EVALUASI PENYIMPANAN *FILE* DAN *BACKUP* TERHADAP RISIKO BENCANA DI SERVER FASILKOM

EVALUATION OF DISASTER RISK FILE STORAGE AND BACKUP IN FASILKOM SERVER

Dinda Adisty Yudianto Putri[1], Efriza Cahya Narendra[1], Fadiyah Dhara Al Arsya[1], Siti Mukaromah[1]
E-mail: dndadisty@gmail.com

[1]Sistem Informasi, Fakultas Ilmu Komputer, UPN"Veteran" Jawa Timur

Abstrak

Sebagai pengelola dan penyedia layanan data, server bertanggung jawab untuk menyimpan data, memproses informasi, memberikan akses ke jaringan atau internet, serta menjalankan aplikasi yang terdapat di dalam jaringan tersebut. Di Fakultas Ilmu Komputer UPN "Veteran" Jawa Timur sendiri terdapat server yang bertugas untuk mengintegrasi seluruh data dalam *website* Fakultas Ilmu Komputer dan berfungsi untuk mengumpulkan, menyimpan, dan mengolah data ajuan administrasi mahasiswa. Oleh karena itu, Fakultas Ilmu Komputer diharapkan dapat menjaga servernya selalu aman dan tertata dalam hal *file storage* dan *backup*. Penulis berinisiatif untuk melakukan evaluasi terhadap ancaman yang terjadi pada server Fakultas Ilmu Komputer. Dengan menggunakan metode penelitian terapan, penulis menemukan 9 ancaman atas dasar observasi yang telah dilakukan kepada pihak pengelola server, dimana 4 dari 9 ancaman tersebut menduduki kategori *Medium* dan *High* dengan kemungkinan dan dampak kejadian cukup besar. Untuk mengatasi hal tersebut, penulis menyarankan untuk membuat *backup* data dan *recovery* sebagai rekomendasi umum yang dapat diterapkan. Berkaca kepada hasil yang penulis temukan pada artikel ini evaluasi sangat diperlukan terutama pada dua kategori ancaman tersebut, yang secara umum dapat diselesaikan dengan menyediakan penyimpanan *backup* data dan *recovery* yang tepat serta tindakan *monitoring* pada setiap ancaman yang diperkirakan akan terjadi.
Kata kunci; *penyimpanan file, back-up, risiko bencana, server*

Abstract

As a manager and provider of data services, the server is responsible for storing data, processing information, providing access to the network or the internet, and running applications contained in the network. At the Faculty of Computer Science UPN "Veteran" East Java itself there is a server whose job is to integrate all data on the Faculty of Computer Science website and functions to collect, store, and process data on student administrative submissions. Therefore, the Faculty of Computer Science is expected to be able to keep its servers safe and organized in terms of file storage and backups. The author took the initiative to evaluate the threats that occur on the Faculty of Computer Science server. By using applied research methods, the authors found 9 threats on the basis of observations that had been made to the server manager, where 4 of the 9 threats occupied the Medium and High categories with the probability and impact of events being quite large. To overcome this, the authors suggest backing up data and recovery as a general recommendation that can be applied. Reflecting on the results that the authors found in this article, evaluation is needed, especially in these two categories of threats, which in general can

be solved by providing proper data backup and recovery storage as well as monitoring actions for any threats that are expected to occur.
***Keywords**: file storage, back-up, disaster risk, servers*

1. PENDAHULUAN

Server merupakan sistem atau komputer yang terdapat pada suatu jaringan dan berfungsi untuk menyediakan layanan kepada *client* [1]. Sebagai pusat pengelolaan dan penyediaan layanan, server bertanggung jawab untuk menyimpan data, memproses informasi, memberikan akses ke jaringan atau internet, serta menjalankan aplikasi yang terdapat di dalam jaringan tersebut. Server dapat berbentuk perangkat keras atau perangkat lunak. Perangkat keras server adalah komputer yang dirancang secara khusus untuk menyediakan layanan server. Sedangkan, perangkat lunak server adalah program yang berjalan di dalam sistem operasi dan juga bertindak untuk menyediakan layanan server.

