Turnitin Originality Report

wiyli_jieet by Wiyli Yustanti

From Thesis_Desertasi (Recheck)

Processed on 21-Sep-2019 15:28 WIB
ID: 1177018268
Word Count: 2754

Similarity Index	Similarity by Source	
16%	Internet Sources:	10%
	Publications:	3%
	Student Papers:	12%

sources:

1 2% match (Internet from 26-May-2019)
https://docplayer.info/29684938-International-standard.html

2 1% match (Internet from 07-Dec-2018)
https://www.scribd.com/document/343767759/Risk-di-IT

3 1% match (student papers from 06-Aug-2018)
Submitted to University of Northumbria at Newcastle on 2018-08-06

4 1% match (student papers from 26-Jul-2019)
Submitted to STEI Tazkia on 2019-07-26

5 1% match (student papers from 19-Nov-2015)
Submitted to Fakultas Ekonomi Universitas Indonesia on 2015-11-19

6 1% match (Internet from 02-Dec-2013)
http://www.deltaprima.net/konsultan-iso-27001-consultant/

7 1% match (Internet from 14-Jul-2012)
http://www.enotes.com/topic/IT_risk

8 1% match (student papers from 11-Mar-2019)
Submitted to St Dominic College of Asia on 2019-03-11

9 < 1% match (publications)
Shi-Cho Cha, Li-Ting Liu, Bo-Chen Yu. "Process-Oriented Approach for Validating Asset Value for Evaluating Information Security Risk", 2009 International Conference on Computational Science and Engineering, 2009

10 < 1% match (student papers from 30-Oct-2015)
Submitted to City University of Hong Kong on 2015-10-30

11 < 1% match (student papers from 07-Dec-2017)
Submitted to UIN Sunan Gunung DJati Bandung on 2017-12-07

12 < 1% match (Internet from 19-Aug-2005)
http://www.raidersfb.com/pdf/game_history.pdf

13 < 1% match (Internet from 09-Feb-2007)
http://network.zjwchc.com/downloads/patch/Windows.XP.SP2.ISO

14 < 1% match (Internet from 21-Oct-2012)
http://data.pakkau.edu.hk/~ngcheukkin/1C_CIT/20120928_1c_sonic/s20120098_1c01.001

15 < 1% match (Internet from 12-Jan-2007)
http://nws.noaa.gov/sp/comms.shw

16 < 1% match (publications)
Ihor Dobrynin, Tamara Radivilova, Nadiia Maltseva, Dmytro Ageyev. "Use of Approaches to the Methodology of Factor Analysis of Information Risks for the Quantitative Assessment of Information Risks Based on the Formation of Cause-And-Effect Links", 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), 2018

17 < 1% match (student papers from 19-Sep-2017)
Submitted to University of Central England in Birmingham on 2017-09-19

18 < 1% match (student papers from 05-Mar-2016)
Submitted to STIKOM Surabaya on 2016-03-05

19 < 1% match (Internet from 16-Sep-2019)
http://muhaz.org/konsep-pendidikan-islam-analisis-terhadap-pandangan-filosof-mu.html

20 < 1% match (student papers from 20-May-2018)
Submitted to Universitas Brawijaya on 2018-05-20

21 < 1% match (Internet from 20-May-2016)
http://www.slideshare.net/asrinovita/portofolio-pelatihan-inhouse-inovasi-sigma-perkasa

22 < 1% match (Internet from 21-Nov-2014)
http://ftp.cbi.pku.edu.cn/pub/database/hssp/hssp/1h4p.hssp

23 < 1% match (Internet from 20-Aug-2019)
https://ejournal.stipwunaraha.ac.id/index.php/AGRIKAN/article/download/274/pdf_1

24 < 1% match (Internet from 03-Mar-2019)
http://amidhani.blogspot.com/2009/02/password.html

25 < 1% match (Internet from 16-Nov-2018)
https://jurnal.umj.ac.id/index.php/semnastek/article/view/3461

26 < 1% match (student papers from 14-May-2018)
Submitted to Universitas Diponegoro on 2018-05-14

27 < 1% match (student papers from 06-Jan-2014)
Submitted to iGroup on 2014-01-06

28 < 1% match (student papers from 22-Jun-2019)
Submitted to Universitas Brawijaya on 2019-06-22

