

Manajemen Risiko Sistem Informasi Mengacu pada NIST SP 800-30 dan NIST SP 800-53 rev.5

Cindy Asari^{1a}, Yulhendri^{2b*}

^aSistem Informasi, Ilmu Komputer, Universitas Esa Unggul, asaricindy21@gmail.com

^bSistem Informasi, Ilmu Komputer, Universitas Esa Unggul, yulhendri@esaunggul.ac.id

Submitted: 19-06-2023, Reviewed: 12-07-2023, Accepted: 07-08-2023

<https://doi.org/10.47233/jteksis.v5i4.898>

Abstract

Through the Research Institute, the Ministry of Agriculture makes use of the website, namely bsip.pertanian.go.id which aims to help users by disseminating information. Where risk management has not been carried out and there are several problems such as data loss in July due to ransomware which caused the data backup to be delayed for several months and had an impact on the website's operations, so in this study an analysis of risk management will be carried out. The goal of this research is to assess the risk and suggestions or recommendations for handling these risks based on the NIST SP 800-30 method in asset identification, assistance, vulnerability assistance, analysis, likelihood control, location analysis, risk recovery, control recommendations with NIST supporting guidelines SP 800-53 rev.5 and result documentation. By using data collection methods in the form of interviews and observations. According to this study, there are 18 risks 2 high, 3 moderate, 7 low and 6 very low at the level of risk assessment and their recommendations for each risk on the bsip.pertanian.go.id website.

Keywords: Website, Risk Management, Recommendations, NIST SP 800-30, NIST SP 800-53 rev.5.

Abstrak

Melalui Balai Penelitian, Kementerian Pertanian memanfaatkan penggunaan *website* yaitu bsip.pertanian.go.id yang bertujuan untuk keperluan membantu pengguna dengan cara penyebaran informasi. Dimana belum dilakukan manajemen risiko dan terdapat beberapa masalah seperti kehilangan data pada bulan Juli akibat terkena *ransomware* yang menyebabkan backup data menjadi mundur beberapa bulan dan berdampak pada operasi *website* tersebut, sehingga pada penelitian kali ini akan dilakukan analisis mengenai manajemen risiko. Tujuan dari penelitian ini adalah untuk menentukan risiko dan saran atau rekomendasi untuk penanganan risiko tersebut yang berdasarkan metode NIST SP 800-30 dalam identifikasi aset, identifikasi ancaman, identifikasi kerentanan, analisis kontrol, penentuan kemungkinan, analisis dampak, penentuan risiko, rekomendasi kontrol dengan pedoman pendukung NIST SP 800-53 rev.5 dan hasil dokumentasi. Dengan menggunakan metode pengumpulan data berupa wawancara dan observasi. Menurut penelitian ini, terdapat 18 risiko diantaranya 2 *high*, 3 *medium*, 7 *low* dan 6 *very low* pada tingkat penilaian risiko beserta rekomendasinya pada setiap risiko pada *website* bsip.pertanian.go.id.

Keywords: Website, Manajemen Risiko, Rekomendasi, NIST SP 800-30, NIST SP 800-53 rev.5.

This work is licensed under Creative Commons Attribution License 4.0 CC-BY International license



PENDAHULUAN

Sistem informasi, sebagai wadah, tentu berperan dalam pelaksanaan Rencana Pengelolaan Teknologi, serta dalam masalah-masalah yang sebanding dengan yang disebutkan dalam Pasal 18, Pasal UU Tahun 2002 Tentang Sistem Riset Nasional. Teknologi sangat penting untuk kemajuan dan penerapan ilmu pengetahuan dan teknologi. Secara operasional untuk memperluas daya dukung ilmu pengetahuan dan teknologi untuk pemanfaatan, serta keberlanjutannya, untuk mempercepat upaya pencapaian tujuan nasional [1]

Teknologi informasi memungkinkan akses cepat dan mudah ke situs berita. Risiko yang terkait dengan penggunaan teknologi informasi dapat membahayakan aset aktual dan tidak berwujud. Tindakan pencegahan dapat mengurangi berbagai bahaya yang terjadi dalam manajemen risiko untuk

mengelola risiko dengan menerapkan kerangka yang tepat.

Melalui Peraturan Presiden Nomor 117 Tahun 2022, Badan Penelitian dan Pengembangan Pertanian (Balitbang Pertanian) berubah namanya menjadi Badan Standardisasi Instrumen Pertanian. Secara khusus, untuk mengembangkan dan mengkoordinasikan standar instrumen pertanian, serta standarisasi penerapan dan pemeliharaannya, sehingga mengubah domain *website* menjadi bsip.pertanian.go.id. Fungsi mana yang juga berubah, terutama standarisasi pertanian daripada penelitian. Publikasi, kemitraan, layanan, profil organisasi, reformasi birokrasi, dan KIP (keterbukaan informasi publik) semuanya tersedia di *website* ini.

Diketahui bahwa selama *website* diterapkan, berbagai masalah yaitu kehilangan data pada bulan Juli akibat terkena *ransomware* yang

menyebabkan backup data menjadi mundur beberapa bulan, *website* yang tidak beroperasi atau diakses, serta mati listrik jarang terjadi, walaupun terjadi hanya musim hujan dan di bantu oleh *Uninterruptible Power Supply (UPS)* dan *Electricity Treatment System (ETS)* yang hanya dapat bertahan hampir sejam saja.

Dari berbagai permasalahan yang muncul tersebut, diperlukan suatu metode yang efektif khususnya dalam *risk assessment* yang dijadikan sebagai inti dari *risk management and control*, dimana yang dilakukan adalah menganalisis aset baik dari sistem maupun teknologi informasi yang memiliki potensi risiko baik ancaman dan dampak, yang menimbulkan kerusakan/gangguan, serta mengakibatkan kerugian.