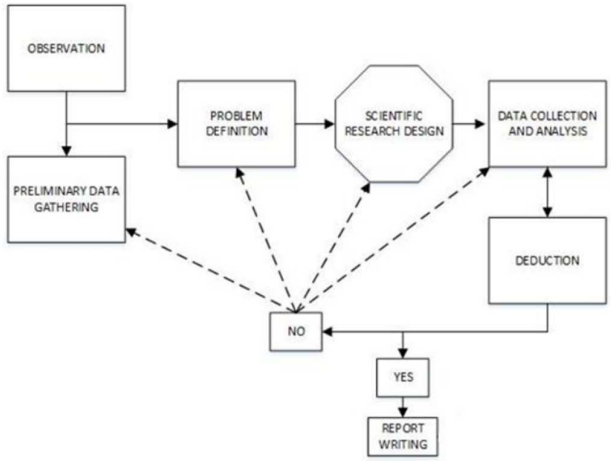
Berdasarkan Undang-undang Nomor 24 Tahun 2007 Tentang Penanggulangan Bencana [2], bencana adalah peristiwa yang mengancam dan mengganggu kehidupan dan penghidupan masyarakat yang disebabkan oleh faktor alam. faktor non-alam, maupun faktor manusia sehingga mengakibatkan timbulnya korban jiwa, kerusakan lingkungan, kerugian harta benda, dan dampak psikologis. The Atlas of the Human Planet 2017 [3] menunjukkan data ancaman bencana telah meningkat sebesar dua kali lipat dalam 40 tahun kebelakang seiring berkembangnya jumlah populasi dunia. Indonesia sendiri memiliki bencana tahunan berupa banjir, tanah longsor, dan puting beliung yang sering terjadi dalam periode 2010-2020 dengan catatan tertinggi pada tahun 2019, yakni 3.814 kejadian [4].

Fakultas Ilmu Komputer UPN "Veteran" Jawa Timur adalah salah satu fakultas yang menyediakan *website* berisi tentang informasi fakultas maupun per program studi, layanan untuk mengurus administrasi keperluan mahasiswa, dan bantuan *online* yang diperlukan oleh mahasiswa Fakultas Ilmu Komputer. Seluruh data dalam *website* Fakultas Ilmu Komputer terintegrasi dengan server yang berada pada gedung FIK 2. Server ini berfungsi untuk mengumpulkan, menyimpan, dan mengolah data ajuan administrasi mahasiswa. Kesiapan server Fakultas Ilmu Komputer ini dituntut untuk menjadi aman terhadap segala ancaman. Tujuan dari artikel ini adalah untuk mengevaluasi sejauh mana sistem penyimpanan file dan backup yang terdapat pada server Fakultas Ilmu Komputer mampu mengatasi risiko bencana yang terjadi. Maka dari itu, Fakultas Ilmu Komputer diharapkan dapat menjaga servernya selalu tertata dalam hal *file storage* and *backup*.

2. METODOLOGI

2.1 Penelitian Terapan

Penelitian terapan merupakan metode penelitian yang memiliki alasan praktis dan keinginan untuk mengetahui lebih lanjut. Metode ini bertujuan untuk dapat melakukan sesuatu yang jauh lebih baik, efektif, dan efisien. artikel terapan yang juga disebut sebagai *applied research* dilakukan bertepatan dengan fakta-fakta dan pengembangan ilmu pengetahuan berdasarkan artikel dasar pada kehidupan nyata. Fungsi dari metode ini adalah menemukan solusi tentang masalah tertentu. Sementara itu, tujuan utamanya adalah memecahkan masalah pada hasil artikel agar dapat dimanfaatkan untuk kepentingan bersama dan tidak sekedar untuk wawasan keilmuan [5].



