JIKOM: JURNAL ILMU KOMPUTER
Volume 2 Nomor 1, Juli, 2024
ISSN: 3031-125X (ONLINE)
Penerbit: Program Studi Teknik Informatika S-2 Universitas Pamulang

Analisis *Disaster Recovery Plan* Keamanan Data dan Informasi Menggunakan NIST Framework (Studi Kasus: Biro Teknologi Informasi Yayasan Pendidikan Internal Audit)

* Faruk Muhamad [1], Tukiyat [2], Sajarwo Anggai [3]

[1,2,3)] Teknik Informatika, Program Pascasarjana Universitas Pamulang, Tangerang Selatan, Banten
[2)] Badan Riset dan Inovasi Nasional

Email: [1] farukmuhamad1@gmail.com, [2] tukiyat@brin.go.id, [3] sajarwo@gmail.com

ABSTRACT

Disasters are unexpected and potentially significant risks to the continuity of company and organization operations, especially those related to information systems and information technology (IS/IT). The Internal Audit Education Foundation (YPIA) in handling disasters related to data and information security often faces obstacles that cause problems that become more widespread in the future. Therefore, a disaster recovery plan (DRP) becomes an urgent need. The purpose of this study is to evaluate resilience to disasters and data and information security attacks, and to ensure better business continuity in the face of emergency situations. Researchers use the National Institute of Standards and Technology (NIST) Framework in conducting a DRP analysis of security and data. The study begins by identifying and evaluating risks, conducting risk assessments, conducting Business Impact Analysis (BIA) determining preventive controls, and formulating contingency strategies. This study produces priority handling of high maturity risks in data damage, with an initial risk value of 3.8 and an impact of 4.4. After the control was carried out, there was a residual risk with a risk value of 1.6 and an impact of 3, with a very low maturity level and a residual value of 13.5 (80%). The reduction in the risk of data damage was significant with a very low residual value, indicating that the implementation of DRP using the NIST Framework in risk mitigation on critical assets of the Internal Audit Education Foundation was quite effective.

Keywords: Plan, Disaster Recovery, Data Security, NIST Framework.

ABSTRAK

Bencana merupakan risiko yang tidak terduga dan berpotensi signifikan bagi kelangsungan operasional perusahaan dan organisasi, khususnya yang terkait dengan sistem informasi dan teknologi informasi (SI/TI). Yayasan Pendidikan Internal Audit (YPIA) dalam menangani bencana yang terjadi terkait keamanan data dan informasi sering kali menghadapi kendala yang menyebabkan masalah yang semakin meluas di kemudian hari. Oleh karena itu, rencana pemulihan bencana (Disaster Recovery Plan atau DRP) menjadi suatu kebutuhan yang mendesak. Tujuan dari penelitian ini yaitu mengevaluasi ketahanan terhadap bencana dan serangan keamanan data dan informasi, serta memastikan kelangsungan bisnis yang lebih baik dalam menghadapi situasi darurat. Peneliti menggunakan *National Institute of Standards and Technology* (NIST) *Framework* dalam melakukan analisis DRP keamanan dan data. Penelitian dimulai dengan mengenali dan mengevaluasi risiko, melakukan *risk asesssment*, melakukan *Bussiness Impact* Analisis (BIA) menentukan kontrol preventif, dan merumuskan strategi kontingensi. Studi ini menghasilkan prioritas penanganan pada risiko dengan maturitas tinggi pada kerusakan data, dengan risiko awal nilai nilai risiko 3.8 dan dampak 4.4. Setelah dilakukan kontrol, terdapat *residual risk* dengan nilai risiko 1.6 dan dampak 3, dengan tingkat maturitas sangat rendah dan nilai residual 13.5 (80%). Penurunan risiko kerusakan data signifikan dengan nilai *residual* yang sangat rendah, menunjukkan bahwa penerapan DRP menggunakan NIST *Framework* dalam mitigasi risiko pada aset kritis Yayasan Pendidikan Internal Audit cukup efektif.