29 < 1% match (student papers from 26-Mar-2016)
Submitted to STIKOM Surabaya on 2016-03-26

30 < 1% match (student papers from 28-Jan-2014)
Submitted to STIKOM Surabaya on 2014-01-28

paper text:

Strategi Identifikasi Resiko Keamanan Informasi Dengan Kerangka Kerja ISO 27005:2018 W Yustanti1, A Qoiriah2, R Bisma3, A Prihanto4 1,2,3,4 (Jurusan Teknik Informatika, Universitas Negeri Surabaya) 1wiyliyustanti@unesa.ac.id Abstrak— Penelitian ini membahas hasil kajian penerapan ISO 27001:2013 dengan melihat aspek manajemen resiko yang diatur dalam standar ISO 27005:2018. Namun demikian , karena pada dokumen standar tidak dijelaskan secara rinci bagaimana metodologi penilaian resiko sebagai proses yang harus dilakukan untuk mencapai tujuan dari apa yang telah dinyatakan dalam kontrol

30**sistem manajemen keamanan informasi (SMKI),** maka **digunakan**

pendekatan operasional dalam penilaian resiko yang disebut sebagai Factor Analysis Information Risk (FAIR). Kesimpulan yang didapatkan adalah bahwa dengan menggunakan metode FAIR, maka proses penilaian resiko yang ditetapkan dalam ISO 27005:2018 sebagai bentuk kelengkapan untuk SMKI klausul 6 pada ISO 27001:2013 dapat dilakukan dengan lebih mudah. Kata Kunci— ISO 27001:2013, ISO 27005:2018, Sistem Manajemen Keamanan Informasi , metode FAIR I. PENDAHULUAN Sejak tahun 2017, pemerintah khususnya dibawah lingkungan Kemenristekdikti mengeluarakan peraturan menteri no. 62 tahun 2017 terkait Tata Kelola Teknologi Informasi (TI) di lingkungan kementrian ristek dikti. Maksud dan tujuan dikeluarkan peraturan ini adalah sebagai pedoman dalam penyelenggaraan tata kelola pemerintah yang baik melalui e-government pada setiap unit organisasi pemerintah. Ruang lingkup dari peraturan ini meliputi struktur

29**tata kelola TI,** enterprise architecture, **tata kelola** pengembangan, **tata kelola**

layanan dan tata kelola pengawasan. Untuk melaksanakan apa yang menjadi himbauan pemerintah maka pada tahun 2017 telah dilakukan audit keamanan informasi dengan menggunakan standart ISO 27001. Dalam bagian dari audit keamanan informasi ini, dibutuhkan sebuah pemahaman mengenai konsep manajemen resiko

24**dari keamanan informasi itu sendiri. Oleh karena itu,**

selain mengenai kelengakapan standart juga perlu memahami jenis-jenis resiko berdasarkan ISO 27005. ISO 27005 merupakan standar yang digunakan untuk memberikan pedoman bagi kebutuhan tata kelola

6**manajemen risiko keamanan informasi.** ISO 27005 **mendukung konsep umum yang** dijelaskan **dalam ISO** 27001 **dan dirancang untuk membantu penerapan keamanan informasi** yang tepat **berdasarkan pendekatan manajemen risiko.**

ISO 27005 tidak merinci, merekomendasikan atau bahkan secara khusus menunjukkan metode analisis risiko, meskipun didalamnya ada penjelasan terstruktur, sistematis, dan ketat dari awal hingga analisis risiko untuk menciptakan perlakuan risiko.

19**Permasalahan yang akan dibahas dalam tulisan ini adalah bagaimana**

melakukan identifikasi resiko TI untuk memenuhi standart ISO 27001:2013 dengan pendekatan metodolofi yang telah di atur dalam ISO 27005:2018. II.