Gambar 1. Metode Penelitian Terapan

Pada Gambar 1 terdapat beberapa simbol yang memiliki arti tersendiri. Penjelasan untuk arti dari masing-masing simbol dapat dilihat pada Tabel 1.

Tabel 1. Penjelasan Simbol Metode Penelitian Terapan

No.	Simbol	Penjelasan
1.	Entitas segi 4	Proses yang akan dilakukan
2.	Entitas segi 8	Proses yang memungkinkan adanya penyesuaian
3.	Garis panah tebal 1 arah	Penunjuk arah aliran proses penelitian terapan
4.	Garis panah tebal 2 arah	Penunjuk arah aliran 2 (atau lebih) proses penelitian terapan yang dilakukan secara bersamaan (paralel)
5.	Garis panah putus-putus 1 arah	Penunjuk arah aliran proses penelitian terapan yang dimana arah panah ditentukan oleh hasil proses sebelumnya

Metode penelitian terapan dimulai dari tahap *observation* (observasi) yang digambarkan dengan garis tebal satu arah terhadap permasalahan yang akan dituangkan pada artikel. Setelah melakukan observasi, tahapan selanjutnya adalah *preliminary data gathering* (pengumpulan data awal) dengan kondisi data yang tersedia tidak cukup lengkap untuk dapat digunakan dalam identifikasi permasalahan dan tahap *problem definition* (definisi masalah) untuk mendefinisikan masalah yang akan dibahas. Kedua tahap tersebut berjalan secara beriringan dilihat pada garis panah yang digambarkan. Jika tahap *problem definition* telah dilakukan, tahap selanjutnya adalah membuat *scientific research design* (desain penelitian ilmiah) sebagai jembatan untuk mengintegrasikan berbagai komponen penelitian, seperti metode yang digunakan, jenis data dan pertanyaan untuk wawancara. Selanjutnya adalah tahap *data collection and analysis* (koleksi data dan analisis) dengan tujuan untuk mengumpulkan data yang sesuai dalam permasalahan untuk ditelaah dalam artikel ini. Pada tahap selanjutnya adalah *deduction* (deduksi) yang digambarkan

dengan garis tebal dua arah terhadap tahapan *data collection and analysis* yang berarti penarikan kesimpulan dari hasil data yang telah diulas. Jika tahap *deduction* sesuai dengan tujuan artikel dan hasil pembahasan, maka tahap selanjutnya adalah *report writing* (penulisan laporan) sebagai penulisan laporan untuk hasil kesimpulan yang telah diambil. Jika tidak sesuai, maka akan diarahkan kembali ke tahap yang sekiranya memiliki hasil kurang sesuai digambarkan dengan garis putus-putus satu arah pada masing-masing tahapan. Tahapan-tahapan pada metode ini ditunjukkan dalam Gambar 1 [6].

3. HASIL DAN PEMBAHASAN

3.1 Identifikasi Ancaman

Identifikasi ancaman ini berfokus untuk menjabarkan ancaman yang memiliki pengaruh terhadap fasilitas-fasilitas ruangan server Fakultas Ilmu Komputer UPN "Veteran" Jawa Timur dan komputer lain yang terhubung dengan sistem. Identifikasi ancaman dibutuhkan untuk mengelompokkan penyebab dan dampak terjadinya ancaman yang mungkin terjadi dan bermanfaat untuk menentukan tahap-tahap yang sesuai untuk mengurangi risiko yang terjadi [7]. Risiko yang terjadi pada ruangan server dan gedung fakultas dapat merusak aset-aset penting yang terdapat di dalamnya. Aset penting yang dipilih adalah aset yang berharga bagi Fakultas Ilmu Komputer yang berhubungan dengan informasi, baik berupa data, *hardware*, *software*, maupun jaringan [8]. Ancaman terhadap aset juga harus diperhatikan karena aset adalah sebuah sumber daya berupa benda yang dapat menopang seluruh aktivitas yang berlangsung. Dalam hal ini, aktivitas yang dimaksud adalah proses administrasi sesuai permintaan mahasiswa yang dilakukan oleh pegawai tata usaha Fakultas Ilmu Komputer seperti pembuatan surat, pendaftaran skripsi dan pendaftaran yudisium.

