

LAPORAN AKHIR IMPLEMENTASI PROYEK PERUBAHAN

OPTIMALISASI PUSDATIK DALAM MELAKUKAN MANAJEMEN RISIKO SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN BADAN SIBER DAN SANDI NEGARA



Oleh:

RAKHMAT DAMDAMI, S.A.P, M.Si

NDH 26

**Peserta Pelatihan Kepemimpinan Nasional Tingkat II
Angkatan XVIII Tahun 2022**

**LEMBAGA PENDIDIKAN DAN PELATIHAN POLRI
PUSAT PENDIDIKAN DAN ADMINISTRASI BANDUNG
2022**

LEMBAR PERSETUJUAN

OPTIMALISASI PUSDATIK DALAM MELAKUKAN MANAJEMEN RISIKO SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN BADAN SIBER DAN SANDI NEGARA

Peserta pelatihan

RAKHMAT DAMDAMI, S.A.P, M.Si

NDH 26

Telah disetujui pada tanggal : 8 Nopember 2022

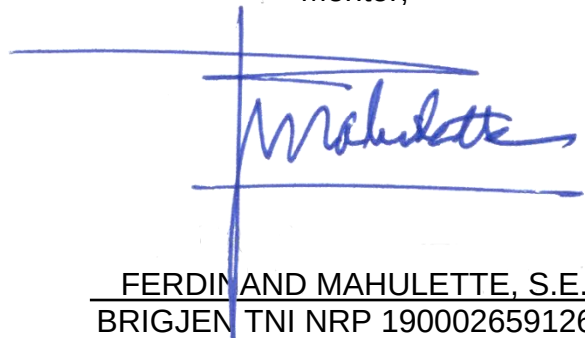
Di Pusdikmin Lemdiklat Polri Bandung

Coach,



BURDAN ALI JUNJUNAN, S.H., M.Si.
NIP 196012011986031016

Mentor,



FERDINAND MAHULETTE, S.E.
BRIGJEN TNI NRP 1900026591265

LEMBAR PENGESAHAN

OPTIMALISASI PUSDATIK DALAM MELAKUKAN MANAJEMEN RISIKO SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN BADAN SIBER DAN SANDI NEGARA



Disusun oleh :

RAKHMAT DAMDAMI, S.A.P, M.Si
NDH 26

Telah dipresentasikan pada Evaluasi Implementasi Proyek Perubahan yang
diselenggarakan tanggal : 15 Nopember 2022
Di Pusdikmin Lemdiklat Polri Bandung

Mengetahui,

**KAPUSDIKLAT
LEMDIKLAT POLRI**

Drs. TAUFIK RIYADI
KOMBES POL NRP. 65110550

PERNYATAAN KEASLIAN

Yang bertanda tangan di bawah ini :

Nama : RAKHMAT DAMDAMI, S.A.P., M.Si.

NRP : 74050727

Instansi : Bareskrim Polri (Badan Siber dan Sandi Negara)

Jabatan : Kepala Bagian Umum Pusat Data dan Teknologi Informasi dan Komunikasi

Dengan ini menyatakan bahwa Proyek Perubahan yang berjudul :

OPTIMALISASI PUSDATIK

DALAM MELAKUKAN MANAJEMEN RISIKO

SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

DI LINGKUNGAN BADAN SIBER DAN SANDI NEGARA

adalah karya saya sendiri, bukan pengambilalihan tulisan orang lain. Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa sebagian atau keseluruhan isi Proyek Perubahan ini hasil karya orang lain, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Bandung, 8 Nopember 2022



Rakhmat Damdami, S.A.P, M.Si

EXECUTIVE SUMMARY

Di Era Teknologi saat ini, perkembangan Teknologi Informasi dan Komunikasi (TIK) berkembang demikian pesatnya. TIK bagaikan pedang yang bermata dua, di satu sisi dapat memberikan kemudahan/keuntungan dan berkontribusi dalam meningkatkan kemajuan peradaban manusia tetapi di sisi lain juga menjadi peluang terjadinya pelanggaran hukum, seperti serangan siber, pencurian data, penyebaran virus, perusakan sistem dan sebagainya.

Ancaman ini tentunya perlu disikapi dengan serius, terutama dimana saat ini pemerintah melalui Perpres nomor 95 tahun 2018, mengamanatkan kepada setiap Kementerian/Lembaga untuk menerapkan Sistem Pemerintah Berbasis Elektronik (SPBE). Hal ini tentu akan membuka peluang bagi pelaku kejahatan untuk melakukan serangan ataupun pencurian informasi / data penting milik instansi Pemerintah.

