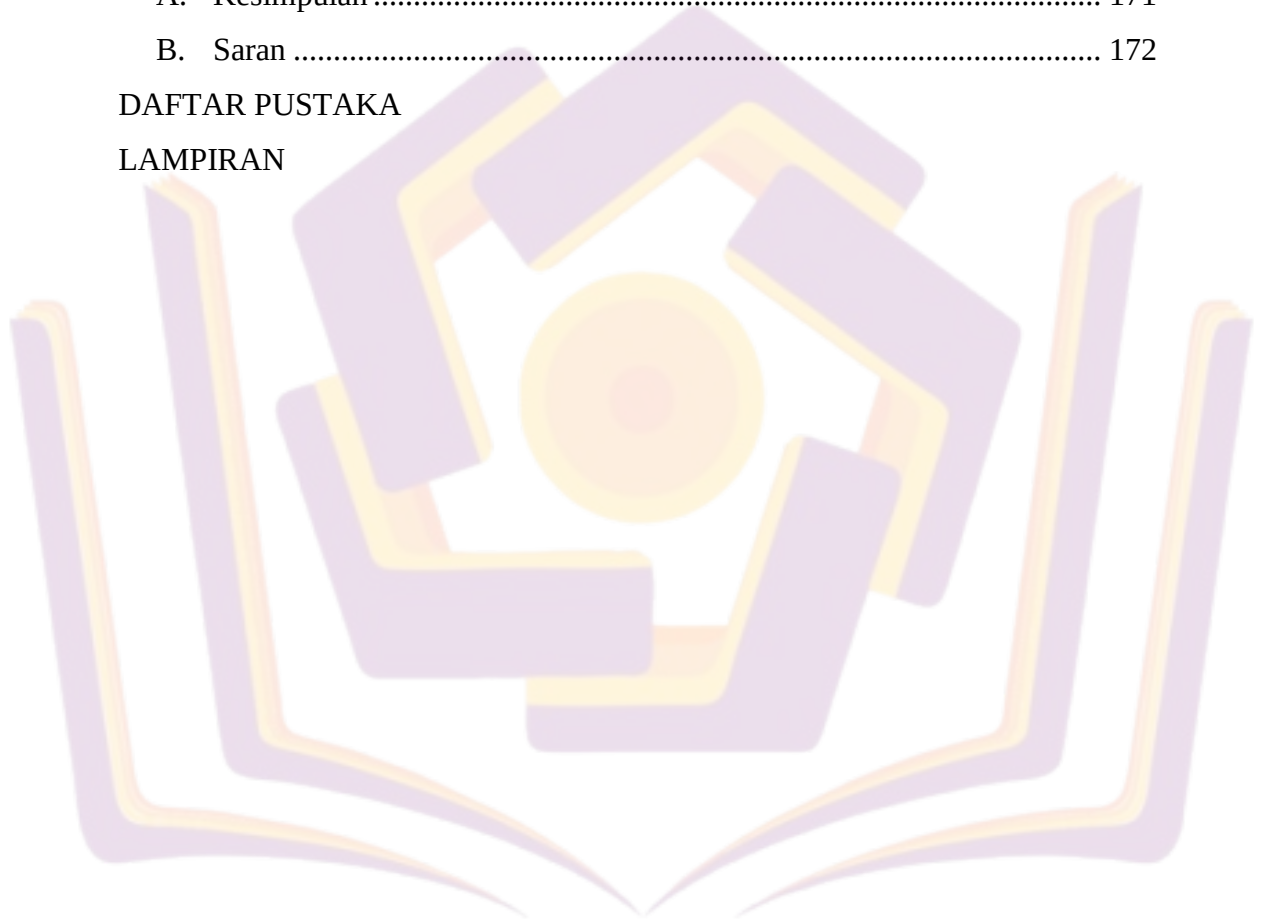


DAFTAR ISI

HALAMAN SAMPUL.....	i
HALAMAN JUDUL	ii
HALAMAN PERSETUJUAN	iii
HALAMAN PENSAHAN.....	iv
HALAMAN PERNYATAAN KEASLIAN	v
HALAMAN PERSEMBAHAN	vi
HALAMAN MOTTO.....	vii
KATA PENGANTAR.....	viii
DAFTAR ISI	x
DAFTAR TABEL	xii
DAFTAR GAMBAR.....	xiii
DAFTAR ISTILAH.....	xiv
DAFTAR LAMPIRAN	xviii
ABSTRAK.....	xix
ABSTRACT	xx
BAB I PENDAHULUAN.....	1
A. Latar Belakang Masalah	1
B. Rumusan Masalah.....	9
C. Batasan Masalah	10
D. Tujuan Penelitian	10
E. Manfaat Penelitian	11
BAB II TINJAUAN PUSTAKA	13
A. Landasan Teori.....	13
B. Penelitian Sebelumnya.....	40
BAB III METODE PENELITIAN	46
A. Tempat dan Waktu Penelitian.....	46
B. Metode Pengumpulan Data.....	46
C. Alat dan Bahan Penelitian.....	48