Hasil dari observasi yang telah dilakukan mengenai ancaman yang dapat timbul, data kerentanan terhadap ancaman, aset penting, dan konsekuensi atas ancaman yang terjadi dituliskan dalam bentuk narasi seperti pada Tabel 2.

Tabel 2. Tabel Identifikasi Ancaman yang Terjadi

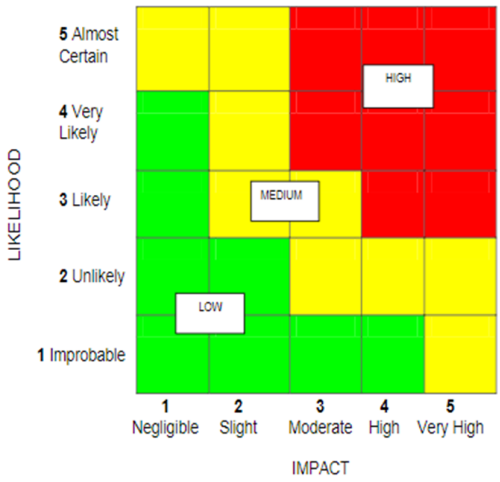
No.	Ancaman	Kejadian Ancaman	Kerentanan	Aset Penting	Konsekuensi
1.	Aliran listrik putus	Mengakibatkan listrik mengalami instabilitas dalam penggunaannya pada perangkat komputer	Server dan perangkat komputer tidak dapat berfungsi karena harus tersambung ke aliran listrik	Server dan komputer	Perangkat komputer tidak dapat digunakan
2.	Gempa bumi	Merusak server dan jaringan komputer lain yang terhubung	Server terletak dalam gedung yang kurang tahan gempa	Ruangan server dan gedung FIK 2	Kerusakan fasilitas ruangan dan gedung FIK 2 serta alat server tersebut

3.	Kebakaran	Menimbulkan api yang disebabkan oleh korsleting listrik atau sumber api lainnya	Ruangan server kemungkinan dapat terbakar karena terdapat banyak kertas	Ruangan server dan gedung FIK 2	Kerusakan fasilitas ruangan dan gedung FIK 2 serta alat server tersebut
4.	Petir	Menyebabkan kerusakan jaringan listrik di server dan komputer yang terhubung	Petir dapat menyambar server	Server, komputer, dan ruangan server	Rusaknya alat-alat yang tersambar petir
5.	Jaringan komputer mati	Terdapat perangkat jaringan yang rusak atau perangkat yang telah kelebihan beban kerja	penanggung jawab server tidak mengetahui kelebihan beban pada perangkat jaringan	Server dan komputer	Terjadi kerusakan pada perangkat komputer
6.	Serangan virus, *worm*, atau *malware*	Terdapat *bugs* pada aplikasi atau sistem yang digunakan pada komputer jaringan karena serangan virus, *worm*, atau *malware*	Aplikasi atau sistem yang digunakan terdapat *bugs*	Informasi dan data	Aplikasi atau sistem dapat kehilangan data
7.	Kegagalan server dan penyimpanan	Server mengalami penurunan kemampuan karena beban kerja server dan penyimpanan telah melebihi batas	Pemrosesan data menjadi lebih lama	Informasi, komputer	Sistem atau aplikasi tidak dapat dijalankan dengan baik serta data pada sistem tidak dapat di *backup*
8.	Ancaman *cyber*	Keamanan pada sistem memiliki celah yang dapat ditembus untuk mengambil data	Pemanipulasian akun oleh pihak tidak bertanggungjawab karena	Informasi, reputasi	Data administrasi fakultas akan bocor dan reputasi

		fakultas	kata sandi yang lemah		fakultas akan rusak
9.	*Human error*	Menyebabkan kerusakan pada fasilitas atau sistem pada ruangan server	Tidak terdapat SOP resmi pada ruangan server	Server	Kerusakan pada server atau perangkat lain yang terhubung