Untuk itu perlu adanya suatu upaya yang dilakukan secara terus menerus untuk mengetahui kerentanan sistem elektronik pada masing-masing institusi tersebut, termasuk diantaranya adalah di lingkungan Badan Siber dan Sandi Negara (BSSN). Namun dalam kenyataan sampai dengan saat ini BSSN melalui Pusat Data dan Teknologi Informasi Komunikasi (Pusdatik) belum dapat melakukan penilaian risiko di dalam Satuan Kerjanya karena adanya beberapa kendala terutama terkait dasar hukum pelaksanaannya. Hal ini dibuktikan dengan masih rendahnya nilai indeks SPBE BSSN dari target yang telah ditentukan, terutama pada domain Manajemen Risiko.

Oleh karena itu perlu adanya suatu upaya untuk melakukan “Optimalisasi Pusdatik Dalam Melakukan Manajemen Risiko Sistem Pemerintah Berbasis Elektronik di Lingkungan Badan Siber dan Sandi Negara”, yaitu dengan menerbitkan Peraturan Kepala BSSN tentang Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik dan beberapa aturan turunannya berupa Standar Operasional Prosedur dan Petunjuk Teknis Penilaian Risiko.

KATA PENGANTAR

Alhamdulillah, puji syukur penulis panjatkan kehadirat Allah SWT atas limpahan rahmat dan hidayah-Nya kepada penulis sehingga dapat menyelesaikan Laporan Proyek perubahan yang berjudul “Optimalisasi Pusdatik Dalam Melakukan Manajemen Risiko Sistem Pemerintah Berbasis Elektronik di Lingkungan Badan Siber dan Sandi Negara”. Laporan Proyek Perubahan ini disusun untuk memenuhi dan melengkapi tugas dalam pelaksanaan Pelatihan Kepemimpinan Nasional (PKN) Tingkat II angkatan XVIII Tahun 2022.

Dalam menyusun proyek perubahan ini, penulis menemukan berbagai hambatan, kesulitan dan kendala, namun berkat pengarahan serta bantuan dan dorongan dari berbagai pihak akhirnya penulis dapat menyelesaikan Laporan Proyek Perubahan ini dengan tepat waktu. Oleh karena itu dengan segala hormat dan kerendahan hati perkenankanlah penulis mengucapkan terima kasih kepada :

1. Komisaris Jenderal Polisi Drs. Luki Hermawan, M.Si, Wakil Kepala Badan Siber dan Sandi Negara, yang telah memberikan dukungan dan arahan dari awal sampai dengan akhir dalam pelaksanaan Pelatihan Kepemimpinan Nasional Tingkat II di Pusdikmin Polri.
2. Brigadir Jenderal TNI Ferdinand Mahulelette, SE, Kepala Pusat Data dan Teknologi Informasi Komunikasi Badan Siber dan Sandi Negara, selaku Mentor yang telah memberikan persetujuan atas terlaksananya implementasi proyek perubahan ini dalam memberikan bimbingan dan dukungan penuh serta memberikan dukungan bagi selesainya penyelesaian proyek perubahan ini sampai kepada tahap akhir.
3. Bapak Burdan Ali Junjuran, S.H, M.Si, selaku coach yang telah memberikan bimbingan, koreksi, motivasi dan feedback terhadap laporan progres implementasi proyek perubahan.
4. Para Stakeholder/Tim Kerja Proyek perubahan yang telah membantu dan mendukung penulis dalam melaksanakan implementasi proyek perubahan serta memberikan masukan dan saran bagi kelancaran dan keberhasilan proyek perubahan ini.
5. Keluarga tercinta, Istri dan anak-anak, yang memberikan dukungan semangat serta doa dalam penyelesaian proyek perubahan ini.

6. Para Widyaiswara, pengajar, dan penyelenggara Diklat PKN II yang telah memfasilitasi dan memberikan inspirasi dalam penyelesaian proyek perubahan ini.
7. Rekan-rekan seperjuangan peserta Pelatihan Kepemimpinan Nasional II Angkatan XVIII Tahun 2022 yang telah memberikan dukungan selama kegiatan pelatihan.

Dalam penyusunan laporan proyek perubahan ini, penulis menyadari masih terdapat banyak kekurangan, untuk itu penulis mohon maaf atas segala kekurangan tersebut seraya tidak menutup diri terhadap segala saran dan kritik serta masukan yang bersifat konstruktif bagi perbaikan proyek perubahan ini. Semoga laporan ini dapat bermanfaat bagi semua pihak, khususnya Badan Siber dan Sandi Negara.

Bandung, 8 Nopember 2022

A handwritten signature in dark ink, featuring a large, stylized loop at the beginning and a series of smaller, connected strokes extending to the right.