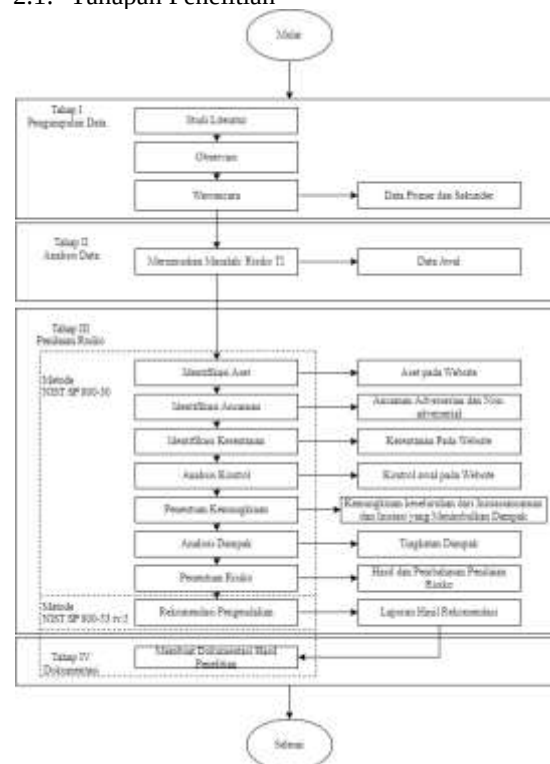
Pemilihan framework NIST SP 800-30 untuk menentukan tingkat risiko implementasi sistem dan teknologi informasi dengan tahapan pada penilaian risiko, dimana memiliki perspektif menilai risiko yang fleksibel untuk organisasi dengan memiliki detail dibandingkan dengan lainnya, melakukan evaluasi dan membuat saran kontrol yang efektif dan luas, sehingga NIST dianggap baik untuk organisasi yang berada di tahap awal pengembangan rencana manajemen risiko. Dan NIST SP 800-53 rev.5 untuk lebih menekankan pada aspek privasi dan keamanan tersebut.

Penelitian sebelumnya [2] yang mana keamanan informasi dengan metode NIST SP 800-30 dengan langkah hingga penentuan risiko dan hasil akhir memiliki 1 tingkat resiko tinggi, 5 tingkat risiko sedang dan 52 tingkat risiko rendah. Dibandingkan dengan penelitian sebelumnya, penelitian ini akan melakukan manajemen risiko hingga rekomendasi kontrol dengan hasil akhir dengan pedoman pendukung yang dapat memberikan tingkat risiko serta rekomendasi kontrol yaitu NIST SP 800-53 rev.5 rekomendasi untuk kontrol keamanan dan privasi yang disesuaikan dengan berbagai kelompok dalam mengurangi risiko yang mengamankan informasi penting dengan baik yang memproses, menyimpan, dan menyampaikan data.

METODE PENELITIAN

Menjelaskan tentang teknik pengumpulan data dengan wawancara, observasi dan studi literatur; objek penelitian pada *website* bsip.pertanian.go.id di BSIP (Badan Standarisasi Instrumen Pertanian) dan metode penilaian risiko dengan NISTSP 800-30 dan pedoman pendukung NIST SP 800-53 rev.5.

2.1. Tahapan Penelitian



Dimulai dari pengumpulan data, analisis data, penilaian risiko dengan bantuan NIST SP 800-30 dan NIST SP 800-53 rev.5, serta dokumentasi.

2.2. Objek Penelitian

Di BSIP (Badan Standarisasi Instrumen Pertanian), pada penelitian ini penulis mengambil data tentang sistem dan teknologi informasi pada *website* bsip.pertanian.go.id. Dimana belum dilakukan manajemen risiko, sehingga pada penelitian kali ini akan dilakukan analisis mengenai manajemen risiko.

2.3. Pengumpulan data

Pendekatan penelitian kualitatif diterapkan dalam penelitian ini. Penelitian kualitatif adalah metode pengumpulan data deskriptif individu, bahasa tertulis dan lisan digunakan untuk menggambarkan perilaku yang diamati.

2.3.1 Data Primer

Data dari hasil observasi serta wawancara pada *website* pada BSIP (Badan Standarisasi Instrumen Pertanian). Dimana dilakukan wawancara kepada Pranata Komputer Pertama dan Pranata Humas Muda selaku staff IT bagian teknis dan konten. Dengan narasumber sebagai berikut:

Tabel 1 Narasumber

Narasumber	Keterangan
Sony hanjaya	Staff IT (Bagian

Narasumber	Keterangan
Tundunsekar	Teknisi
Rahmi Juwita Sukma	Staff IT (Bagian Konten)
Vevi Martina	Pengguna
Muhammad Adi	Pengguna
Pramilania	Pengguna
Doni Permana	Pengguna
Neviana	Pengguna
Rieo Aji	Pengguna
Widya	Pengguna
Nadia Husain	Pengguna
Cahya Faradila	Pengguna

2.3.2 Data Sekunder

Sebagai penunjang, data diperoleh dari publikasi dan penelitian mengenai studi yang sedang dilakukan. Merujuk pada penelitian sejenis yang sudah dilakukan oleh [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19] dan [20].

2.4 Analisis Data

Dalam tahap analisis risiko dari observasi dan wawancara yang dilakukan yaitu selama pada di *website* bsip.pertanian.go.id diterapkan dengan diidentifikasi risiko yang ada yaitu terdapat *virus malware*, *kehilangan data*, *pencurian data*, *kegagalan backup*, *server down*, *kegagalan penggunaan password* dan *pemadaman listrik*.

2.5 Penilaian Risiko

Merujuk dalam tahap penggunaan teknik NIST SP 800-30 untuk mendukung penelitian pada *website* bsip.pertanian.go.id, sebagai berikut:

- **Identifikasi Aset:** mengidentifikasi ruang lingkup sistem dan teknologi informasi pada *website* BSIP (Badan Standarisasi Instrumen Pertanian) melalui mengamati dan mewawancarai dan mengumpulkan fakta dan informasi.
- **Identifikasi Ancaman:** mengidentifikasi berbagai ancaman adversarial dan non-adversarial pada *website* yang berpotensi merusak fungsi sistem tersebut.
- **Identifikasi Kerentanan:** mengembangkan daftar kekurangan maupun kelemahan yang ada pada sistem dan teknologi informasi di *website* bsip.pertanian.go.id yang dapat dipicu atau disebabkan oleh ancaman.
- **Analisis Kontrol:** menganalisis kerentanan sistem dengan mendokumentasikan dan mengevaluasi keefektifan tindakan teknis dan non-teknis untuk mengurangi potensi risiko.