Kata Kunci: Perencanaan, *Disaster Recovery*, Keamanan Data dan NIST *Fremework*.

1. PENDAHULUAN

Penelitian ini dilatar belakangi pada kebutuhan terkait rencana pemulihan terhadap bencana dan kemungkinan bencana yang ada di internal YPIA. Penelitian juga merujuk dari penelitian sebelumnya, ada 30 sumber penelitian sebelumnya yang 3 penelitian tersebut jadi referensi utama antara lain:

1. Afiansyah dkk (2023) yang menindaklanjuti munculnya aturan dari PP Nomor 71 Tahun 2019, terkait dengan Peraturan Pemerintah (PP) Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Hasil penelitian ini menghasilkan enam rencana pemulihan untuk sistem dengan prioritas tinggi, tiga rencana pemulihan untuk sistem dengan prioritas sedang, dan dua rencana pemulihan untuk sistem dengan prioritas rendah [1].
2. Delpia Amanda dkk (2023) adanya kekhawatiran data dan informasi semakin banyak disimpan dan dikelola sehingga ada potensi kerusakan, kehilangan atau terekspose kepada pihak lain yang tidak berwenang, dari hasil penilaian penelitian telah tercapai level 2 dari *maturity* level dan rekomendasi perbaikan yang diharapkan [2].
3. Zulkarnain (2022) melakukan analisa penerapan *Disaster Recovery Plan* (DRP) pada *data centre* perusahaan, peneliti ingin mengetahui implementasi DRP agar memiliki gambaran terkait keberhasilan implementasi DRP. Hasil dari penelitian ini peneliti mengetahui kegiatan dan proses DRP yang telah dilakukan dengan benar dan juga beberapa kegiatan atau proses yang harus jadi fokus perbaikan [3].

Berdasarkan tinjauan Pustaka dari penelitian sebelumnya banyak penelitian terbaru terkait topik *disaster recovery plan* menggunakan NIST *Framework*. Adapun kenapa penelitian melalui pendekatan NIST *Framework* yang mana dari pengamatan peneliti terkait *disaster recovery plan* banyak dimanfaatkan oleh peneliti sebelumnya dalam membuat dokumen rencana dan mitigasi bencana terhadap IT. Sehingga peneliti berusaha mengimplementasikan *framework* tersebut untuk organisasi yang diteliti. Setiap organisasi meliki pembeda dalam kebijakan terkait teknologi dan pemanfaatan teknologi di dalamnya sehingga dalam pengamanan dan memitigasi risiko terkait keamanan data dan informasi menggunakan NIST *Framework* adalah pilihan tepat.

2. TINJAUAN PUSTAKA

2.1. *Disaster Recovery Plan* (DRP)

DRP adalah serangkaian langkah-langkah dan strategi yang dirancang untuk mengidentifikasi risiko, merespons, memulihkan, dan melanjutkan operasi bisnis setelah terjadinya bencana. Tujuan utamanya adalah untuk meminimalkan dampak negatif terhadap organisasi dan memastikan bahwa sistem dan infrastruktur kritikal dapat kembali berfungsi secepat mungkin. Pendekatan dari FEMA, NIST, BCI, dan ISACA menekankan pentingnya perencanaan yang komprehensif dan kesiapan yang berkelanjutan untuk menghadapi situasi darurat [4], [5], [6], [7].

2.2. Keamanan Data dan Informasi

Keamanan data dan informasi menekankan pentingnya menjaga kerahasiaan informasi dengan teknik seperti enkripsi dan kontrol akses dengan tetap menjaga akurasi, kelengkapan data memastikan data dapat diakses oleh pihak berwenang kapan saja dengan otentikasi verifikasi identitas pengguna menggunakan metode seperti kata sandi dan *biometric* dengan kontrol akses dalam mengatur hak akses pengguna untuk melindungi data sensitif. Selanjutnya manajemen risiko dapat melakukan identifikasi, penilaian, dan pengendalian ancaman terhadap aset informasi untuk mengurangi dampak potensial ancaman [4], [8], [9], [10], [11], [12].