18**TATA KELOLA TEKNOLOGI INFORMASI** Konsep **tata kelola teknologi informasi merupakan sebuah**

kerangka bagaimana manajemen TI dapat menyediakan struktur untuk menyelaraskan strategi TI dengan strategi bisnis. Dengan mengikuti kerangka kerja formal, organisasi dapat menghasilkan hasil yang terukur untuk mencapai strategi dan tujuannya. Program formal juga memperhitungkan kepentingan para pemangku kepentingan, serta kebutuhan staf dan proses yang mengikuti. Secara umum,

4**tata kelola TI** adalah **bagian integral dari tata kelola**

bisnis umum. Pada era saat ini, wilayah otoritas TI semakin kompleks dan berisiko. Munculnya teknologi seluler, media sosial, dan cloud semakin memperluas bisnis di luar sistem keamanan perusahaan, yang memungkinakan untuk terbentuknya departemen TI bayangan (pihak ketiga). Sementara itu, data adalah aset bisnis yang juga sangat meningkatkan manajemen risiko dan tekanan kepatuhan. Meningkatnya ketergantungan pada pihak ketiga semakin memperumit model operasi.Pada kondisi seperti ini, terjadilah ketergantungan yang belum pernah terjadi sebelumnya pada teknologi, sehingga terdapat konsekuensi besar ketika gagal. Untuk itu diperlukan Tata kelola TI yang efektif untuk mengatasi tantangan yang kompleks ini. Dengan mengelola kinerja yang dapat menciptakan nilai dengan lebih baik melalui system pendukung keputusan berbasis TI , maka organisasi dapat mencapai sasaran strategisnya. Kerangka kerja tata kelola TI akan membantu mengidentifikasi mekanisme yang diperlukan untuk menciptakan nilai dan mengelola risiko yang terkait dengan TI. III. MANAJAMEN RESIKO KEAMANAN INFORMASI A. ISO 27001:2013 ISO / IEC 27001 merupakan standar keamanan informasi, versi terbaru diterbitkan pada tahun 2013 dengan beberapa pembaruan kecil. Standar ini

11**diterbitkan oleh Organisasi Internasional untuk Standardisasi (ISO) dan** Komisi Listrik Internasional **(IEC)** di subkomite **ISO dan IEC,**

ISO / ICC JTC3 / SC3. ISO / IEC 27001 berisi konsep dalam menetapkan sistem manajemen yang terkait dengan keamanan informasi dalam manajemen dan memenuhi persyaratan tertentu serta dinyatakan lulus audit oleh sebuah lembaga audit. Keangka ISO 27001: 2013 ini merupakan dokumen yang berisi : 1) Lingkup standar 2) Dokumen rujukan 3) Persyaratan dan definisi ISO / IEC 27000 4) Konteks organisasi dan pemangku kepentingan 5) Keamanan informasi dan dukungan kebijakan tingkat tinggi 6) Merencanakan

5**sistem manajemen keamanan informasi , penilaian risiko dan**

pengelolaan risiko 7) Faktor pendukung

5**sistem manajemen keamanan informasi** 8) Implementasi **sistem manajemen keamanan informasi**

9) Evaluasi kinerja sistem keamanan informasi 10) Tindakan korektif 11) Lampiran A: daftar kontrol dan tujuan Pada tulisan ini akan lebih difokuskan bagaimana merencanakan manajemen keamanan informasi berdasarkan penilaian resiko dan pengelolaannya. Gambar 1. Elemen manajemen resiko B. ISO 27005:2018 ISO 27005 merupakan kerangka yang menjelaskan metodologi manajemen risiko. Dimana , manajemen resiko merupakan salah satu konsep kunci dari ISO 27001 khususnya untuk mengidentifikasi risiko (bagian ke-6) dan kemudian menggabungkannya dengan risiko yang berpotensi dihadapi. Standar ISO 27005 ini terdiri dari

21**55 halaman, dan berlaku untuk semua jenis organisasi**

[2] ISACA [1] mendefiniskan bahwa manajemen risiko TI adalah penerapan metode manajemen risiko pada teknologi informasi untuk mengelola

4**risiko TI,** yaitu **risiko bisnis yang terkait dengan penggunaan, kepemilikan, operasi, keterlibatan, pengaruh dan adopsi TI dalam** suatu **perusahaan** atau organisasi. Manajemen **risiko TI** merupakan komponen **dari**

sistem manajemen risiko perusahaan yang lebih luas. Kegiatan melakukan identifikasi, pemeliharaan, dan