Rakhmat Damdami, SAP, MSi

DAFTAR ISI

Halaman Judul	
Lembar Persetujuan	
Lembar Pengesahan	
Pernyataan Keaslian	
Daftar Isi	
Daftar Tabel	
Daftar Gambar	
Daftar Lampiran	
Executive Summary	
Kata Pengantar	

BAB I : RANCANGAN PROYEK PERUBAHAN	1
I. DESKRIPSI PROYEK PERUBAHAN	1
II. LATAR BELAKANG	5
A. Dasar Hukum	5
B. Struktur Organisasi	6
C. Tugas Pokok BSSN	6
D. Fungsi BSSN	6
E. Tugas Pokok Pusdatik BSSN	7
F. Fungsi Pusdatik BSSN	7
G. Isu-isu Strategis Ancaman Siber	9
H. Kondisi Awal	16
I. Kondisi Yang Diharapkan	22
J. Gap Yang Muncul Berdasarkan Kondisi Awal dan Kondisi Yang diharapkan	22
K. Gagasan Proyek Perubahan	23
L. Strategi Untuk Mewujudkan Gagasan	23
M. Ruang Lingkup Proyek Perubahan	27
III. TUJUAN DAN MANFAAT	28
A. Tujuan	28
B. Manfaat	29
IV. OUTPUT DAN OUTCOME	30
A. Output	30
B. Outcome	32

V.	IDENTIFIKASI STAKEHOLDER	32
VI.	POTENSI RISIKO DAN RENCANA MITIGASI	35
VII.	ORGANISASI TIM EFEKTIF	36
VIII.	ANGGARAN	39
BAB II : IMPLEMENTASI PROYEK PERUBAHAN		40
I.	CAPAIAN TAHAPAN RENCANA STRATEGIS.....	40
II.	DESKRIPSI KEPEMIMPINAN STRATEGIS.....	59
III.	IMPLEMENTASI STRATEGI MARKETING	65
A.	Dukungan/Peta Stakeholder	65
B.	Desiminasi dan Publikasi	68
IV.	KEBERLANJUTAN PROYEK PERUBAHAN	72
A.	Dukungan Mentor Untuk Keberlanjutan Proyek Perubahan	72
B.	Rencana Implementasi Jangka Menengah dan Jangka Panjang	73
V.	IMPLEMENTASI SOLUSI TERHADAP KENDALA	75
VI.	PEMBERDAYAAN ORGANISASI PEMBELAJARAN	77
VII.	KONTRIBUSI MATA PELATIHAN PENDUKUNG	85
VIII.	PEMBELAJARAN KEPEMIMPINAN (LESSON LEARNT)	91
BAB III : PENUTUP		94
I.	SIMPULAN	94
II.	REKOMENDASI	95

DAFTAR PUSTAKA

LAMPIRAN LAMPIRAN

DAFTAR TABEL

Tabel 1 : Nilai indeks SPBE BSSN yang dikeluarkan KemenPAN RB	
Tahun 2021	2
Tabel 2 : Perubahan Target SPBE BSSN	3
Tabel 3 : Tren Anomali Trafik Keamanan Siber periode Januari-Desember	
2021	10
Tabel 4 : Data Serangan Siber di Dunia.....	11
Tabel 5 : Rekapitulasi Notifikasi ke Pemangku Kepentingan	14
Tabel 6 : Daftar pegawai, aplikasi, perangkat dan Security Perimeter	18
Tabel 7 : Analisis USG	20
Tabel 8 : Analisis SOAR	26
Tabel 9 : Potensi Risiko dan Rencana Mitigasi	35
Tabel 10 : Tata Kelola Proyek Perubahan	36

DAFTAR GAMBAR

Gambar 1 : Struktur Organisasi BSSN	6
Gambar 2 : Pemetaan Stakeholder	33
Gambar 3 : Tim Efektif	36
Gambar 4 : Perubahan Peta Stakeholder	65

DAFTAR LAMPIRAN

- LAMPIRAN 1 : Draft Peraturan Kepala Badan Siber Dan Sandi Negara Tentang Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik
- LAMPIRAN 2 : Standar Operasional Prosedur (Sop) Penilaian Risiko (Risk Assesment)
- LAMPIRAN 3 : Petunjuk Tekhnis (Juknis) Penilaian Risiko (Risk Assesment)
- LAMPIRAN 4 : Rapat Pembentukan Tim Efektif
- LAMPIRAN 5 : Rapat Penyusunan Draft Peraturan Kepala Badan Siber Dan Sandi Negara Tentang Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik
- LAMPIRAN 6 : Rapat Penyusunan Standar Operasional Prosedur (Sop) Penilaian Risiko (Risk Assesment)
- LAMPIRAN 7 : Rapat Penyusunan Petunjuk Tekhnis (Juknis) Penilaian Risiko (Risk Assesment)
- LAMPIRAN 8 : Pelatihan Peningkatan Kemampuan Dasar Pegawai Dalam Melakukan Penilaian Risiko
- LAMPIRAN 9 : Sosialisasi Draft Peraturan Kepala Badan Siber Dan Sandi Negara Tentang Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik
- LAMPIRAN 10 : Sertifikat Pelatihan Mata Pelajaran Pilihan
- LAMPIRAN 11 : Dukungan Pimpinan Terhadap Proyek Perubahan Yang Dilakukan
- LAMPIRAN 12 : Lembar Konsultasi / Bimbingan
- LAMPIRAN 13 : Promosi, Brosur Dan Leaflet