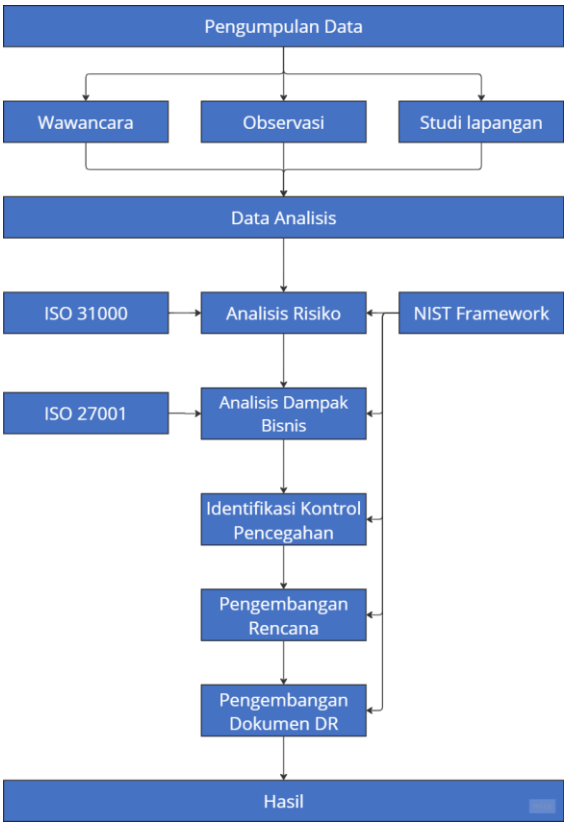
2.3. NIST *Framework*

National Institute of Standards and Technology (NIST) *Framework* yang diterbitkan oleh *US National Institute of Standards and Technology* adalah sebuah kerangka kerja (*framework*) untuk mengelola risiko keamanan siber [12]. Yang memuat pedoman dalam penyusunan *Contingency Planning* atau rencana penanganan darurat [13]. NIST *Framework* terdiri dari lima pilar utama: *Identify, Protect, Detect, Respond,* dan *Recover* [12].

2.4. Sistem Informasi Manajemen (SIM)

SIM adalah sistem formal atau nonformal yang dirancang untuk memecahkan masalah pada kegiatan manajemen[14], [15], [16] .

3. METODE



Gambar 1. Kerangka Pemikiran

3.1. Data Collection

Alur dimulai dari pengumpulan Data (*Data Collection*) pengumpulan data melalui berbagai metode seperti wawancara (*Interview*), observasi (*Observation*), dan studi lapangan (*Field Study*).

3.2. Data Analisis

1. *Risk Asessmen* dengan penilaian risiko dilakukan untuk menilai tingkat risiko yang mungkin terjadi pada sistem informasi [17]. Dalam melakukan penilaian risiko peneliti menggunakan panduan dari ISO 31000
2. *Bussiness Impact Analisis* Dalam melakukan *business impact analysis* menggunakan data aset SI dan TI yang dimiliki yang diperoleh melalui hasil identifikasi aset, serta data yang diperoleh dari hasil wawancara dengan pengguna layanan TI pada organisasi peneliti menggunakan panduan NIST SP 800-53 Rev 5 dan NIST SP 800-34 Rev 1 [18].
3. *Identivi Preventive Control*/ pengendalian preventif dibuat agar sistem informasi yang telah mengidentifikasi dan menilai risiko serta membuat analisis dampak

bisnis mendapat perhatian sesuai tingkat risiko dan memiliki prosedur pengendalian. Dalam melakukan identifikasi pengendalian preventif peneliti menggunakan panduan dari NIST SP 800-34 Rev1 [17].