D. Konsep Penelitian	50
BAB IV HASIL DAN PEMBAHASAN.....	61
A. Hasil Penelitian	61
B. Hasil Akhir Penelitian.....	147
C. Pembahasan.....	155
BAB V PENUTUP	171
A. Kesimpulan	171
B. Saran	172
DAFTAR PUSTAKA	
LAMPIRAN	



DAFTAR TABEL

Tabel 2. 1 Perbandingan Metode Manajemen Risiko	19
Tabel 2. 2 Kriteria Kemungkinan Frekuensi Kejadian	33
Tabel 2. 3 Kriteria Dampak Risiko	35
Tabel 2. 4 Matriks Evaluasi Risiko	37
Tabel 2. 5 Kriteria Tingkat Risiko	38
Tabel 2. 6 Penelitian Sebelumnya.....	43
Tabel 4. 1 Hasil Komunikasi dan Konsultasi.....	76
Tabel 4. 2 Identifikasi Aset Teknologi Informasi SMEGA Learn.....	85
Tabel 4. 3 Identifikasi Kemungkinan Risiko	85
Tabel 4. 4 Identifikasi Dampak Risiko	122
Tabel 4. 5 Kriteria Likelihood.....	125
Tabel 4. 6 Nilai <i>Likelihood</i>	126
Tabel 4. 7 Kriteria Impact	129
Tabel 4. 8 Nilai Impact.....	129
Tabel 4. 9 Matriks Evaluasi	133
Tabel 4. 10 Tabel Tingkat Risiko.....	134
Tabel 4. 11 Hasil Evaluasi Risiko	134
Tabel 4. 12 Rekomendasi Perlakuan Risiko	139
Tabel 4. 13 Rekomendasi Monitoring dan Review.....	146
Tabel 4. 14 Ketercapaian Tujuan Penelitian	154

DAFTAR GAMBAR

Gambar 2. 1 Proses Manajemen Risiko ISO 31000.....	29
Gambar 3. 1 Konsep Penelitian.....	52



DAFTAR ISTILAH

2FA (Two-Factor Authentication)	: Cara verifikasi yang melibatkan dua langkah untuk memperkuat keamanan akun pengguna
Admin IT	: Individu yang memiliki tanggung jawab untuk mengelola, merawat, dan mengembangkan sistem teknologi informasi
Aset (Asset)	: Sumber daya yang bernilai bagi organisasi dan harus dilindungi dari berbagai ancaman.
Autentikasi	: Proses mengonfirmasi identitas pengguna sebelum diberikan izin untuk mengakses sistem.
Backup	: Proses menyimpan data untuk menghindari kehilangan informasi saat terjadi kerusakan atau masalah sistem.
Blank Screen	: Situasi dimana halaman sistem tidak dapat diperlihatkan sehingga pengguna tidak bisa mengakses layanan.
Catastrophic	: Tingkat dampak sangat besar yang mengakibatkan sistem tidak dapat berfungsi sehingga kegiatan organisasi terhenti.
Certain	: Tingkat kemungkinan hampir pasti akan terjadi (1-3 bulan).
Cloud Server	: Server virtual yang disediakan melalui layanan komputasi awan.
Database	: Sekumpulan data yang tersusun dengan sistematis untuk mendukung fungsi sistem informasi.
Firewall	: Sebuah sistem pengaman jaringan yang berperan dalam mengatur arus data yang masuk dan keluar sesuai dengan kebijakan keamanan tertentu.
Framework Laravel	: Framework yang berbasis PHP dan digunakan untuk mengembangkan Sistem Informasi SMEGA <i>Learn</i> .
Hashing Password	: Mengonversi kata sandi menjadi format terenkripsi sehingga tidak bisa dibaca secara langsung.
Human Error	: Kesalahan yang terjadi akibat tindakan pengguna atau operator saat menggunakan sistem informasi.
Impact	: Tingkat konsekuensi yang akan muncul jika suatu risiko terjadi pada organisasi atau sistem informasi.
Insignificant	: Tingkat dampak yang sangat kecil sehingga tidak mengganggu fungsi sistem.