BAB I

RANCANGAN PROYEK PERUBAHAN

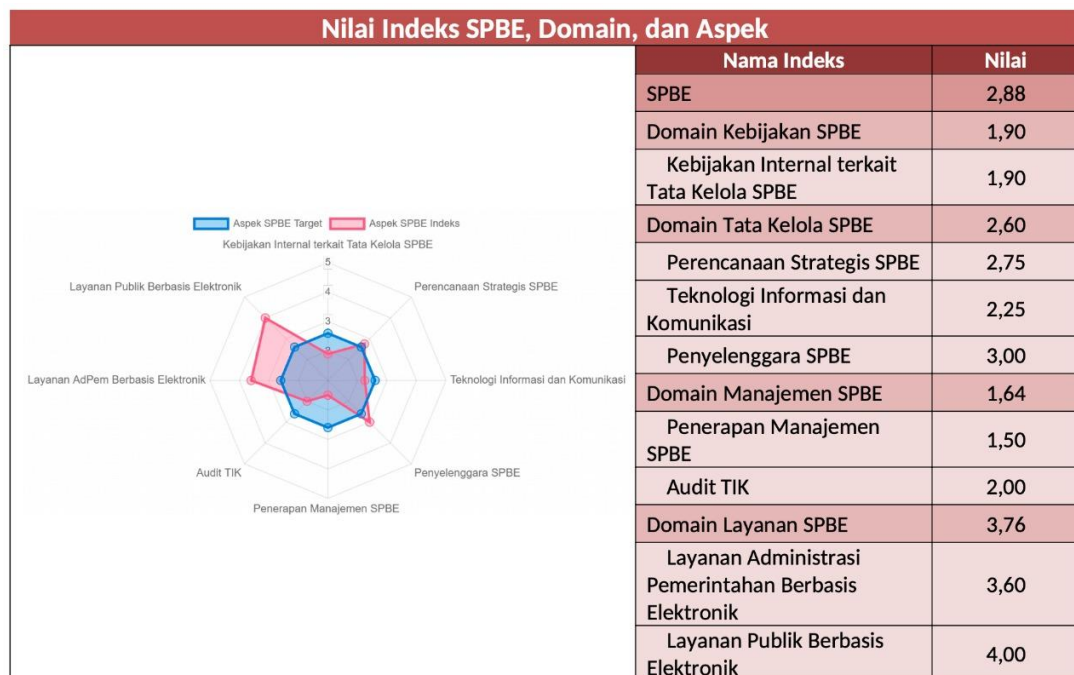
I. DESKRIPSI PROYEK PERUBAHAN

Pusat Data dan Teknologi Informasi Komunikasi (Pusdatik) Badan Siber dan Sandi Negara (BSSN) merupakan salah satu Unit Kerja di lingkungan BSSN yang mempunyai tugas secara garis besarnya adalah perencanaan, pengelolaan dan evaluasi teknologi informasi dan komunikasi, dimana didalam salah satu fungsinya adalah untuk melakukan manajemen risiko sistem pemerintahan berbasis elektronik. Hal ini sesuai dengan yang diamanatkan dalam Peraturan Presiden nomor 95 tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, (SPBE) untuk dapat diterapkan di lingkungan setiap Instansi kementerian/Lembaga.

Dalam prakteknya sejak dibentuknya Pusdatik BSSN tahun 2017 dan mengalami validasi tahun 2021 sampai dengan sekarang, Pusdatik belum dapat (belum pernah) melaksanakan kegiatan manajemen risiko, sehingga dari hasil laporan evaluasi SPBE BSSN yang dilaksanakan oleh Kemenpan RB tahun 2021 didapatkan indeks untuk Domain Manajemen SPBE masih sangat rendah yaitu 1,64 dari skala 1 – 5, seperti dalam tabel di bawah.

Tabel 1

Nilai indeks SPBE BSSN yang dikeluarkan KemenPAN RB Tahun 2021



Dari table 1 di atas, menunjukkan bahwa hasil Penilaian SPBE BSSN dari Kemenpan RB tahun 2021 adalah 2,88. Nilai ini dibawah target yang telah ditentukan sebelumnya yaitu 3,30. Domain Manajemen SPBE menyumbang nilai terendah yaitu 1,64. Indeks 2,88 ini telah menempatkan BSSN pada urutan ke 80 dari keseluruhan instansi pemerintah.

Karena perubahan organisasi yang masih baru, menyebabkan alat kelengkapan organisasi yang ada saat ini belum memadai, menyebabkan kesulitan untuk mencapai target nilai indeks SPBE yang telah ditetapkan, maka Kapusdatik melalui Nota Dinas Nomor : 11/P2/PR.01.02/01/2022 tanggal 17 Januari 2022, BSSN mengajukan permohonan perubahan Target Indeks SPBE BSSN pada Renstra BSSN Tahun 2020-2024, sebagaimana dalam Tabel 2 di bawah.