28**peningkatan berkelanjutan dari Sistem Manajemen Keamanan Informasi**

(SMKI) merupakan sebuah bukti bahwa perusahaan telah menggunakan metode yang sistematis untuk mengidentifikasi, menilai, dan mengelola risiko keamanan informasi. Resiko TI tidak hanya mencakup resiko yang memiliki dampak negatif dari operasi dan layanan yang dapat menyebabkan kehancuran atau devaluasi organisasi akan tetapi juga resiko yang memiliki manfaat yang dapat menciptakan perbaikan

organisasi akibat tidak dimanfaatkannya peluang dalam pembaruan teknologi untuk kegiatan pengelolaan bisnis atau proyek TI seperti kelebihan pengiriman atau keterlambatan, yang mungkin bias memicu perusahaan untuk melakukan inovasi teknologi. Dalam dokumen OHSAS 18001:2007 didefinisikan bahwa resiko adalah kombinasi dari kemungkinan suatu peristiwa atau paparan berbahaya dan tingkat keparahan cedera atau masalah kesehatan yang mungkin timbul dari peristiwa atau paparan tersebut. Jika dikaitkan dengan asset teknologi informasi maka resiko IT merupakan gambaran komprehensif tentang semua

> 20**risiko yang terkait dengan penggunaan teknologi informasi di** bidang TI, **dan**

menyediakan pendekatan umum untuk manajemen risiko, mulai dari hilir hingga masalah budaya dan operasional. Secara umum dapat diformulasikan : Risk = Threat Likelihood * Magnitude of Impact (1) Dalam kerangka kerja ISO 27005:2018 , proses manajemen resiko

> 27**dapat digambarkan seperti Gambar 2.[2] Gambar 2.**

> 1**Proses Manajemen** Resiko **Keamanan Informasi Seperti yang** ditunjukkan **pada Gambar** 2, **proses manajemen risiko keamanan informasi dapat** diulang **untuk** menilai **risiko dan/atau** melakukan tindakan manajemen **risiko. Pendekatan** berulang **penilaian risiko** ini **dapat meningkatkan kedalaman dan** detail **penilaian** di **setiap iterasi. Pendekatan** iteratif ini **memberikan keseimbangan**

dalam mengurangi waktu dan upaya yang dihabiskan untuk mengidentifikasi tindakan pengendalian serta penilaian risiko yang tepat. Ketika konteks masalah sudah ditentukan sebelumnya, maka penilaian risiko dalam dilakukan kemudian. Jika proses ini sudah dapat memberikan informasi yang cukup dan efektif untuk melakukan

> 1**tindakan yang diperlukan** dalam mengurangi **risiko ke** level **yang dapat diterima, maka tugas** dapat diselesaikan **dan perlakuan risiko** dapat ditentukan. **Jika tidak** ada informasi yang **cukup,** maka **iterasi lain**

harus dilakukan. TABEL I KESESUAIAN ANTARA KERANGKA ISO 27001:2013 DENGAN ISO 27005:2018 ISO 27001 :2013 ISO 27005:2018 Plan • • • •

> 2**Menetapkan konteks Penilaian risiko Mengembangkan rencana penanganan risiko Penerimaan risiko Do Penerapan** rencanan **penanganan risiko Check Pemantauan dan peninjauan berkala terhadap risiko** Action **Meningkatkan dan memelihara Proses Manajemen Risiko Keamanan Informasi**

IV. METODOLOGI PENILAIAN RESIKO TI Pada ISO / IEC 27001,

> 1**tidak menyediakan metodologi khusus untuk manajemen risiko** yang terkait dengan **keamanan informasi.** Sehingga setiap **organisasi** dapat **menentukan pendekatan**