- **Penentuan Kemungkinan (*Likehood*):** menilai keseluruhan dari kemungkinan pada sumber ancaman di *website* dengan skala penilaian kemungkinan inisiasi kejadian adversarial dan non-adversarial dan skala penilaian kemungkinan inisiasi kejadian ancaman yang mengakibatkan dampak.
- **Analisis Dampak:** membuat tingkatan dari pada dampak negatif pada *website* dengan skala penilaian dampak kejadian ancaman dengan hasil yaitu daftar dampak dari asset serta tingkat dampak tersebut.
- **Penentuan Risiko:** penetapan Risiko diurutkan meningkatkan nilai dari terendah ke tertinggi atau melalui besaran *likelihood* dan *impact*, lalu dihitung dengan menggunakan tabel *matriks* penilaian risiko pada tingkat risiko.
- **Rekomendasi Kontrol:** mengidentifikasi kontrol untuk mengurangi ataupun menghilangkan risiko yang berdasarkan pada pedoman pendukung NIST SP 800-53 rev.5 yang disesuaikan dengan 20 kelompok kontrol yang ada.

Tabel 2 Kelompok Kontrol

ID	Kelompok	ID	Kelompok
AC	Access Control (Kontrol akses)	PE	Physical and Environmental Protection (Perlindungan Fisik dan Lingkungan)
AT	Awareness and Training (Kesadaran dan Pelatihan)	PL	Planning (Perencanaan)
AU	Audit and Accountability (Audit dan Akuntabilitas)	PM	Program Management (Manajemen Program)
CA	Access Control (Kontrol akses)	PE	Physical and Environmental Protection (Perlindungan Fisik dan Lingkungan)
CM	Awareness and Training (Kesadaran dan Pelatihan)	PL	Planning (Perencanaan)
CP	Audit and Accountability (Audit dan Akuntabilitas)	PM	Program Management (Manajemen Program)
IA	Assessment, Authorization, and Monitoring (Penilaian, Otorisasi, dan Pemantauan)	PS	Personnel Security (Keamanan Personil)
IR	Configuration Management	PT	PII Processing and Transparency

	(Manajemen konfigurasi)		(Pemrosesan dan Transparansi PII)
MA	<i>Contingency Planning</i> (Perencanaan kontingensi)	RA	<i>Risk Assessment</i> (Penilaian Risiko)
MP	<i>Identification and Authentication</i> (Identifikasi dan Otentikasi)	SA	<i>System and Services Acquisition</i> (Akuisisi Sistem dan Layanan)

Sumber: NIST SP 800-53 rev.5 2020

2.6 Hasil Dokumentasi

Tahapan ini yaitu penulis akan membuat dokumentasi dari penilaian risiko yang dihasilkan dan dijadikan bentuk laporan secara resmi dan memberikannya kepada pihak yang bersangkutan untuk mengurangi risiko tersebut.

HASIL DAN PEMBAHASAN

Menjelaskan tentang penilaian risiko yang ada pada *website* bsp.pertanian.go.id dengan bantuan NIST SP 800-30 untuk manajemen risiko sendiri yang berfokus pada sistem dan teknologi informasi yang ada pada *website* tersebut. Langkahnya dengan identifikasi aset pada asset yaitu *software*, *hardware*, data manusia dan infrastruktur; identifikasi ancaman yang berkemungkinan ada; identifikasi kerentanan serta menentukan tingkatannya; analisis kontrol yang ada sekarang; penentuan kemungkinan serta menentukan tingkatannya; analisis dampak; penentuan risiko dengan menentukan tingkatannya; rekomendasi kontrol dengan pedoman pendukung NIST SP 800-53 rev.5 yang disesuaikan dengan 20 kelompok kontrol yang ada dan hasil dokumentasi.

3.1. Identifikasi Aset

Tahapan ini yaitu akan mengidentifikasi lingkup sistem dan teknologi informasi pada *website* bsp.pertanian.go.id di BSIP (Badan Standarisasi Instrumen Pertanian), karena berbagai aset tersebut dapat menyebabkan risiko yang mana tidak terlepas dari berbagai serangan. Yang mana aset tersebut diakses dan dikelola oleh *stakeholder* yaitu staff IT pada BSIP (Badan Standarisasi Instrumen Pertanian) selaku pengawas. Aset yang didapatkan yaitu terdapat pada tabel 3 berikut:

Tabel 3 Identifikasi Aset

Jenis Aset	Nama Aset	Stakeholder
Hardware	Komputer/PC (Dell OptiPlex 9010)	Staff IT (Bagian Teknis)
	Server (Memori 4 GB, <i>processors</i> 4, <i>hard disk</i> 100 GB,	Staff IT (Bagian Teknis)