3.2 Evaluasi Ancaman

Kriteria risiko adalah ukuran standar tentang seberapa besar kemungkinan dampak atau konsekuensi akan terjadi dan seberapa besar kemungkinan atau frekuensi risiko akan terjadi. Matriks kriteria risiko diambil untuk referensi dari jurnal yang memiliki penggunaan matriks serupa [9]. Matriks tersebut menggunakan tabel kemungkinan dan dampak 5x5 yang terdiri atas 5 tingkat kemungkinan dan 5 tingkat dampak yang dapat dilihat pada Gambar 1. Maka, semakin besar nilainya maka semakin sering terjadi risiko dan semakin besar dampak yang akan ditimbulkan [10]. Untuk mengetahui standar dan kriteria dampak yang timbul dari setiap penilaian ancaman, ajuan atas kriteria kemungkinan dan dampak dapat diterapkan setelah diverifikasi oleh penanggung jawab server Fakultas Ilmu Komputer UPN "Veteran" Jawa Timur.



Gambar 2. Matriks Kriteria Risiko

Berdasarkan matriks *risk criteria* atau kriteria ancaman (Gambar 2), kategori ancaman dibagi menjadi tiga yaitu *Low*, *Medium*, dan *High* setelah ditentukan oleh variabel *likelihood* (kemungkinan) dan *impact* (dampak). Kategori tersebut dapat memudahkan dalam mengklasifikasikan ancaman yang perlu menjadi pusat perhatian lebih dan tidak.

Tabel 3. Evaluasi atas Ancaman yang Terjadi

No.	Ancaman	Nilai Kemungkinan	Nilai Dampak	Kategori
1.	Aliran listrik putus	5	5	*High*
2.	Gempa bumi	2	3	*Medium*
3.	Kebakaran	3	5	*High*
4.	Petir	1	1	*Low*
5.	Jaringan komputer mati	1	4	*Low*
6.	Serangan virus, *worm*, atau *malware*	5	2	*Low*
7.	Kegagalan server dan penyimpanan	2	2	*Low*
8.	Ancaman *cyber*	3	3	*Medium*
9.	*Human error*	2	2	*Low*

Ancaman dengan kategori *Low* dapat dianggap sebagai ancaman kecil yang tidak terlalu berpengaruh terhadap kinerja server. Selanjutnya, ancaman dengan kategori *Medium* mulai harus dianggap dan diwaspadai sebagai ancaman yang memiliki pengaruh terhadap kinerja server. Kategori ini pun terpantau memiliki jumlah ancaman paling banyak daripada kategori lain. Sementara itu, untuk kategori *High* terlihat hanya memiliki dua ancaman yaitu aliran listrik putus dan kebakaran. Meskipun hanya dua ancaman yang masuk dalam kategori *High*, penanggung jawab server dan monitor harus tetap memperhatikan jika ancaman tersebut mulai menyerang.