yang dipilih berdasarkan perjanjian internal organisasi berdasarkan ruang lingkup manajemen keamanan informasi, konteks manajemen risiko, atau jenis sektor organisasi. Untuk alasan ini, maka penelitian ini menggunakan analisis faktor risiko informasi (FAIR) sebagai metode identifikasi resiko. Dengan demikian kaitan antara ISO 27001, ISO 27005 dan FAIR adalah jika didalam 27001 dijelaskan deskripsi proses untuk sistem manajemen keamanan informasi dan ISO / IEC 27005 menyediakan metodologi analisis risiko, maka metode FAIR digunakan untuk menganalisis risiko dalam konteks ISO / IEC 27005 dan SMKI. Secara model dapat digambarkan seperti pada gambar 3. Pada klausul 4.2.1 dalam dokumen ISO / IEC 27001 disebutkan point penting untuk bagian manajemen risiko dari SMKI yaitu [4] : a) Menentukan pendekatan penilaian risiko organisasi b) Identifikasi risiko c) Menganalisis dan mengevaluasi risiko d) Mengidentifikasi dan mengevaluasi opsi untuk perawatan risiko e) Pilih tujuan kontrol dan kontrol untuk perawatan risiko f) Dapatkan persetujuan manajemen dari risiko residual yang diusulkan Poin ini menguraikan proses umum untuk mengelola risiko pada level manajemen tingkat atas dalam perusahaan. Sementara itu ISO / IEC 27005 menetapkan secara lebih rinci pengelolaan risiko tanpa memberikan spesifikasi atau mengidentifikasi metodologi untuk menentukan tingkat risiko. Sehingga FAIR dapat digunakan sebagai metodologi untuk mencapai proses yang dijelaskan dalam dokumen ISO baik 27001 dan 27005 khususnya mengidentifikasi risiko dan menganalisis serta mengevaluasi risiko. [6] PROSES • Keputusan pimpinan terkait penerapan ISO 27001 • Komitmen manajemen, pembentukan tim dan tugasnya OUTPUT • Mendefinisikan kebijakan • Dokumen ISO 27005 INPUT keamanan kebijakan informasi keamanan • Mendefinisikan informasi • Dokumen ruang • mengidentifikasi ruang lingkup ancaman utama, SMKI lingkup SMKI • Prosedur risiko, dampak, • Melakukan dan kerentanan Penilaian Resiko Penilaian Resiko Metode • Melakukan pada ruang pada ruang FAIR pendekatan lingkup SMKI lingkup SMKI • Dokumen organisasi dalam • Memutuskan manajemen bagaimana persetujuan dan tanggung jawab resiko berbasis mengelola resiko ISO 27005 dan yang sudah terhadap resiko yang sudah menentukan diidentifikasi diidentifikasi metode yang • Memilih tujuan • Dokumen dipilih dan control yang persiapan • Kontrol dan akan diterapkan pedoman pada berdasarkan ISO penryataan 27002 control apa saja ISO 27002 dan yang diterapkan dokumen lain • Menerapkan berdasarkan ISO control ISO 27002 27002 Gambar 3. Penggunaan ISO / IEC 27005 dan FAIR dalam Proses Pengembangan SMKI berbasis ISO / IEC 27001 Berdasarkan gambar 2 tentang gambaran detil tentang proses manajemen resiko, metode FAIR berada pada kegiatan

> 26**penilaian resiko** yang **terdiri dari** tahapan **identifikasi resiko,** estimasi resiko **dan** evaluasi **resiko.**

Secara taksonomi dapat dijelaskan dalam table 2. TABEL 2 METODE FAIR DALAM PENILAIAN RESIKO BERBASIS ISO 27005:2018 ISO 27005:2018 FAIR Analisis Resiko Keseluruhan komponen dalam taksonomi FAIR Identifikasi Resiko Tahap 1.Tahapan ini mencakup kegiatan mengidentifikasi skenarion komponen resiko yang beupa" • Mengidentifikasi aset yang beresiko • Menidentifikasi ancaman ISO 27005:2018 FAIR Evaluasi dan Estimasi Kapan terjadinya Resiko Tahap 2 , yaitu : • • • • • • Mengevaluasi

3**Loss Event Frequency (LEF)** Memperkirakan **Threat Event Frequency (TEF)** Memperkirakan **Threat Capability (TCap)** Memperkirakan **Control Strength (CS)** Menurunkan **Vulnerability (Vuln)** Menurunkan **Loss Event Frequency (LEF)**

Evaluasi dan Estimasi Berapa besar kerugian jika terjadi Resiko Tahap 3 , yaitu : • Mengevaluasi Probable

3**Loss Magnitude (PLM)** • Memperkirakan **worst-case loss** • Memperkirakan **Probable Loss Magnitude (PLM)** Keputusan Tahap **4**

, yaitu menurunkan dan menjelaskan semua resiko V. PEMBAHASAN Dalam bagian ini akan dijelaskan bagaimana strategi penggunaan metode FAIR untuk