4. *Developing Contigency Plan* Strategi kontinjensi difokuskan pada penentuan strategi cadangan dan alternatif lokasi layanan sistem informasi [17]. Adapun dalam melakukan rencana kontinjensi peneliti menggunakan panduan dari NIST SP 800-34 Rev 1.
5. Dokumen *Disaster Recovery Plan* disusun berdasarkan ancaman yang sudah diidentifikasi dan diberi skala penilaian dalam *risk assessment.* Dalam penyusunan dokumentasi DRP juga dilakukan penilaian yang dikombinasikan dengan bobot persentasi penilaian sub sistem.

4. HASIL DAN PEMBAHASAN

4.1. Hasil

4.1.1. *Risk Analysis*

Tabel 1. Tabel *Risk Analysis* Kemungkinan Ancaman

Kemungkinan Ancaman	Penyebab	Tingkat Level Risiko Akhir (R)	Tingkat Maturitas
Kerusakan data	Kesalahan pengguna *Ransomware* (terenkripsi oleh pihak yang tidak bertanggung jawab)	3.8	Tinggi
Aplikasi tidak dapat diakses	VPS *down* Akses user melebihi kapasitas *server* Kesalahan konfigurasi	3	Sedang
Rekapitulasi instruktur *error*, instruktur hanya dapat melihat materi apa, dan peserta saja	Pembatasan sistem *Bug* pada *interface* aplikasi	1.4	Rendah

4.1.2. *Business Impact Analisys* (BIA)

Tabel 2. Tabel *Business Impact Analysis* Kemungkinan Ancaman

Kemungkinan Ancaman	Dampak	Hasil BIA Akhir (D)	Tingkat Maturitas
Aplikasi tidak dapat diakses	Peserta tidak dapat melakukan pelatihan, risiko reputasi, risiko keuangan dan terganggunya proses bisnis utama	5	Sangat Tinggi
Data Hilang	Terganggunya proses bisnis terkait data	3.8	Tinggi
Kinerja *server* menurun	Proses bisnis yang berkaitan dengan *server* terganggu	2.8	Sedang
Kerusakan pada Laptop	Tidak dapat melakukan pekerjaan rutin terkait *system*	1.6	Rendah

4.1.3. *Identify Prefentive Control*

Tabel 3. Tabel Identifikasi Kontrol Pencegahan / Prefentif Control

Kemungkinan Ancaman	Tingkat Maturitas	Kerentanan	*Prefentif Control*
Aplikasi tidak dapat diakses	Sangat Tinggi	Pembayaran *server* terlambat, *Bandwith server* penuh, DDoS, *Bug*	*Billing reminder*, *capacity planning*, Penerapan OTP pada saat *login Quality assurance* program dan penerapan IT *Helpdesk*
Data Hilang	Tinggi	Pencurian, kerusakan perangkat, kehilangan perangkat penyimpanan, kesalahan pengguna	Lakukan *backup* berkala, pemanfaatan NAS, SOP, dan ada teguran dari masing-masing atasan
Kinerja *server* menurun	Sedang	Penggunaan semakin besar dan perangkat *out of date*	*Review* perangkat dan evaluasi berkala penggunaan perangkat
Kerusakan pada Laptop	Rendah	Masa pakai/ umur perangkat, konsleting, kesalahan pengguna, cacat produksi, perangkat *out of date*, dan kemasukan kotoran/ debu	Pengaturan masa pakai, Instruksi kerja dan penambahan UPS/*Powersupply*, perbaikan, SOP penghapusan perangkat, dan *general checkup* perangkat