3.3 Rekomendasi Ancaman

Tabel 4. Tabel Rekomendasi dari Ancaman yang Terjadi

No.	Ancaman	Kontrol yang Telah Disediakan	Kontrol yang Direkomendasikan
1.	Aliran listrik putus	Menyediakan UPS (*Uninterruptible Power Supply*)	Menggunakan UPS yang memadai, merawat UPS secara

		dengan daya tahan 30 menit untuk persiapan *shut down* pada komputer	teratur, dan mengimplementasikan protokol *shut down* yang tepat
2.	Gempa bumi	Belum terdapat sistem yang berfungsi untuk mencegah gempa bumi pada gedung FIK 2	Melakukan penyimpanan data *offsite* agar pemulihan data dapat dilakukan dengan cepat setelah gempa bumi
3.	Kebakaran	Ruangan server dilengkapi dengan sebuah *hydrant*	Memasang pendeteksi api di ruangan server agar tindakan penanggulangan dapat segera diambil jika terdeteksi api
4.	Petir	Terdapat UPS anti petir untuk mencegah petir secara langsung mengenai jaringan server	Memasang sistem *grounding* dan *surge* (transien) protector dengan standar keamanan yang relevan
5.	Jaringan komputer mati	Adanya notifikasi jika komputer jaringan tidak terhubung ke server	Melakukan *monitoring* komputer jaringan dan server serta mengatur konfigurasi *firewall* dengan bijak
6.	Serangan virus, *worm*, atau *malware*	Menerapkan sistem *file sharing* pada setiap monitor yang terhubung kepada server	Menggunakan VLAN (*Virtual Local Area Network*) untuk memisahkan jaringan dan enkripsi seperti SSH *(Secure Shell*) atau SSL (*Secure Sockets Layer*) untuk mengamankan data
7.	Kegagalan server dan penyimpanan	Menerapkan RAID (*Redundant Array of Independent Disks*) *mirroring* untuk server dan komputer yang terhubung	Melakukan *monitoring* dan pemeliharaan rutin, serta penggantian *hardware* yang terjadwal dengan baik
8.	Ancaman *cyber*	Password untuk admin *monitor* menganut dari server sehingga kombinasi *password* selalu aman	Menggunakan MFA (*Multi-factor Authentication*) serta melakukan penyaringan dan proteksi *email*
9.	*Human error*	Belum terdapat SOP (Standar Operasional Prosedur) resmi terbitan dari Fakultas Ilmu Komputer.	Membuat pelatihan dan memberikan panduan untuk pengoperasian data center oleh pegawai pengoperasian server

Pada Tabel 4, rekomendasi tindakan yang dapat dilakukan oleh pihak Fakultas Ilmu Komputer terutama penanggung jawab server berdasarkan ancaman yang telah disebutkan adalah melakukan monitoring terhadap server dan komputer yang terhubung.

4. KESIMPULAN DAN SARAN

4.1 Kesimpulan

Artikel dengan studi kasus di Fakultas Ilmu Komputer UPN "Veteran" Jawa Timur ini membahas mengenai evaluasi risiko bencana terhadap *file storage* dan *backup* di server yang berisikan tentang data administrasi permintaan mahasiswa menggunakan metode penelitian terapan.

Melalui identifikasi ancaman yang dituangkan pada Tabel 1, telah ditemukan 9 perkiraan ancaman yang dapat terjadi pada server. Ancaman-ancaman tersebut berdampak pada rusaknya aset penting seperti server, komputer jaringan, ruangan server, gedung FIK 2, informasi dan data dari server, serta reputasi dari Fakultas Ilmu Komputer itu sendiri. Dampak lain atas terjadinya ancaman-ancaman tersebut adalah berhentinya proses bisnis dari Fakultas Ilmu Komputer seperti pembuatan surat, pendaftaran skripsi, dan pendaftaran yudisium.

Setelah identifikasi ancaman dilakukan, selanjutnya adalah tahap wawancara kepada penanggung jawab server. Hasil dari wawancara tersebut dituangkan ke dalam Tabel 2 yang berisi nilai kemungkinan dan nilai dampak atas ancaman yang terjadi. Pedoman yang digunakan dalam tahap ini adalah matriks kriteria risiko yang memiliki 3 kategori ancaman diukur dari variabel *likelihood* dan *impact*. Kategori *Low* berisikan 5 ancaman, kategori *Medium* berisikan 2 ancaman, dan kategori *High* berisikan 2 ancaman.

