kedua	Koneksi jaringan terputus
T.25	Peremajaan pada *hardware* tidak terlaksana	Koneksi jaringan terganggu dan terputus
T.26	Tegangan listrik yang tidak stabil	Terjadi korsleting arus listrik
T.27	Penerimaan jaringan internet yang tidak	Tempat-tempat tertentu yang tersedia akses internet

 DOI: https://doi.org/10.52435/jaiit.v5i1.216

No.	Risiko	Dampak
	merata	
T.28	Keterbatasan dalam konfigurasi antar perangkat jaringan	Membutuhkan tenaga ahli dan waktu tambahan untuk melakukan konfigurasi antar perangkat

Keterangan: S = Departemen Satu; D = Departemen Dua; T = Departemen Tiga; Angka untuk penomoran risiko dari nomor satu sampai dua puluh delapan.

b. Analisis Risiko

Sebagai upaya dalam memahami risiko lebih mendalam dalam menganalisis risiko dilaksanakan penilaian terhadap risiko yang sudah terjadi. Dengan cara menilai risiko dari risiko yang sudah di identifikasi kemudian mengalikan besaran dampak risiko dengan kemungkinan kejadiannya, untuk menentukan kegawatan risiko. Dari hasil analisis risiko adalah besaran dampak yang diperoleh ini akan menjadi masukan dalam evaluasi dan pengambilan keputusan dalam mengelola risiko dan mengendalikan risiko. Guna mengetahui seberapa prioritas dan perlakuan risiko maka peneliti mengukurnya dengan *level of risk* atau tingkatan risiko. Dari tingkatan risiko tersebut dapat di analisis dengan menggolongkan ke dalam lima tingkatan *level of risk*. Penetapan *level of risk* pada kemungkinan kejadian yang terjadi bertujuan untuk mengukur dan menetapkan seberapa besar kemungkinan dan dampak risiko yang dapat terjadi pada sebuah organisasi.

Tabel 2. Matriks Analisis Risiko IT Organisasi XYZ

			Impact				
		Nilai	**1**	**2**	**3**	**4**	**5**
			Tidak Signifikan	**Minor**	**Moderat**	**Mayor**	**Ekstrem**
Likelihood	5	Hampir Pasti		S.9, D.12	S.1, S.2, S.3, S.5, D.15, D.16		
	4	Kemungkinan Besar	T.28	S.8, D.13, D.14	S.7		
	3	Kemungkinan Sedang					
	2	Kemungkinan Kecil	T.27	S.4, S.10, S.11, T.25, T.26	T.21, T.22, T.23, T.24		
	1	Jarang	D.17	D.18, D.20	S.6, D.19		

c. Evaluasi Risiko

Evaluasi risiko merupakan proses mengklasifikasikan risiko dengan perlakuan dan seberapa besar risiko tersebut diprioritaskan dalam mengelola risiko. Secara umum, perlakuan terhadap suatu risiko dapat berupa salah satu dari empat perlakuan (Badan Standardisasi Nasional, 2018). Berdasarkan hasil dari penetapan *level of risk* pada Tabel 2 di tahap analisis, hasil pengelompokan risiko pada tahap evaluasi risiko memberikan klasifikasi terhadap risiko yang muncul seperti pada Tabel 3.

Tabel 3. Evaluasi Risiko

No.	Evaluasi Risiko	Risiko
1	Menerima Risiko (*risk acceptance*)	D.17, D.27, D.28
2	Mitigasi (*mitigation*)	S.2, S.3, S.4, S.5, S.6, S.7, S.8, S.9, S.10, S.11, D.12, D.13, D.14, D.15, D.16, D.18, D.19,

No.	Evaluasi Risiko	Risiko
		D.20, T.21, T.22, T.25, T.26
3	Berbagi Risiko (*risk sharing / risk transfer*)	S.1, T.23, T.24
4	Menghindari Risiko (*risk avoidance*)	-

4. Kesimpulan (*Conclusion*)

Pada manajemen risiko organisasi XYZ dengan menggunakan kerangka kerja ISO31000:2018 diketahui terdapat dua puluh delapan risiko dari ketiga departemen, sebelas risiko terdapat pada departemen satu, sembilan risiko terdapat pada departemen dua dan delapan risiko terdapat pada departemen tiga. Hasil dari penilaian kedua puluh delapan risiko tersebut dikelompokkan menjadi empat bagian yang terdiri dari tiga risiko dapat diterima, tiga risiko harus dibagi dan dua puluh dua risiko harus dimitigasi. Dari hasil penelitian ini kedua puluh delapan macam risiko yang muncul yang nantinya dapat direkomendasikan dan dikoordinasikan kepada pimpinan sebagai wujud nyata dan upaya untuk menentukan keputusan dan kebijakan dalam mengelola berbagai risiko yang muncul dan meminimalkan, mengurangi bahkan menghilangkan dampak risiko yang ditimbulkan.