Tabel 2

Perubahan Target SPBE BSSN

No.	Sasaran Kegiatan	Indikator Kinerja Sasaran Kegiatan	Target Semula			
			2021	2022	2023	2024
1.	Terwujudnya Tata Kelola TIK yang aman dan andal	1.1 Indeks Sistem Pemerintahan Berbasis Elektronik	3.30	3.50	3.80	4.00

No.	Sasaran Kegiatan	Indikator Kinerja Sasaran Kegiatan	Target Menjadi			
			2021	2022	2023	2024
1.	Terwujudnya Tata Kelola TIK yang aman dan andal	1.1 Indeks Sistem Pemerintahan Berbasis	2.70	2.90	3.10	3.30

Belum dapat dilaksanakannya kegiatan Manajemen risiko oleh Pusdatik saat ini disebabkan karena adanya beberapa kendala yaitu :

1. Belum adanya peraturan yang dapat dijadikan landasan bagi Pusdatik untuk dapat melakukan kegiatan penilaian risiko di unit kerja lain
2. Masih sangat minimnya jumlah pegawai yang memiliki kompetensi atau mengikuti pelatihan penilaian risiko, yaitu baru 1 orang saja.
3. Tidak adanya sarana prasarana pendukung untuk melakukan kegiatan dalam penilaian risiko.

Oleh karena itu dalam rangka meningkatkan capaian nilai indeks SPBE pada Domain Manajemen SPBE, maka perlu adanya optimalisasi pada Pusdatik khususnya dalam hal penilaian risiko, sehingga kegiatan manajemen risiko di BSSN dapat dilaksanakan, yaitu meliputi :

1. Pembuatan Peraturan / Kebijakan berupa :
 - Peraturan Kepala BSSN tentang Manajemen Risiko SPBE.
 - Standar Operasional Prosedur Penilaian Risiko (Risk Assesment).
 - Petunjuk Tekhnis Risiko (Risk Assesment).
2. Peningkatan kompetensi pegawai sebagai Tim Risk Assesment.
3. Pemenuhan sarana prasarana Tim Risk Assesment.
4. Sosialisasi tentang Manajemen risiko SPBE kepada pegawai.

Pengertian Istilah:

1. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada Pengguna SPBE.
2. Teknologi Informasi Komunikasi yang selanjutnya disingkat TIK adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi.
3. Manajemen Risiko SPBE adalah pendekatan sistematis yang meliputi proses, pengukuran, struktur, dan budaya untuk menentukan tindakan terbaik terkait Risiko SPBE.
4. Risiko SPBE adalah peluang terjadinya suatu peristiwa yang akan mempengaruhi keberhasilan terhadap pencapaian tujuan penerapan SPBE.