Jenis Aset	Nama Aset	Stakeholder
Software	<i>network adapter bridged (automatic)</i> . Router	Staff IT (Bagian Teknis)
	Ubuntu (Ubuntu 16.04.5 LTS (GNU/Linux 4.4.0-210- generic x86 64).	Staff IT (Bagian Teknis)
	Laravel 8.0	Staff IT (Bagian Teknis)
Data dan Informasi	Postgresql 13	Staff IT (Bagian Teknis)
	Data Publikasi (Buku, Pedum/ Juknis dan Siaran Pers, maupun berita).	Staff IT (Bagian Konten)
	Data Kerja Sama (Kegiatan penelitian, pengkayasaan, pengkajian dan pengembangan).	Staff IT (Bagian Konten)
	Data Layanan (Pengujian dan kesesuaian standar seperti tanaman pangan, alat dan mesin pertanian, perkebunan peternakan, hortikultura. Dan pasca panen. Serta pada penerbitan, pengaduan, pengadaan)	Staff IT (Bagian Konten)
	Data Organisasi (Profil, Visi & Misi, Struktur Organisasi, Tugas & Fungsi, Pimpinan, Renstra (Rencana Strategis), Satuan Kerja, Sumberdaya dan Kerjasama).	Staff IT (Bagian Konten)
	Data Reformasi Birokrasi (Manajemen Perubahan, Deregulasi Kebijakan, Penataan Dan Penguatan Organisasi, Penataan Tata Laksana, Penataan Sistem Manajemen SDM, Penguatan Akuntabilitas, Penguatan Pengawasan, Peningkatan Kualitas dan Pelayanan Publik).	Staff IT (Bagian Konten)
	Data Keterbukaan Informasi Publik (KIP) (Portal PPID, Pengelolaan Informasi Publik, Rencana Kinerja Tahunan (RKT), Anggaran, LAKIP/ LAKIN, Laporan Tahunan, Regulasi, Laporan Kekayaan, Indeks Kepuasan Masyarakat dan Agenda Kegiatan).	Staff IT (Bagian Konten)
Sumber Daya Manusia (SDM)	Staff IT Bagian Teknis (Pranata Komputer Pertama)	Staff IT (Bagian Teknis)
	Staff IT Bagian Konten (Pranata Humas Muda)	Staff IT (Bagian Konten)

Jenis Aset	Nama Aset	Stakeholder
Infrastruktur	Ruang Server	Staff IT (Bagian Teknis)
	Listrik	Staff IT (Bagian Teknis)

3.2. Identifikasi Ancaman

Tahapan ini yaitu akan mengidentifikasi berbagai ancaman pada *website* bsip.pertanian.go.id dengan hasil berupa berbagai daftar sumber ancaman yang berpotensi merusak maupun mengganggu fungsi dari sistem tersebut. Terdapat berbagai sumber ancaman beserta kejadian ancaman adversarial dan non-adversarial yaitu pada tabel 4 berikut:

Tabel 4 Ancaman

Jenis Aset	Sumber Ancaman
Hardware	Kerusakan pada aset yang sudah menua ataupun rusak.
Software	Adanya serangan <i>malware</i> atau <i>virus</i> yang disebabkan oleh pihak luar/dalam.
	Update sistem yang belum dilakukan menyebabkan sistem berhenti/error.
	Windows tidak berjalan semestinya.
	Pemanfaatan celah keamanan oleh pihak dalam/luar.
Data dan Informasi	Server Down yang menyebabkan halaman tidak bisa diakses.
	Pencurian pada aset data sehingga bisa terjadinya permasalahan pada semua sistem.
	Kehilangan data yang sifatnya sensitif.
SDM (Sumber Daya Manusia)	Kegagalan Backup
	Menggunakan <i>password</i> yang lemah/default <i>password</i> .
	Terjadi kesalahan dalam pengelolaan data oleh staff IT.
	Akses <i>password</i> oleh karyawan yang tidak berwenang.
Infrastruktur	Kesalahan operasional yang disebabkan oleh staff IT.
	Gangguan tegangan listrik/tegangan listrik tidak stabil.
	Ruangan server yang temperatur suhunya tidak sesuai standart.
	Gangguan Jaringan.
	Kerusakan kabel LAN akibat hewan pengerat.
	Bencana alam (banjir, kebakaran, gempa bumi) sehingga bisa terjadinya kerusakan pada server.

3.3. Identifikasi Kerentanan

Pada tahapan ini yaitu membuat *list* kecacatan dan kelemahan sistem dan teknologi informasi yang dapat dipicu atau disebabkan oleh ancaman dengan skala penilaian kerentanan dengan hasil yaitu daftar kerentanan berdasarkan temuan ancaman dengan tingkatan yang didapat yaitu terdapat pada tabel 5 berikut:

Tabel 5 Kerentanan

Sumber Ancaman	Kerentanan	Tingkat
Kerusakan pada aset yang sudah menua ataupun rusak.	Kemungkinan terjadinya rendah karena selalu diperhatikan dan diganti.	Low
Adanya serangan <i>malware</i> atau <i>virus</i> yang disebabkan oleh pihak luar/dalam.	Kemungkinan terjadinya tinggi karena keterlambatan dalam melakukan update <i>virus</i> sehingga memungkinkan terjadinya <i>virus</i> masuk ke sistem.	High
Update sistem yang belum dilakukan menyebabkan sistem berhenti/error.	Kemungkinan terjadinya rendah karena selalu diupdate pada sistem.	Low
Windows tidak berjalan semestinya.	Kemungkinan terjadinya sangat rendah karena selalu meng update windows secara teratur.	Very low
Pemanfaatan celah keamanan oleh pihak dalam/luar.	Kemungkinan terjadinya sedang karena pergantian <i>password</i> .	Medium
Server Down yang menyebabkan halaman tidak bisa diakses.	Kemungkinan terjadinya medium karena diperlukan pengecekan.	Low
Pencurian pada aset data sehingga bisa terjadinya permasalahan pada semua sistem.	Kemungkinan terjadinya tinggi karena pernah terjadi <i>ransomware</i> .	High
Kehilangan data yang sifatnya sensitif.	Kemungkinan terjadinya tinggi karena pernah kehilangan data selama 3 bulan ke belakang.	High
Kegagalan Backup	Kemungkinan terjadinya tinggi karena pernah kehilangan data selama 3 bulan ke belakang.	High
Menggunakan <i>password</i> yang lemah/default <i>password</i> .	Kemungkinan terjadinya sedang karena selalu diganti dan sesuai standar.	Low
Terjadi kesalahan dalam pengelolaan data oleh staff IT.	Kemungkinan terjadinya rendah karena dilakukan pengecekan dan edit dengan baik sesuai standar.	Low
Akses <i>password</i> oleh karyawan yang tidak berwenang.	Kemungkinan terjadinya rendah karena selalu diganti dan sesuai standar.	Low
Kesalahan operasional yang disebabkan oleh staff IT.	Kemungkinan terjadinya sangat rendah karena selalu dilakukan dengan baik sesuai standar.	Very Low
Gangguan tegangan listrik/tegangan listrik tidak stabil.	Kemungkinan terjadinya rendah karena ada cadangan UPS (Uninterruptible Power Supply) dan ETS (Electricity Treatment System), serta ada gardu cadangan.	Low