Ucapan Terima Kasih (*Acknowledgement*)

Tidak lupa peneliti juga mengucapkan terima kasih sebesar-besarnya kepada semua pihak yang selalu memberi dukungan baik moril dan materiil selama proses penelitian ini sampai selesai.

Daftar Pustaka

Alijoyo, A. (2019, Juni 6). *Indonesia Risk Management Professional Association*. Retrieved from SNI ISO 31000:2018 MANAJEMEN RISIKO: Satu-Satunya Standar Nasional Manajemen Risiko Indonesia – Berbasis UU NO: 20/2014: https://irmapa.org/sni-iso-310002018-manajemen-risiko-satu-satunya-standar-nasional-manajemen-risiko-indonesia-berbasis-uu-no-202014/

Badan Standardisasi Nasional. (2018). *Manajemen Risiko Berbasis SNI ISO 31000*. Jakarta: Badan Standardisasi Nasional.

Basfain, N. (n.d.). *Pengertian Studi Pendahuluan.* Retrieved May 15, 2022, from Academia: https://www.academia.edu/7218460/Pengertian_Studi_Pendahuluan

Carolyn, C., & Soileau, J. (2017). Does enterprise risk management enhance operating performance? *Advances in accounting, 37*, 122-139.

Ditjen Aplikasi Informatika. (2022, November 19). *APTIKA KOMINFO*. Retrieved from Akselerasi Transformasi Digital Pacu Pertumbuhan Ekonomi Digital: https://aptika.kominfo.go.id/2022/11/akselerasi-transformasi-digital-pacu-pertumbuhan-ekonomi-digital/

Handayani, N. U., Sari, D. P., Irawan, D. O., & Afdi, Z. (2017). Evaluasi Kesiapan Implementasi ISO 31000: 2009 Pada Departemen Teknik Industri Universitas Diponegoro. *J@ ti Undip: Jurnal Teknik Industri, 12*(1), 23-34.

Mudjiyanto, B. (2018). Tipe penelitian eksploratif komunikasi. *Jurnal studi komunikasi dan media, 22*(1), 65-74.

Oliveira, U. R., Espindola, L. S., & Marins, F. A. (2017). Analysis of supply chain risk management researches. *Gestão & Produção, 25*, 671-695.

 DOI: https://doi.org/10.52435/jaiit.v5i1.216

Oliveira, U. R., Marins, A. S., Rocha, H. M., & Salomon, V. A. (2017). The ISO 31000 standard in supply chain risk management. *Journal of Cleaner Production, 151*, 616-633. doi:10.1016/j.jclepro.2017.03.054.

Pemerintah Pusat Indonesia. (2008). *Peraturan Pemerintah (PP) No. 60 Tahun 2008: Sistem Pengendalian Intern Pemerintah.* Retrieved from Database Peraturan JDIH BPK RI: https://peraturan.bpk.go.id/Details/4876

Pemerintah Pusat Indonesia. (2018). *Peraturan Pemerintah (PP) Nomor 34 Tahun 2018: Sistem Standardisasi dan Penilaian Kesesuaian Nasional.* Retrieved from Database Peraturan JDIH BPK RI: https://peraturan.bpk.go.id/Details/89215/pp-no-34-tahun-2018

Ross, J. W., Beath, C. M., & Goodhue, D. L. (1996). *Develop long-term competitiveness through IT assets.* MIT Sloan Management Review.

Simota, J., Tupa, J., & Steiner, F. (2018). *Chapter Risk Management to Enhance Performance in the Construction SME Sector; Theory and Case Study.* InTechOpen. doi:10.5772/intechopen.68798

Halaman ini sengaja dikosongkan

 DOI: https://doi.org/10.52435/jaiit.v5i1.216