ISO 31000:2018	:	Standar Internasional yang menyajikan pedoman tentang prinsip, struktur, dan prosedur pengelolaan risiko.
Jurnal Pembelajaran	:	Catatan digital berisi kegiatan belajar yang dimasukkan oleh guru melalui <i>SMEGA Learn</i> .
Learning Management System (LMS)	:	Platform yang digunakan untuk mengatur proses pendidikan secara daring, termasuk konten, tugas, kehadiran, dan penilaian.
Likelihood	:	Tingkat peluang terjadinya suatu risiko dalam jangka waktu tertentu.
Likely	:	Tingkat Kemungkinan besar terjadi (3-6 bulan)
Load Balancing	:	Teknik distribusi beban jaringan atau server untuk mempertahankan kestabilan kinerja sistem.
Log Aktivitas (Activity Log)	:	Catatan otomatis yang merekam sejarah aktivitas pengguna dalam sistem informasi.
Major	:	Tingkat dampak yang signifikan mengganggu sebagian besar layanan sistem dan kegiatan organisasi
MariaDB	:	Sistem pengelolaan basis data (DBMS) yang berfungsi sebagai tempat penyimpanan data di <i>SMEGA Learn</i> .
Medium	:	Tingkat dampak sedang yang mengakibatkan beberapa layanan sistem terganggu, tetapi operasional tetap dapat dilanjutkan.
Minor	:	Tingkat dampak rendah yang hanya menyebabkan sedikit gangguan dan tetap dapat dikelola
Mitigasi Risiko	:	Usaha untuk menurunkan kemungkinan terjadinya risiko serta dampak yang dihasilkannya.
Monitoring	:	Kegiatan pemantauan rutin terhadap efisiensi pengelolaan risiko.
Node.js	:	Lingkungan (<i>runtime</i>) JavaScript yang dimanfaatkan untuk pengembangan aplikasi web.
Observasi	:	Pengumpulan informasi melalui pengamatan langsung terhadap objek yang diteliti.
Possible	:	Kemungkinan dapat terjadi kapan saja (6-12 bulan)
Presensi Digital	:	Sistem registrasi kehadiran yang dilakukan secara elektronik menggunakan aplikasi.

Rare	: Tingkat kemungkinan sangat rendah atau hampir tidak pernah terjadi (> 2 tahun).
Risk Analysis	: Proses untuk mengevaluasi kemungkinan dan efek dari setiap risiko.
Risk Assessment	: Proses yang mencakup identifikasi, analisis, serta evaluasi risiko.
Risk Evaluation	: Proses mengidentifikasi tingkat prioritas risiko berdasar hasil analisis.
Risk Identification	: Prosedur untuk mengenali dan mendokumentasikan semua kemungkinan risiko.
Risk Matrix	: Matriks yang dipakai untuk menetapkan level risiko berdasarkan kombinasi nilai kemungkinan dan dampak.
Risk Register	: Dokumen yang memuat daftar risiko yang telah diidentifikasi, termasuk informasi mengenai aset yang terdampak, sumber risiko, penyebab, dan dampak risiko sebagai dasar untuk proses analisis dan evaluasi risiko.
Risk Treatment	: Perlakuan risiko sebagai proses penentuan langkah-langkah untuk mengurangi atau mengontrol risiko.
Review	: Evaluasi yang berkesinambungan terhadap efektivitas pengendalian risiko.
SEMAKIN	: Sistem informasi pendidikan yang diterapkan sebelum pelaksanaan SMEGA Learn.
Server	: Server komputer yang menawarkan layanan, penyimpanan data, dan sumber daya kepada pengguna melalui jaringan.
Sistem Informasi	: Suatu sistem yang menggabungkan manusia, perangkat keras, perangkat lunak, data, dan prosedur untuk menghasilkan informasi.
SMEGA Learn	: Platform informasi pembelajaran daring yang dimiliki oleh SMK Negeri 1 Purbalingga.
Snapshot	: Salinan keadaan server pada waktu tertentu yang digunakan untuk proses pemulihan data.
SOP (Standard Operating Procedure)	: Dokumen yang berisi prosedur kerja standar sebagai panduan untuk melaksanakan suatu aktivitas
Teknologi Informasi (TI)	: Merupakan teknologi yang dipakai untuk mendapatkan, mengolah, menyimpan, serta mendistribusikan informasi.

Unlikely : Tingkat kemungkinan sangat kecil (1-2 tahun).

Virtual Private Server (VPS) : Server virtual yang memiliki sumber daya tersendiri dan berfungsi untuk menjalankan aplikasi serta penyimpanan data

Wawancara : Metode pengumpulan data dengan cara berdialog langsung dengan narasumber untuk mendapatkan informasi penelitian.



DAFTAR LAMPIRAN

Lampiran 1. Surat Izin Penelitian

Lampiran 2. Surat Keterangan Telah Melakukan Penelitian

Lampiran 3. Hasil Wawancara Kepala Sekolah

Lampiran 4. Hasil Wawancara Wakil Kepala Sekolah (Waka Kurikulum)

Lampiran 5. Hasil Wawancara Admin IT

Lampiran 6. Hasil Wawancara Staff / Pengelola Teknologi Informasi IT

Lampiran 7. Hasil Wawancara Guru

Lampiran 8. Hasil Wawancara 5 Siswa

Lampiran 9. Hasil Turnitin

Lampiran 10. Dokumentasi wawancara dan observasi