Sumber Ancaman	Kerentanan	Tingkat
Ruangan server yang temperatur suhunya tidak sesuai standart.	Kemungkinan terjadinya sangat rendah karena ada keberadaan AC di dalam ruangan server.	Very Low
Gangguan Jaringan.	Kemungkinan terjadinya sangat rendah karena Jaringan sudah versi enterprise.	Very Low
Kerusakan kabel LAN akibat hewan pengerat.	Kemungkinan terjadinya rendah karena belum pernah terjadi.	Low
Bencana alam (banjir, kebakaran, gempa bumi) sehingga bisa terjadinya kerusakan pada server.	Kemungkinan terjadinya sangat rendah karena terjadi hanya waktu hujan saja.	Very Low

3.4. Analisis Kontrol

Pada tahapan ini yaitu akan menganalisis pengendalian kerentanan sistem dengan adanya kontrol untuk sumber informasi sebagai berikut: ruangan server dilengkapi dengan *doorlock* yang menggunakan *finger print* dan kunci, ruangan server dilengkapi dengan AC, keamanan jaringan versi *enterprise*, mengubah password secara rutin, *supply* listrik oleh *Uninterruptible Power Supply (UPS)* dan *Electricity Treatment System (ETS)* dan menyeleksi data terlebih dahulu sebelum *publish*.

Tabel 6 Analisis Kontrol Saat Ini

Risiko	Analisis
Adanya serangan <i>malware</i> atau <i>virus</i> yang disebabkan oleh pihak luar/dalam.	Terjadi kerentanan pada aset <i>software</i> , dimana terdapat serangan <i>ransomware</i> pada bulan Juli lalu yang menyebabkan sistem berhenti. Sehingga rekomendasi kontrolnya yaitu dengan perlindungan dengan <i>antivirus</i> .
Pemanfaatan celah keamanan oleh pihak dalam/luar.	Terjadi kerentanan pada aset <i>software</i> , dimana pemanfaatan celah keamanan yang menjadikan serangan dari pihak lain untuk masuk, seperti pada serangan <i>ransomware</i> tersebut. Sehingga rekomendasi kontrolnya yaitu dengan pembatasan penggunaan akses sistem.
Pencurian pada aset data sehingga bisa terjadinya permasalahan pada semua sistem.	Terjadi kerentanan pada aset data dan informasi, dimana pada serangan <i>ransomware</i> tersebut menyebabkan data hilang. Sehingga rekomendasi kontrolnya yaitu dengan perlindungan pada <i>storage</i> data.
Kehilangan data yang sifatnya sensitif.	Terjadi kerentanan pada aset data dan informasi, dimana kurangnya salinan <i>backup</i> . Sehingga rekomendasi kontrolnya yaitu dengan menambahkan <i>storage</i> khusus untuk sistem <i>backup</i> .
Kegagalan <i>Backup</i>	Terjadi kerentanan pada aset data dan informasi, dimana pada serangan <i>ransomware</i> tersebut menyebabkan kegagalan <i>backup</i> menjadikan data hilang selama beberapa bulan ke belakang. Sehingga rekomendasi

	kontrolnya yaitu dengan membuat cadangan data.
Adanya serangan <i>malware</i> atau <i>virus</i> yang disebabkan oleh pihak luar/dalam.	Terjadi kerentanan pada aset <i>software</i> , dimana terdapat serangan <i>ransomware</i> pada bulan Juli lalu yang menyebabkan sistem berhenti. Sehingga rekomendasi kontrolnya yaitu dengan perlindungan dengan <i>antivirus</i> .

3.5. Penentuan Kemungkinan (*Likelihood*)

Tahapan ini yaitu akan menjelaskan bagaimana prosedur dalam memperkirakan kemungkinan dan asumsi tentang prosedur yang diklaim dari dugaan insiden ancaman sistem. Risiko prospektif dapat dikurangi dengan mengenali kerentanan yang terkait dengan terjadinya ancaman yang dapat ditentukan yaitu pada tabel 7 sebagai berikut:

Tabel 7 Kemungkinan

Risiko	Peristiwa Ancaman Yang Terjadi	Ancaman dampak Buruk	Keseluruhan Kemungkinan
Kerusakan pada aset yang sudah menua ataupun rusak.	Medium	Low	Low
Adanya serangan <i>malware</i> atau <i>virus</i> yang disebabkan oleh pihak luar/dalam.	High	High	High
Update sistem yang belum dilakukan menyebabkan sistem berhenti/ <i>error</i> .	Medium	Medium	Medium
Windows tidak berjalan semestinya.	Very Low	Low	Very Low
Pemanfaatan celah keamanan oleh pihak dalam/luar.	High	Medium	Medium
Server Down yang menyebabkan halaman tidak bisa diakses.	Medium	Low	Low
Pencurian pada aset data sehingga bisa terjadinya permasalahan	Low	Medium	Low

Risiko	Peristiwa Ancaman Yang Terjadi	Ancaman dampak Buruk	Keseluruhan Kemungkinan
han pada semua sistem.			
Kehilangan data yang sifatnya sensitif.	Low	Medium	Low
Kegagalan Backup	Medium	Medium	Medium
Menggunakan password yang lemah/default password.	Medium	Low	Low
Terjadi kesalahan dalam pengelolaan data oleh staff IT.	Low	Low	Low
Akses password oleh karyawan yang tidak berwenang.	Very Low	Medium	Low
Kesalahan operasional yang disebabkan oleh staff IT.	Very Low	Low	Very Low
Gangguan tegangan listrik/ tegangan listrik tidak stabil.	Low	Very Low	Very Low
Ruangan server yang temperatur suhunya tidak sesuai standart.	Low	Very Low	Very Low
Gangguan Jaringan.	Very Low	Low	Very Low
Kerusakan kabel LAN akibat hewan pengerat.	Low	Low	Low
Bencana alam (banjir, kebakaran, gempa bumi) sehingga bisa terjadinya kerusakan pada server.	Very Low	Very Low	Very Low