II. LATAR BELAKANG

A. Dasar Hukum

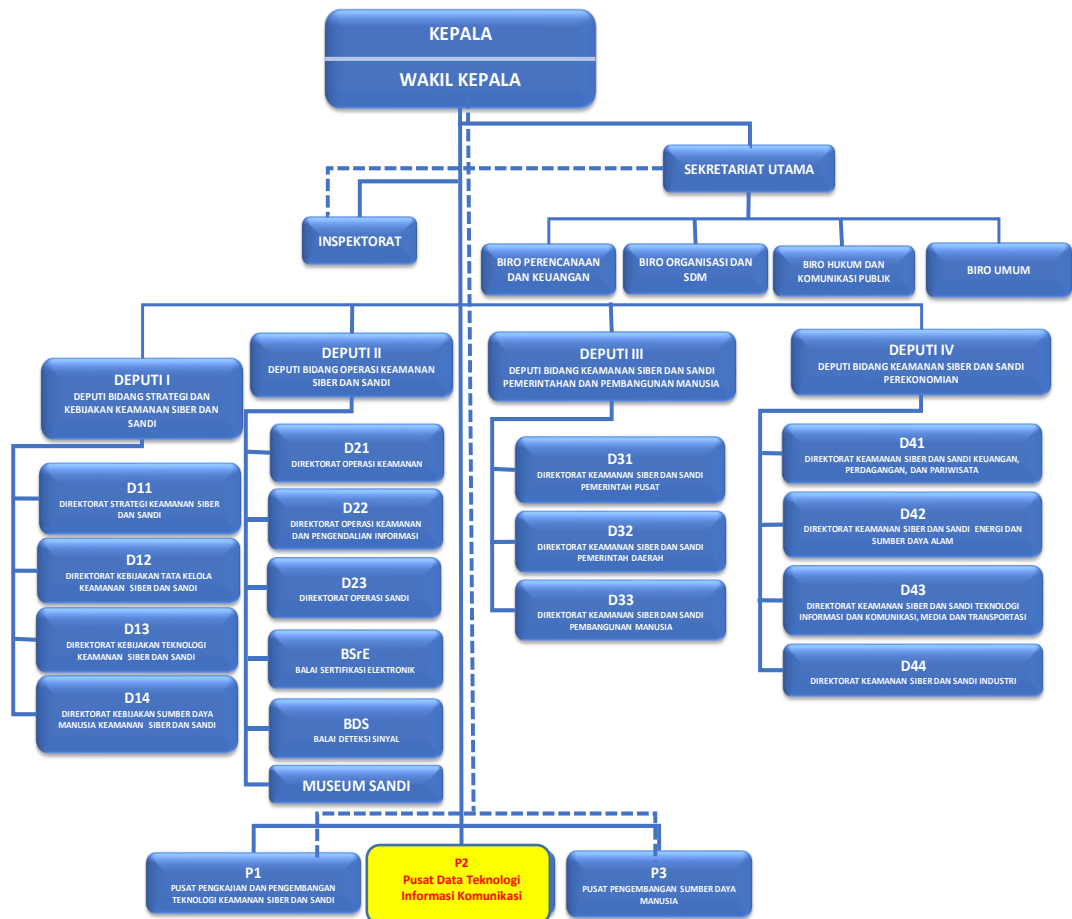
- Peraturan Presiden Nomor 28 tahun 2021 tentang Badan Siber dan Sandi Negara.
- Peraturan Badan Siber dan Sandi Negara Nomor 6 tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara.
- Peraturan Presiden Nomor 95 Tahun 2018, tentang Sistem Pemerintahan Berbasis Elektronik (SPBE).
- Permenpan RB Nomor 59 Tahun 2020 tentang Pemantauan Dan Evaluasi Sistem Pemerintahan Berbasis Elektronik.
- Rencana Strategis (Renstra) BSSN Tahun 2020-2024 yang memuat visi, misi, tujuan, kebijakan, program, dan kegiatan indikatif sesuai dengan tugas dan fungsi BSSN.

Berdasarkan regulasi tersebut maka perlu dilakukan upaya untuk meningkatkan kepercayaan para pemangku kepentingan khususnya dan masyarakat pada umumnya dalam mewujudkan tata Kelola sistem pemerintahan berbasis elektronik yang baik dan aman, salah satunya melalui manajemen penilaian risiko keamanan siber SPBE.

B. Struktur Organisasi

Gambar 1

Struktur Organisasi BSSN



C. Tugas Pokok BSSN

Melaksanakan tugas pemerintahan di bidang keamanan siber dan sandi untuk membantu Presiden dalam menyelenggarakan pemerintahan.

D. Fungsi BSSN

Pasal 3 Peraturan BSSN Nomor 28 Tahun 2021 disebutkan fungsi dari BSSN meliputi:

1. Perumusan dan penetapan kebijakan teknis di bidang keamanan siber dan sandi.
2. Pelaksanaan kebijakan teknis di bidang keamanan siber dan sandi.
3. Penyusunan norma, standar, prosedur, dan kriteria di bidang persandian.
4. Pelaksanaan bimbingan teknis dan supervisi di bidang persandian.
5. Koordinasi pelaksanaan tugas, pembinaan, dan dukungan administrasi kepada seluruh unsur organisasi di lingkungan BSSN.
6. Pengelolaan barang milik negara yang menjadi tanggung jawab BSSN.
7. Pelaksanaan dukungan yang bersifat substantif kepada seluruh unsur organisasi di lingkungan BSSN.
8. Pengawasan atas pelaksanaan tugas di lingkungan BSSN.

E. Tugas Pokok Pusat Data dan Teknologi Informasi Komunikasi (Pusdatik) BSSN.

Melaksanakan perencanaan, pelaksanaan, evaluasi dan pelaporan di bidang data dan teknologi informasi komunikasi.

F. Fungsi Pusdatik BSSN

Peraturan BSSN Nomor 6 Tahun 2021, Pasal 105 disebutkan fungsi dari Pusdatik meliputi:

1. Penyusunan rencana teknologi informasi komunikasi, pengembangan sistem informasi, pengelolaan data, penyelenggaraan pusat data dan teknologi informasi komunikasi, layanan teknologi informasi komunikasi, pengelolaan keamanan informasi dan keamanan teknologi informasi komunikasi, dan penyelenggaran persandian di lingkungan BSSN.
2. Pelaksanaan pengelolaan teknologi informasi komunikasi, pengembangan sistem informasi, pengelolaa data, penyelenggaraan pusat data dan teknologi informasi komunikasi, penjaminan kelangsungan data dan teknologi informasi komunikasi, dan penyelenggaran persandian di lingkungan BSSN.
3. Penyusunan evaluasi dan pelaporan pengelolaan teknologi informasi komunikasi, pengembangan sistem informasi, pengelolaan data, penyelenggaraan pusat data dan teknologi informasi komunikasi, penjaminan kelangsungan data dan teknologi informasi komunikasi, dan penyelenggaran persandian di lingkungan BSSN.
4. Pelaksanaan urusan keuangan, kepegawaian, ketatalaksanaan, tata usaha, arsip, rumah tangga, inventarisasi barang milik negara, pengumpulan bahan laporan kinerja, dan program kerja pusat.