2**sistem manajemen keamanan informasi (SMKI).** Berdasarkan tahapan **yang dijelaskan pada tabel 2,**

maka

5**langkah-langkah yang dilakukan dalam** proses penilaian resiko **adalah sebagai berikut** : a. Tahap **1**

Dalam tahapan ini akan dilakukan identifikasi komponen resiko yang berupa aset dan ancaman. Dalam mengidentifkasi aset maka harus dapat menjawab pertanyaan : (1) Aset apa yang beresiko?. Untuk menjawabnya maka dapat berupa sistem, aplikasi perangkat lunak, database, jaringan atau data center disesuaikan dengan ruang lingkup SMKI. (2) Ancaman apa yang terkait dengan resiko?. Untuk menjawabnya dapat dimulai dari karakteristik organisasi dan komunitas apa yang mungkin terlibat. Misalnya komunitas hacker, pihak internal, pihak ketiga yang berkaitan dengan TI atau kasus kriminalitas lain. b. Tahap 2 Tahapan ini dilakukan evaluasi dan estimasi terhadap frekwensi terjadinya resiko. Persamaan (1) menyatakan bahwa resiko merupakan perkalian antara peluang terjadinya ancaman (threat likelihood) dan besarnya dampak (magnitude of impact). Oleh karena itu kedua elemen tersebut harus diubah dalam bentuk kuantitatif. Nilai skala kuantitatif dari elemen kemungkinan terjadinya

23**ancaman dapat dilihat pada tabel 3. TABEL 3**

RATING FREKWENSI KEJADIAN ASSET YANG BERESIKO Rating Keterangan Sangat Tinggi (ST) Lebih dari 100 kali per tahun Tinggi (T) Antara 10 sampai 100 kali per tahun Sedang (S) Antara 1 sampai 10 kali per tahun Rendah (R) Antara 0.1 sampai 1 kali pertahun Rating Keterangan Sangat Rendah (SR) Kurang dari 0.1 kali per tahun Selanjutnya dilakukan identifikasi ancaman dari semua resiko terhadap asset dikonversi dengan nilai rating pada tabel 3. Kemudian diidentifikasi kemampuan dalam menhadapi ancaman terhadap asset dengan menggunakan tabel 4. TABEL 4 RATING KEMAMPUAN MENGHADAPI ANCAMAN Rating Keterangan Sangat Tinggi (ST) Top 2% dibandingkan semua nacaman Tinggi (T) Top 16% dibandingkan semua ancaman Sedang (S) Antara top 16% dan Bottom 16% dari semua ancaman Rendah (R) Dibawah bottom 16% dibandingkan semua ancaman Sangat Rendah (SR) Dibawah bottom 2% dari

semua ancaman Kemudian perlu dilakukan pengukuran daya tahan organisasi dalam menghadapi ancaman. Ukurannya dapat menggunakan table 5. TABEL 5 RATING DAYA TAHAN ORGANISASI DALAM MENGAHDAPI ANCAMAN Rating Keterangan Sangat Tinggi (ST) Mampu melindungi aset dari ancaman kecuali top 2% dari rata-rata ancaman Tinggi (T) Mampu melindungi aset dari ancaman kecuali top 16 % dari rata-rata ancaman Sedang (S) Mampu melindungi aset dari rata-rata ancaman Rendah (R) Hanya melindungi aset dari bottom 16% dibandingkan semua ancaman Sangat Rendah (SR) Hanya melindungi aset dari bottom 2% dibandingkan semua ancaman Selanjutnya dapat dilakukan analisis skala nilai kerentanan dan frekwensi terjadinya ancaman (threat likelihood). TABEL 6 MATRIX SKALA KERENTANAN Kerentanan Daya Tahan menghadapi ancaman SR R S