4.1.4. *Developing Contigency Planning*

Tabel 4. Tabel *Developing Contigency Planning*

Kemungkinan Ancaman	Penjelasan	Aplikasi	Strategi Pencadangan	Strategi Pemulihan
Aplikasi tidak dapat diakses	Mencakup aplikasi utama penyelenggaraan operasional pelatihan di YPIA	Simpony	1. *Capacity Planing Up to* 50% kebutuhan 2. *Backup database* rutin 3. Mengunakan pihak ke-3 dalam melakukan *pentesting*	*Cold site*
Kerusakan data	Mencakup data kerja yang digunakan	MS *Office*	1. Pemanfaatan NAS/*server* 2. Pencadangan menggunakan Sistem Simpony	*Hot site*

4.1.5. *Developing DR Document*

DR Document di lingkungan YPIA berupa perbandingan antara *inherent* dan *residual* dari *risk analisys dan business impact analisys* dan DR *Team* sebagai berikut*:*

Tabel 5. Tabel Perbandingan Inherent dan Residual dari Analisis Risiko dan Analisis Dampak

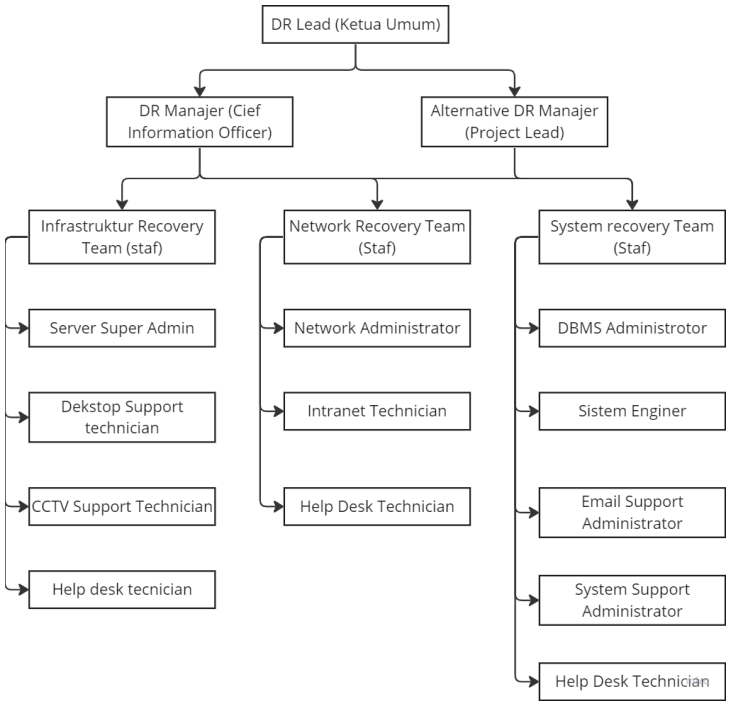
Kemungkinan Ancaman	***Inherent* (Risiko Bawaan)**				***Residual***				
	R	**D**	**N**	**M**	**R**	**D**	**N**	***M***	**Nilai *Residual***
Kerusakan data	3.8	4.4	16.7	T	1.6	3	3.2	SR	13.5 80%
Aplikasi tidak dapat diakses	3	5	15	S	1.8	2	5	R	9.96 66%
Video dari LMS dapat diunduh secara bebas	3.4	3.4	11.5	S	3.2	3	7.2	R	4.36 37.7%

Kemungkinan Ancaman	*Inherent* (Risiko Bawaan)				*Residual*				
	R	**D**	**N**	**M**	**R**	**D**	**N**	***M***	**Nilai *Residual***
Terjadi duplikasi data perusahan pada Aplikasi Simpony	3.4	3.4	11.5	S	2.6	2.2	8.9	R	2.6 22%
Sendgrid tidak mengirimkan pesan	3	3.8	11.4	S	2.6	2.4	6.2	R	8.2 71.9%

Keterangan tabel:

R: Risiko;
D: Dampak
N: Nilai besaran risiko
M: Maturitas

T: Tinggi
S: Sedang
R: Rendah
SR: Sangat Rendah



Gambar 2. DR *Team* IT

4.2. Pembahasan

4.2.1. Penilaian Risiko

Tingkat risiko menunjukkan besarnya risiko di lingkungan YPIA, yang dapat digunakan sebagai acuan untuk menentukan prioritas penanganan risiko dan penentuan tingkat maturitas. Penilaian risiko menggunakan rumus [19]:

$$R = L \times C$$

R = Risiko

L = Nilai *Likelihood* (Nilai Kemungkinan/ Risiko)

C = Nilai *Consequences/severity* (Nilai Keparahan/Dampak)

Adapun penentuan risiko mengacu pada tabel besaran risiko sebagai berikut:

Tabel 6. Tabel Tingkat Maturitas

Tingkat Maturitas	Besaran Risiko	Level
Sangat Tinggi	21 – 25	5
Tinggi	16 – 20	4
Sedang	11 – 15	3
Rendah	6 – 10	2
Sangat Rendah	1 – 5	1

Besaran risiko *inherent* terdapat 1 kemungkinan ancaman tingkat maturitas tinggi dengan kemungkinan ancaman pada kerusakan data. Terdapat 4 kemungkinan dengan maturitas sedang pada aplikasi tidak dapat diakses, video dari LMS dapat diunduh secara bebas, terjadi duplikasi data perusahan pada aplikasi Simpony, dan Sendgrid tidak mengirimkan pesan sesuai yang paparkan pada Tabel 5.

3.2.1. *Residual Risk*

Risiko *residual* adalah tingkat eksposur risiko yang tersisa setelah menerapkan kontrol yang direkomendasikan. Penentuan *residual risk* menggunakan rumus sebagai berikut:

$$Residual\ risk\ =\ Inherent\ risks\ -\ impact\ of\ risk\ controls$$

Keterangan:

Inherent risks = Risiko bawaan/ besaran risiko

Impact of risk controls = Dampak setelah dilakukan kontrol

Berdasarkan hasil *residual risk* dari Tabel 5 adalah sebagai berikut:

1. Kerusakan Data

   Besaran risiko awal nilai risiko 3.8, dampak 4.4, dengan tingkat *maturity* tinggi setelah dilakukan kontrol terdapat *residual risk* dengan risiko 1.6, dampak 3, dengan tingkat *maturity* sangat mendah dan nilai *residual* 13.5 (80%). Penurunan risiko kerusakan data signifikan dengan nilai *residual* yang sangat rendah, menunjukkan bahwa mitigasi yang diterapkan sangat efektif.

2. Aplikasi Tidak Dapat Diakses

   Besaran risiko awal nilai risiko 3, dampak 5, dengan tingkat *maturity* sedang setelah dilakukan kontrol terdapat *residual risk* nilai risiko 1.8, dampak 2 dengan tingkat *maturity* rendah dan nilai *residual* 9.96 (66%). Terdapat penurunan risiko yang baik, dengan nilai *residual* menunjukkan bahwa risiko ini dapat dikontrol dengan cukup efektif meskipun masih ada ruang untuk perbaikan.

3. Video dari LMS Dapat Diunduh Secara Bebas:

   Besaran risiko awal nilai risiko 3.4, dampak 3.4, dengan tingkat *maturity* sedang setelah dilakukan kontrol terdapat *residual risk* nilai risiko 3.2, dampak 3 dengan tingkat *maturity* rendah dan nilai *residual* 4.36 (37,7%). Penurunan risiko cukup rendah, menunjukkan bahwa langkah-langkah mitigasi yang ada kurang efektif dalam mengurangi risiko ini secara drastis. Sehingga perlu dilakukan program pengendalian, agar risiko dapat dikurangi.

4. Terjadi Duplikasi Data Perusahaan pada Aplikasi Simpony

   Besaran risiko awal nilai risiko 3.4, dampak 3.4, dengan tingkat *maturity* sedang setelah dilakukan kontrol terdapat *residual risk* nilai risiko 2.6, dampak 2.2 dengan tingkat *maturity* rendah dan nilai *residual* 2.6 (22%). Penurunan risiko cukup rendah, menunjukan bahwa langkah-langkag mitigasi kurang efektif sehingga risiko residual yang perlu diatasi untuk mengurangi duplikasi data.