3.6. Dampak

Pada tahapan ini yaitu akan mengidentifikasi dampak untuk menentukan potensi dampak buruk dalam pada sistem, terdapat tingkatan yaitu berdasarkan skala penilaian dampak pada tabel 8 berikut:

Tabel 8 Identifikasi Dampak

Risiko	Tingkat Dampak	Dampak yang Dialami
Kerusakan pada aset yang sudah menua ataupun rusak.	Low	Terhambatnya pengerjaan dan mengalami kemunduran dari waktu yang sudah di targetkan.
Adanya serangan malware atau virus yang disebabkan oleh pihak luar/dalam.	High	Sistem akan terhenti jika server terkena virus dan hilangnya data.
Update sistem yang belum dilakukan menyebabkan sistem berhenti/error.	Low	Sistem tidak dapat diakses. Namun hal tersebut bisa diatasi dengan mudah.
Windows tidak berjalan semestinya.	Very Low	Sistem tidak dapat diakses. Namun hal tersebut bisa diatasi dengan mudah.
Pemanfaatan celah keamanan oleh pihak dalam/luar.	Medium	Data yang penting akan hilang maupun akses sistem akan terganggu.
Server Down yang menyebabkan halaman tidak bisa diakses.	Low	Sistem akan tidak bisa diakses. Namun bisa diatasi.
Pencurian pada aset data sehingga bisa terjadinya permasalahan pada semua sistem.	Very High	Data yang penting akan hilang.
Kehilangan data yang sifatnya sensitif.	Very High	Mempengaruhi informasi penting seputaran BSIP.
Kegagalan Backup	Very High	Tidak adanya data backup terbaru.
Menggunakan password yang lemah/default password.	Medium	Akan masuknya akses yang berbahaya.
Terjadi kesalahan dalam pengelolaan data oleh staff IT.	Medium	Data dan informasi yang tidak sesuai tersebar ke publik.
Akses password oleh karyawan yang tidak berwenang.	Medium	Ilegal akses yang menyebabkan kebocoran data.
Kesalahan operasional yang disebabkan oleh staff IT.	Low	Kesalahan setting sistem.
Gangguan tegangan listrik/tegangan listrik tidak stabil.	Very Low	Optimalisasi terhadap server terganggu.
Ruangan server yang temperatur suhunya tidak sesuai standart.	Low	Mengganggu jalannya proses.
Gangguan Jaringan.	Low	Terhambatnya komunikasi data atau informasi sehingga

Risiko	Tingkat Dampak	Dampak yang Dialami
		mengganggu jalannya proses.
Kerusakan kabel LAN akibat hewan pengerat.	Low	Berpengaruh dengan jaringan yang digunakan.
Bencana alam (banjir, kebakaran, gempa bumi) sehingga bisa terjadinya kerusakan pada server.	Very Low	Kerusakan aset serta fasilitas yang ada juga bisa terjadi.

3.7. Penilaian Risiko

Pada tahapan ini yaitu akan membantu potensi dan dampak yang ada. Tingkat resiko yang ditentukan menjadi faktor sejauh mana kejadian tersebut dapat membahayakan sistem, seperti yang pada tabel 9 berikut:

Tabel 9 Penilaian Risiko

Ancaman	Keseluruhan Kemungkinan	Dampak	Risiko Keseluruhan
Kerusakan pada aset yang sudah menua ataupun rusak.	Low	Low	Low
Adanya serangan <i>malware</i> atau <i>virus</i> yang disebabkan oleh pihak luar/dalam.	High	High	High
Update sistem yang belum dilakukan menyebabkan sistem berhenti/error.	Medium	Low	Low
Windows tidak berjalan semestinya.	Very Low	Very Low	Very Low
Pemanfaatan celah keamanan oleh pihak dalam/luar.	Medium	Medium	Medium
Server Down yang menyebabkan halaman tidak bisa diakses.	Low	Low	Low
Pencurian pada aset data sehingga bisa terjadinya permasalahan pada semua sistem.	Low	Very High	Medium

Ancaman	Keseluruhan Kemungkinan	Dampak	Risiko Keseluruhan
Kehilangan data yang sifatnya sensitif.	Low	Very High	Medium
Kegagalan Backup	Medium	Very High	High
Menggunakan password yang lemah/default password.	Low	Medium	Low
Terjadi kesalahan dalam pengelolaan data oleh staff IT.	Low	Medium	Low
Akses password oleh karyawan yang tidak berwenang.	Low	Medium	Low
Kesalahan operasional yang disebabkan oleh staff IT.	Very Low	Low	Very Low
Gangguan tegangan listrik/tegangan listrik tidak stabil.	Very Low	Very Low	Very Low
Ruangan server yang temperatur suhunya tidak sesuai standart.	Very Low	Low	Very Low
Gangguan Jaringan.	Very Low	Low	Very Low
Kerusakan kabel LAN akibat hewan pengerat.	Low	Low	Low
Bencana alam (banjir, kebakaran, gempa bumi) sehingga bisa terjadinya kerusakan pada server	Very Low	Very Low	Very Low

3.8. Rekomendasi

Pada tahapan ini yaitu akan dilakukan evaluasi risiko ancaman terhadap potensi dan dampak. Tingkat resiko yang ditentukan menjadi faktor sejauh mana kejadian tersebut membahayakan,

seperti yang terdapat pada tabel 10, 11, 12 dan 13 berikut:

Tabel 10 Rekomendasi Risiko *High*

Jenis Aset	Sumber Ancaman	Rekomendasi
Software	Adanya serangan <i>malware</i> atau <i>virus</i> yang disebabkan oleh pihak luar/dalam.	SI-3 Perlindungan Kode Berbahaya
Data dan Informasi	Kegagalan <i>Backup</i>	SI-16: Perlindungan Memori CP-9(5): Transfer ke Situs Penyimpanan Alternatif