G. Isu isu strategis ancaman siber

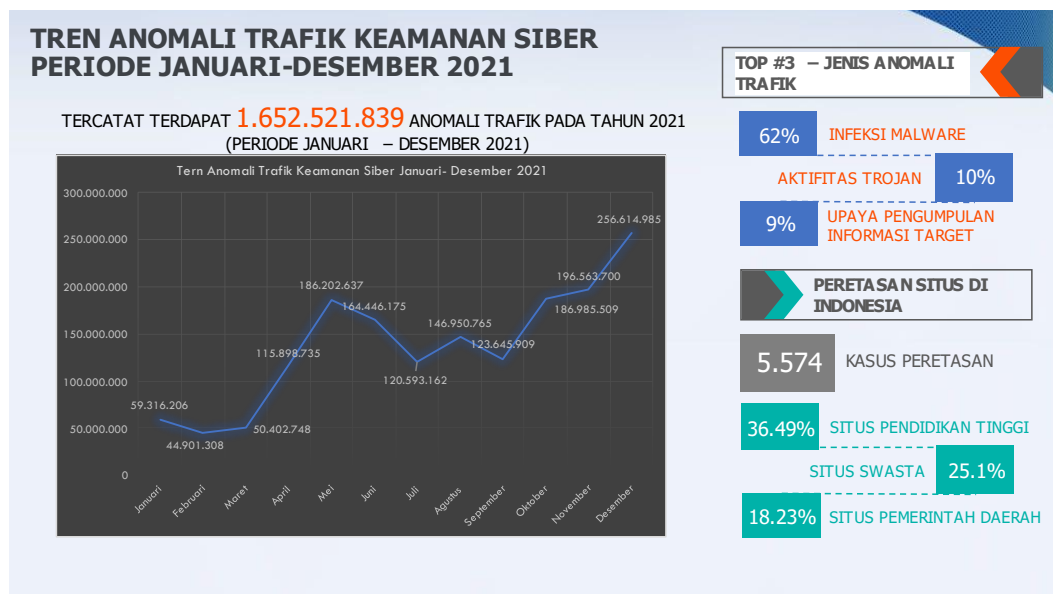
Teknologi Informasi dan Komunikasi (TIK) seperti pedang bermata dua, karena dapat berkontribusi dalam meningkatkan kemajuan peradaban manusia serta dapat juga menjadi sarana yang efektif dalam pelanggaran hukum. Transformasi TIK membuat ancaman siber yang dihadapi suatu negara menjadi lebih kompleks, mengubah pemahaman terhadap kekuatan dan kedaulatan negara, tidak hanya dilihat dari aspek ekonomi dan militer yang dimiliki, tetapi juga dilihat dari aspek kekuatan siber dalam menghadapi ancaman siber. TIK dapat menjadi sumber dari berbagai ancaman dengan aktor (sumber ancaman) yang berasal dari pemerintah, organisasi, kelompok, dan perorangan yang dilakukan dengan unsur kesengajaan maupun tidak dengan maksud untuk mendapatkan keuntungan secara politik, militer, dan ekonomi, maupun dengan tujuan lain. Dalam era siber, jika suatu negara tidak mampu untuk menguasai TIK secara baik dan tepat guna serta terjadi penyalahgunaan TIK, hal tersebut dapat menjadi sumber ancaman bagi keamanan dan ketahanan nasional suatu negara. Keamanan siber memiliki peran penting dalam menjaga keamanan informasi karena menjadi hal yang krusial untuk menjaga data dalam media penyimpanan dan menjamin informasi yang dikirim dalam keadaan aman serta perlindungan sistem informasi terhadap ancaman siber.

Berdasarkan hasil monitoring BSSN, pada periode bulan Januari-Desember 2021 tercatat telah terdapat 1.652.521.839 (satu