5. Sendgrid Tidak Mengirimkan Pesan

   Besaran risiko awal nilai risiko 3, dampak 3.8, dengan tingkat *maturity* sedang setelah dilakukan kontrol terdapat *residual risk* nilai risiko 2.6, dampak 2.4 dengan tingkat *maturity* rendah dan nilai *residual* 8.2 (71.9%). Penurunan risiko cukup besar, menunjukkan bahwa mitigasi cukup efektif dalam mengurangi risiko, meskipun nilai *residual* masih menunjukkan adanya risiko yang perlu diperhatikan.

5. KESIMPULAN

Penilaian risiko dilakukan dengan mengidentifikasi kemungkinan ancaman pada aset kritis. Besaran risiko *inherent* terdapat 1 kemungkinan ancaman tingkat maturitas tinggi dengan kemungkinan ancaman pada kerusakan data. Terdapat 4 kemungkinan dengan maturitas sedang pada aplikasi tidak dapat diakses, video dari LMS dapat diunduh secara bebas, terjadi duplikasi data perusahan pada aplikasi Simpony, dan Sendgrid tidak mengirimkan pesan. Setelah dilakukan pengendalian risiko, prioritas penanganan pada risiko dengan maturitas tinggi pada kerusakan data besaran risiko awal nilai risiko 3.8, dampak 4.4, setelah dilakukan kontrol terdapat *residual risk* dengan risiko 1.6, dampak 3, dengan tingkat maturitas sangat rendah dan nilai *residual* 13.5 (80%). Penurunan risiko kerusakan data signifikan dengan nilai *residual* yang sangat rendah, menunjukkan bahwa

penerapan DRP dengan menggunakan *NIST Framework* dalam mitigasi kemungkinan yang terjadi pada aset kritis Yayasan Pendidikan Internal Audit cukup efektif.

6. DAFTAR PUSTAKA

[1] H. G. Afiansyah, S. U. Sunaringtyas, and A. Amiruddin, "Perancangan Rencana Pemulihan Bencana Menggunakan NIST SP 800-34 REV 1, NIST SP 800-53 REV 5 DAN SNI 8799 (Studi Kasus: UNIT TI XYZ)," *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*, vol. 10, no. DRP, pp. 329–338, Apr. 2023, doi: 10.25126/jtiik.20231026507.

[2] D. Amanda, N. Mutiah, and S. Rahmayudha, "Analisis Tingkat Kematangan Keamanan Informasi Menggunakan NIST Cybersecurity Framework dan CMMI," 2023. doi: 10.26418/coding.v11i2.65088.

[3] Zulkarnain, "Analisa Penerapan Disaster Recovery Plan Pada Data Center Perusahaan," *CBIS Journal*, vol. 10, no. DRP, pp. 1–6, 2022, doi: 10.33884/cbis.v10i2.5774.

[4] R. Von Solms and J. Van Niekerk, "From Information Security to Cyber Security," *Comput Secur*, vol. 38, pp. 97–102, 2013, doi: 10.1016/j.cose.2013.04.004.

[5] Muhaemin, "Mengembangkan Busines Continuity Planning (BCP)dengan Pendekatan Kuantitatif Studi Kasus: SIAK –DITJEN ADMINDUK KEMENDAGRI," *Jurnal Sistem Informasi, Teknologi Informatika dan Komputer*, vol. 9, no. BCP, DRP, SIAK, pp. 1–11, 2018, doi: 10.24853/justit.9.1.1-11.

[6] NIST, "https://www.nist.gov/cyberframework," cyberframework@nist.gov.