Tabel 11 Rekomendasi Tingkat Risiko *Medium*

Jenis Aset	Sumber Ancaman	Rekomendasi
Software	Pemanfaatan celah keamanan oleh pihak dalam/luar.	RA-3: <i>Risk Assessment</i>
Data dan Informasi	Pencurian pada aset data sehingga bisa terjadinya permasalahan pada semua sistem.	SI-4(4): Lalu Lintas Komunikasi Masuk dan Keluar CP-9(8): Perlindungan Kriptografi AC-4: Penegakan Arus Informasi
	Kehilangan data yang sifatnya sensitif.	CP-9(8): Perlindungan Kriptografi

Tabel 12 Rekomendasi Tingkat Risiko *Low*

Jenis Aset	Sumber Ancaman	Rekomendasi
Hardware	Kerusakan pada aset yang sudah menua ataupun rusak.	PE-20: Pemantauan dan Pelacakan Aset
Software	<i>Update</i> sistem yang belum dilakukan menyebabkan sistem berhenti/error.	SI-2(5): Pembaruan Perangkat Lunak dan <i>Firmware</i> Otomatis
SDM (Sumber Daya Manusia)	Akses <i>password</i> oleh karyawan yang tidak berwenang.	AC-9: Pemberitahuan <i>Logon</i> Sebelumnya AT-2(2): Ancaman Orang Dalam

		PS-3: Penyaringan Personil IA-5(1)(a): Otentikasi berbasis kata sandi IA-2: Identification and Authentication (<i>Organizational Users</i>)
	Menggunakan <i>password</i> yang lemah/default <i>password</i> .	IA-5(1)(a): Otentikasi berbasis kata sandi
Infrastruktur	Kerusakan kabel LAN akibat hewan pengerat.	PE-20: Pemantauan dan Pelacakan Aset
Hardware	Kerusakan pada aset yang sudah menua ataupun rusak.	PE-20: Pemantauan dan Pelacakan Aset

Tabel 13 Rekomendasi Tingkat Risiko *Very Low*

Jenis Aset	Sumber Ancaman	Rekomendasi
Software	<i>Windows</i> tidak berjalan semestinya.	SI-4: Pemantauan Sistem
SDM (Sumber Daya Manusia)	Kesalahan operasional yang disebabkan oleh staff IT.	SI-11: Penanganan Kesalahan
Infrastruktur	Gangguan tegangan listrik/tegangan listrik tidak stabil.	PE-9: Peralatan Listrik dan Kabel PE-11: Daya Darurat
	Gangguan Jaringan.	SC-10: Putus Jaringan
	Ruangan <i>server</i> yang temperatur suhunya tidak sesuai <i>standart</i> .	PE-14: Kontrol Lingkungan PE-17: Tempat Kerja Alternatif AT-3(1): Kontrol Lingkungan
	Bencana alam (banjir, kebakaran, gempa bumi) sehingga terjadinya kerusakan pada <i>server</i> .	PE-17: Tempat Kerja Alternatif CP-10: Pemulihan dan Rekonstitusi Sistem AT-3(1): Kontrol Lingkungan

3.9. Dokumentasi

Pada tahapan ini yaitu akan membuat dokumen resmi berisi dari karakteristik sistem hingga rekomendasi yang telah diberikan sesuai.

SIMPULAN

Menurut temuan melalui wawancara dan obeservasi pada *website* bsip.pertanian.co.id di BSIP (Badan Standarisasi Instrumen Pertanian), dimana belum dilakukan manajemen risiko, sehingga pada penelitian kali ini akan dilakukan analisis mengenai manajemen risiko, dimana penggunaan *framework* NIST SP 800-30 yang berfokus pada sistem dan teknologi informasi, serta NIST SP 800-53 sebagai pedoman pendukung dalam rekomendasi kontrolnya. Terdapat kesimpulan terhadap beberapa poin sebagai berikut:

1. Terdapat 2 *high*, 3 *medium*, 7 *low* dan 6 *very low* pada penilaian risiko di *website* bsip.pertanian.co.id, yang mana *high* pada adanya serangan *malware* atau *virus* yang disebabkan oleh pihak luar/dalam, dan kegagalan *Backup*.
2. Terdapat rekomendasi kontrol berdasarkan NIST SP 800-53 yaitu pada *high* adalah SI-3, SI-16 dan CP-9(5); *medium* adalah Rekomendasi RA-3, SI-4(4), CP-9(8), AC-4; *low* adalah PE-20, SI-2(5), AC-9, AT- 2(2), PS-3, IA-5(1)(a), IA-2, MA-1, SI-10, IR-4; dan *very low* adalah SI-4, SI-11, PE-9, PE-11, PE-14, PE-17, CP-10, AT-3(1) dan SC-10.

DAFTAR PUSTAKA

- [1] B. P. dan P. Pertanian, "40 Inovasi Kelembagaan Diseminasi Teknologi Pertanian Catatan Perjalanan 40 Tahun Balitbangtan," *News.Ge*, p. <https://news.ge/anakliis-porti-aris-qveynis-momava>, 2014.
- [2] A. Elanda and R. L. Buana, "Analisis Manajemen Risiko Infrastruktur Dengan Metode NIST (National Institute of Standards and Technology) SP 800-30 (Studi Kasus : STMIK Rosma)," *Elkom J. Elektron. dan Komput.*, vol. 14, no. 1, pp. 141–151, 2021, doi: 10.51903/elkom.v14i1.387.
- [3] E. Supristiowadi and Y. G. Suchahyo, "Manajemen Risiko Keamanan Informasi pada Sistem Aplikasi Keuangan Tingkat Instansi (SAKTI) Kementerian Keuangan," *Indones. Treas. Rev. J. Perbendaharaan Keuang. Negara dan Kebijak. Publik*, vol. 3, no. 1, pp. 23–33, 2018, doi: 10.33105/itrev.v3i1.20.
- [4] I. Santosa and R. Yusvinindya, "Analisis Risiko dan Kontrol Perlindungan Data Pribadi pada Sistem Informasi Administrasi Kependudukan," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 3, no. 3, pp. 496–504, 2019.
- [5] M. Al Fikri, F. A. Putra, Y. Suryanto, and K. Ramli, "Risk assessment using NIST SP 800-30 revision 1 and ISO 27005 combination technique in profit-based organization: Case study of ZZZ information system application in ABC agency," *Procedia Comput. Sci.*, vol. 161, pp. 1206–1215, 2019, doi: 10.1016/j.procs.2019.11.234.