Beberapa ancaman pada Tabel 2 telah disediakan kontrol yang cukup memadai oleh pihak penanggung jawab server. Adapun juga kontrol yang kurang memadai contohnya adalah pada ancaman human error dan gempa bumi yang mana belum adanya sistem dan SOP untuk menanggulanginya. Namun, untuk ancaman dengan kategori *Medium* dan *High* perlu kontrol yang lebih serius dari yang telah disediakan. Untuk itu, harus diberikan evaluasi terhadap kontrol yang diberikan kepada dua kategori ancaman tersebut secara umum berupa penyimpanan backup data yang tepat dan tindakan *monitoring* pada setiap ancaman yang diperkirakan akan terjadi.

4.2 Saran

Keamanan server merupakan hal yang penting untuk diperhatikan dalam pemeliharaan fasilitas dalam Fakultas Ilmu Komputer. Keamanan yang baik dapat menjamin sedikit adanya ancaman gangguan yang terjadi pada server. Rekomendasi yang diberikan pada artikel ini cukup membantu untuk mengatasi risiko dalam beberapa ancaman yang akan terjadi. Namun, diharapkan pihak penanggung jawab server tetap memperhatikan keamanan server dengan atau tidak adanya ancaman yang terjadi.

Diharapkan dengan artikel yang dibuat ini dapat menumbuhkan kesadaran masyarakat umum khususnya para pegawai penanggung jawab server akan pentingnya keamanan data atas ancaman-ancaman yang akan dan mungkin telah terjadi.

5. DAFTAR RUJUKAN

[1] A. M. Fanggidae, H. Hermawan, and H. I. Pratiwi, "Sistem Monitoring Server Dengan Menggunakan SNMP," Widyakala J., vol. 6, no. 2, p. 163, 2019, doi: 10.36262/widyakala.v6i2.218.

[2] Indonesia, "Undang-Undang (UU) Nomor 24 Tahun 2007 tentang Penanggulangan Bencana." Sekretariat Negara, Jakarta, 2007.

[3] E. D. Martino, Atlas of the Human Planet 2017: Global Exposure to Natural Hazards. Publications Office of the European Union, 2017.

[4] Y. Pusparisa, "2010-2020: Dekade Penuh Bencana Bagi Indonesia," Databoks Kata Data, 2021. https://databoks.katadata.co.id/datapublish/2021/01/19/2010-2020-dekade-penuh-bencana-bagi-indonesia.

[5] F. Irina, Metode Penelitian Terapan. Yogyakarta: Parama Ilmu, 2017.

[6] R. A. Pratama and E. Amalia, "Analisis dan Evaluasi Penyimpanan File dan Cadangan Risiko Bencana di Pusat Data Diskominfo Analysis and Evaluation of File Storage and Back Up of Disaster Risk in Diskominfo Data Center," J. REKAYASA Sist. DAN Ind., vol. 7, 2020.
[7] Z. Rifai, A. Maydina, and A. A. Kurniawan, "Rancangan Dokumen Disaster Recover Plan Pada IS/IT di Dinas XYZ," Comput. Eng. Sci. Syst. J., vol. 3, no. 2, p. 147, 2018, doi: 10.24114/cess.v3i2.9892.
[8] A. F. Rohman, A. Ambarawati, and E. Setiawan, "ANALISIS MANAJEMEN RISIKO IT DAN KEAMANAN ASET MENGGUNAKAN METODE OCTAVE-S," J. Inf. Technol. Comput. Sci., vol. 3, pp. 298–310, 2020.
[9] 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.
[10] M. I. Fachrezi, A. D. Cahyono, and P. F. Tanaem, "Manajemen Risiko Keamanan Aset Teknologi Informasi Menggunakan ISO 31000 : 2018 Diskominfo Kota Salatiga," J. Tek. Inform. dan Sist. Inf., vol. 8, no. 2, pp. 764–773, 2021.