[7] Unitrends, "What is a Business Continuity plan and how can it improve business resilience?," Unitrends. Accessed: Sep. 20, 2023. [Online]. Available: https://www-unitrends-com.translate.goog/blog/business-continuity-plan?_x_tr_sl=en&_x_tr_tl=id&_x_tr_hl=id&_x_tr_pto=tc

[8] N. at al Musyaffa, "Disaster Recovery Plan Jaringan dengan Sistem Backup Otomatis Mikrotik Menggunakan Metode File Transfer Protocol (FTP) pada Jaringan WAN PT. INDOTRANS DATA," *Jurnal Khatulistiwa Informatika*, vol. VIII, no. DRP, pp. 1–7, 2020, doi: 10.31294/jki.v8i1.7724.

[9] A. A. Kuncoro, "Prinsip Dasar Keamanan Informasi Dalam Jaringan Komputer," https://teknik-informatika-s1.stekom.ac.id/informasi/baca/Prinsip-Dasar-

Keamanan-Informasi-dalam-Jaringan-Komputer/d8584ee4d4e39c8139bdd6b69154fb9f61e7ab6d.

[10] A. Jain, A. Ross, and S. Pankanti, "Biometrics: a tool for information security. IEEE Tran Inform Forensics Secur," *Information Forensics and Security, IEEE Transactions on*, vol. 1, pp. 125–143, Jun. 2006, doi: 10.1109/TIFS.2006.873653.

[11] Rubiyanto, Selo, and Widyawan, "Implementasi Role-Based Access Control (RBAC) pada Pemanfaatan Data Kependudukan Ditingkat Kabupaten," *Poster 021*, pp. 1–10, 2017, Accessed: Jul. 18, 2024. [Online]. Available: https://api.semanticscholar.org/CorpusID:86815480

[12] NIST, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," Gaithersburg, MD, Apr. 2018. doi: 10.6028/NIST.CSWP.04162018.

[13] I. G. T. Isa, "Implementasi Pendekatan Kerangka Kerja NIST 800-34 dalam Perancangan Disaster Recovery Plan pada Sistem Informasi Akademik Universitas Muhammadiyah Sukabumi," *Informatika Mulawarman : Jurnal Ilmiah Ilmu Komputer*, vol. 15, no. 2, p. 103, Sep. 2020, doi: 10.30872/jim.v15i2.3724.

[14] Moh. S. Arifin *et al.*, *Sistem Informasi Manajemen*, Maret 2023., vol. Pertama. Padang: PT Global Eksekutif Teknologi, 2023.

[15] A. Oktaviyana, M. B. Aritonang, and E. S. Sembiring, "Analisis dan Pengembangan Sistem Informasi Manajemen," 2023. doi: 10.31219/osf.io/emw2r.

[16] A. Sadikin and N. Wiranda, "Sistem Informasi Manajemen," *Book*, vol. 1, no. SIM, pp. 1–112, Mar. 2022, Accessed: Dec. 15, 2023. [Online]. Available: http://digilib.iain-palangkaraya.ac.id/3890/

[17] Nurhanudin, "Designing a Disaster Recovery Plan using NIST 800-34 Framework on the Information System of the Directorate General of Hajj and Umrah," 2021. doi: 10.38101/sisfotek.v11i2.391.

[18] I. R. Yunita and N. Syafi'ah, "Pengembangan Disaster Recovery Plan Menghadapi Pandemi," 2021. doi: 10.51903/jtikp.v12i1.220.

[19] B. F. Aprilla and D. Yulhendra, "Penerapan Metode HIRARC dalam Menganalisis Risiko Bahaya dan Upaya Pengendalian Kecelakaan Kerja di Area Crusher dan Belt Conveyor PT. Semen Padang," *Jurnal Bina Tambang*, vol. 8, no. 1, 2023, Accessed: Aug. 07, 2024. [Online]. Available: https://ejournal.unp.ac.id/index.php/mining/article/download/122189/107468