- [6] I. G. N. M. Putra Eryawan, G. M. Arya Sasmita, and A. A. K. Agung Cahyawan Wiranatha, "Information Security Risk Strategy at PT. X Using NIST SP 800-30," *J. Ilm. Merpati (Menara Penelit. Akad. Teknol. Informasi)*, vol. 9, no. 3, p. 213, 2021, doi: 10.24843/jim.2021.v09.i03.p03.
- [7] I. M. M. Putra and K. Mutijarsa, "Designing Information Security Risk Management on Bali Regional Police Command Center Based on ISO 27005," *3rd 2021 East Indones. Conf. Comput. Inf. Technol. EIconCIT* 2021, pp. 14–19, 2021, doi: 10.1109/EIconCIT50028.2021.9431865.
- [8] F. Mahardika, "Manajemen Risiko Keamanan Informasi Menggunakan Framework NIST SP 800-30 Revisi 1 (Studi Kasus: STMIK Sumedang)," vol. 02, no. 02, pp. 1–8, 2017.
- [9] M. Megawati and S. Rosnawati, "Penilaian Risiko Jaringan Komputer Menggunakan Framework Nist Sp 800-30 Revisi 1 Pada Smk Muhammadiyah 2 Pekanbaru," *J. Ilm. Rekayasa dan Manaj. Sist. Inf.*, vol. 8, no. 2, p. 189, 2022, doi: 10.24014/rmsi.v8i2.19115.
- [10] F. Panjaitan and A. Aprilo, "Analisis Manajemen Risiko Keamanan Jaringan Menggunakan Framework Nist," *J. Ilm. Matrik*, vol. 24, no. 1, pp. 71–81, 2022, doi: 10.33557/jurnalmatik.v24i1.1682.
- [11] A. Syaputra and B. Muslim, "Implementasi Metode Quantitative dan Qualitative Pada Risk Analysis & IT Risk Management," *Fakt. Exacta*, vol. 15, no. 1, 2022, [Online]. Available: https://journal.lppmunindra.ac.id/index.php/Faktor_Exacta/article/view/12040
- [12] N. Fitrianti Fahrudin, A. Nugraha S, and K. Ramadhan Putra, "Penilaian Risiko Keamanan Data Karyawan Pada Sistem Informasi Dengan Menggunakan Framework Nist Sp 800-30 pada PT. ABC," *J. Ilm. Teknol. Infomasi Terap.*, vol. 8, no. 3, 2022, doi: 10.33197/jitter.vol8.iss3.2022.900.
- [13] A. A. Putro, A. Ambarwati, and E. Setiawan, "Analisa Manajemen Risiko E-Learning Edlink Menggunakan Metode NIST SP 800-30 Revisi 1," *J. Teknol. dan Inf.*, vol. 11, no. 2, pp. 125–136, 2021, doi: 10.34010/jati.v11i2.5314.
- [14] Normah, B. Rifai, S. Vambudi, and R. Maulana, "Maintaining The Continuity of The Company's Operation using the NIST Framework for SME," *J. Tek. Komput. AMIK BSI*, vol. 8, no. 2, pp. 174–180, 2022, doi: 10.31294/jtk.v4i2.
- [15] A. Marsehan, M. I. Herdiansyah, A. H. Mirza, and D. Antoni, "Penilaian Resiko Kejahatan Illegal Content Menggunakan Framework Nist 800-30," *Paradig. - J. Komput. dan Inform.*, vol. 22, no. 2, pp. 215–224, 2020, doi: 10.31294/p.v22i2.8913.
- [16] R. R. Putra, "Analisis Manajemen Risiko TI Pada Keamanan Data E-Learning Dan Aset TI Menggunakan NIST SP 800-30 Revisi 1," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 6, no. 1, pp. 96–105, 2019, doi: 10.35957/jatisi.v6i1.154.
- [17] R. Damalia, A. Ambarwati, and E. Setiawan, "Analisis Manajemen Risiko It Sistem Administrasi Bisnis Retail Menggunakan Metode Nist Sp 800-30 Revisi 1 It Risk Management Analysis Business Administration System Retail Using Nist Sp 800-30 Revision 1," *J. Inf. Technol. Comput. Sci.*, vol. 4, no. 2, p. 2021, 2021.
- [18] F. Wahdah et al., "PENGEMBANGAN MANAJEMEN RESIKO APLIKASI KEUANGAN PADA PERUSAHAAN ABC MELALUI KOMBINASI NIST SP 800-30, COBIT, PMBOK, ISO 31000," *Sains dan Teknol.*, vol. 9, no. 1, pp. 251–263, 2022.
- [19] N. Matondang, I. N. Isnainiyah, and A. Muliawati, "Analisis Manajemen Risiko Keamanan Data Sistem Informasi (Studi Kasus: RSUD XYZ)," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 2, no. 1,

- pp. 282–287, 2018, doi: 10.29207/resti.v2i1.96.
- [20] K. Aprianto, S. Mardi Susiki Nugroho, T. Elektro, F. Teknologi Elektro dan Informatika Cerdas, and I. Surabaya, “Analisis Manajemen Risiko SPBE Menggunakan COBIT 5 For Risk dan ISO 31000:2018 di Kabupaten Magetan E-Government Risk Management Analysis Using COBIT 5 For Risk and ISO 31000:2018 in Magetan Regency,” *J. Ilmu Pengetah. dan Teknol. Komun.*, vol. 23, no. 2, pp. 107–123, 2021.