15T ST Kemampuan ST ST ST ST T M menghadapi T ST ST T

M R ancaman S ST T M

12R SR R T M R SR SR SR M R SR SR SR

TABEL 7 MATRIX SKALA LIKELIHOOD Likelihood Kerentanan SR R S

8T ST ST S T ST ST ST Frekwensi T R S T T T terjadinya ancaman S SR R S S S R

13SR SR R R R SR SR SR SR SR SR

Dimana nilai likelihood yang paling tinggi bernilai 100%. c. Tahap 3 Pengamat- Sumber Likeli- Impact Resiko Rekomendasi Setelah itu dilanjutkan dengan penilaian terhadap besarnya an hood dampak kerugian yang disebabkan dari resiko. Skala yang sebelum digunakan untuk mengukur dampak kerugian dari sebuah digunakan resiko dapat dilihat pada table 8. Server Service S S T Melakukan TABEL 8 menjalan- yang konfigurasi SKALA DAMPAK DARI KERUGIAN kan service tidak sistemulang dan yang tidak perlu/ap mematikan Rating Keterangan diperlukan likasi /membuang Parah (ST) Lebih dari 100 M mal- semua service Tinggi (T) Antara 10 M – 100 M ware yang tidak Signifikan (S) Antara 1 M – 10 M diperlukan Belum Tim S T T Mengembangka Sedang (M) 150 Juta – 1 M memiliki personal n dan Rendah (R) 10 Juta – 150 Juta dokumen yang melakukan Sangat Rendah (SR) Dibawah 10 Juta Disaster bertang simulasi oe Recovery gung gujian terhadap d. Tahap 4 Plan jawab dokumen terha- disaster recovery Pada tahap terakhir dilakukan pengukuran nilai resiko dap plan yang ada dengan membuat matrik hubungan antara likelihood penang- dan dampak resiko. Matrik yang digunakan dapat dilihat pada gulang- table 9. an resiko/ TABEL 9 bencana MATRIK RISIKO Resiko Fr ekwensi (likelihoo d) Hasil analisis resiko tersebut akan menjadi input dari proses SR R S T ST kebijakan manajemen dalam komitmen mengimpelemtasikan ST T T K K K SMKI berdasarkan kerangka 27001:20013. Dampak

22T S T T K K (Impact) S S S T T

K M R S S T T VI. PENUTUP

14**R R R S S** S **SR R R S S S**

25**Kesimpulan yang diperoleh dari kajian ini adalah bahwa**

Sebagai ilustrasi untuk menghitung resiko digunakan data dalam rangka menerapkan tata kelola TI yang salah satunya seperti table 10. adalan menajemen resiko TI dapat menggunakan kerangka 27005:2018 yang didalamnya dapat diintegrasikan dengan TABEL 10 metode FAIR sehingga membantu dalam mendapatkan CONTOH HASIL PENILAIAN RESIKO KEAMANAN INFORMASI prioritas resiko yang akan disiapkan scenario pencegahan dan Pengamat- Sumber Likeli- Impact Resiko Rekomendasi pemulihannya. an hood Password Hacker S S T Kombinasi pengguna password REFERENSI dapat sebaiknya dicek [1] ISACA, The Risk IT Framework Excerpt, Illiniois USA: ISACA,2009. dibobol kompleksitasnya

7**[2] ISO/IEC, Information technology -- Security techniques-Information** yang terdiri dari **security risk management. ISO/IEC FIDIS 27005:**

2018 kombinasi [3]

9**ISO/IEC, Information technology — Security techniques** — huruf, angka dan **Information security management systems — Requirements.ISO/IEC**

karakter khusus FIDIS 27001:2013 serta case

16**[4] Jack Freund, Jack Jones, Measuring and Managing Information Risk,**

sensitive untuk Butterworth-Heinemann,2015 huruf besar dan [5]

10**James Broad, Risk Management Framework : A Lab-Based Approach** kecil **to Securing Information Systems,**

1st Edition, Butterworth-Heinemann, SQL Hacker S S T Dilakukan Syngress, Elsevier, 2013 Injection validasi terhadap [6]

17**The Open Group, FAIR – ISO/IEC 27005 Cookbook, Open Group,**

semua header , United Kingdom, 2010 cookies, sintak query serta hiiden fields sebagai upaya untuk melawan adanya operasi sql yang tidak diijinkan. Database Hacker T S T Memastikan corrupted semua parameter divalidasi ISSN 2301 – 4156 W Yustanti: Strategi Identifikasi Resiko Keamanan (…) ISSN 2301 – 4156 W Yustanti: Strategi Identifikasi Resiko Keamanan (…) ISSN 2301 – 4156 W Yustanti: Strategi Identifikasi Resiko Keamanan (…)