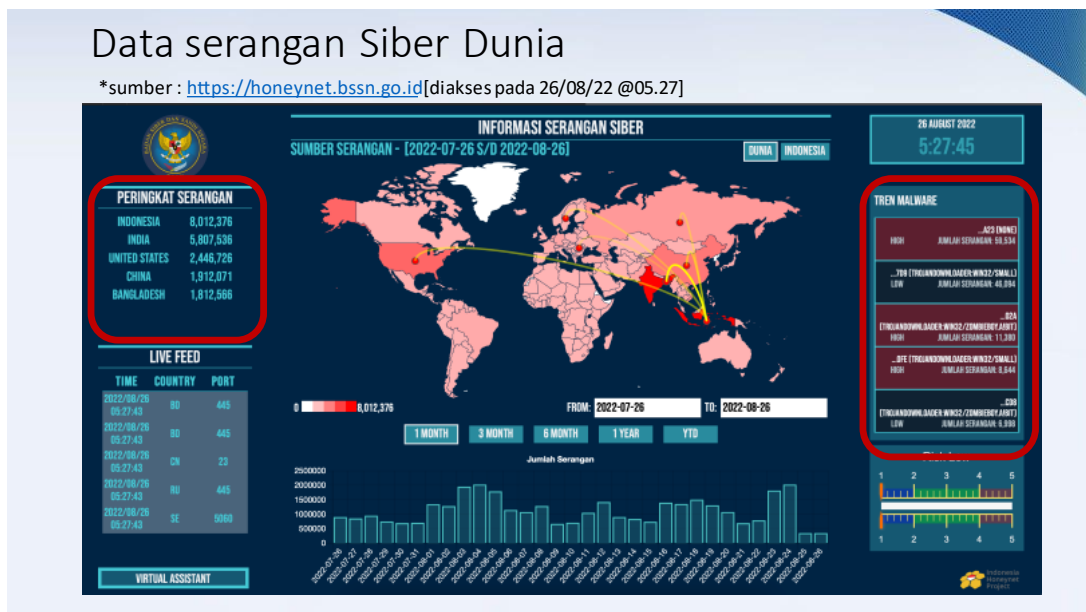
milyar enam ratus lima puluh dua juta lima ratus dua puluh satu ribu delapan ratus tiga puluh sembilan) juta anomali trafik diantaranya berupa serangan siber, dengan kategori anomali terbanyak yaitu malware, Denial of Service (mengganggu ketersediaan layanan), dan trojan activity (aktivitas trojan). Serangan siber yang menjadi perhatian dan terus mengalami peningkatan yaitu banyaknya serangan grup ransomware dan data leaks (kebocoran data) yang dilakukan oleh threat actor yang mayoritas dilatarbelakangi oleh motif untuk mendapatkan data-data milik pemerintah.

Tabel 3

Tren Anomali Trafik Keamanan Siber periode Januari-Desember 2021



Tabel 4
Data Serangan Siber di Dunia



Tercatat sedikitnya ada 10 Serangan siber terbesar dalam Sejarah di dunia, yaitu :

1. Serangan siber di Jaringan PlayStation Sony

Sebuah serangan cyber di Jaringan PlayStation Sony pada bulan April 2011 merenggut informasi pribadi 77 juta pengguna.

2. Serangan Cyber NASA

Pada tahun 1999, James Jonathan yang berusia 15 tahun mampu meretas dan mematikan komputer NASA selama 21 hari. Sekitar 1,7 juta perangkat lunak diunduh selama serangan itu, yang menelan biaya perbaikan sekitar \$ 41.000.

3. Serangan Cyber Estonia 2007

Pada bulan April 2007, Estonia menyaksikan apa yang dianggap sebagai serangan cyber pertama di seluruh negara, di mana sekitar 58 situs Estonia menjadi offline, termasuk situs pemerintah, bank, dan media.

4. Penghancuran Virus Melissa

Salah satu ancaman cyber paling awal dan terbesar dimulai oleh Melissa Virus. Pada tahun 1999, Melissa Virus diluncurkan oleh programmer David Lee Smith dengan mengirimkan file kepada pengguna untuk dibuka oleh Microsoft Word. Virus ini menyebabkan kerusakan parah pada ratusan perusahaan, termasuk Microsoft. Diperkirakan bahwa perbaikan sistem yang terkena biaya sekitar \$80 juta.

5. Serangan Siber Adobe

Serangan siber yang pertama kali dianggap telah membobol data 2,9 juta pengguna segera berlanjut dengan membahayakan data pribadi hingga 38 juta pengguna. Adobe mengklaim bahwa hanya kata sandi dan informasi kartu kredit dari 2,9 juta pertama yang dikompromikan, sedangkan 35,1 juta sisanya hanya kehilangan kata sandi dan ID mereka.

6. Serangan Cyber 2014 di Yahoo

Pada tahun 2014, Yahoo menyaksikan salah satu serangan cyber terbesar tahun itu ketika 500 juta akun disusupi. Namun, dilaporkan bahwa informasi dasar dan kata sandi dicuri, sedangkan informasi bank tidak.

7. Serangan Jaringan Listrik Ukraina

Dalam serangan siber pertama pada jaringan listrik, serangan tersebut menyebabkan sekitar setengah dari rumah di wilayah Ivano-Frankivsk di Ukraina tanpa listrik pada tahun 2015 selama sekitar beberapa jam.

8. WannaCry Ransomware Cyber Attack 2017

Salah satu ransomware terbesar sepanjang masa terjadi pada tahun 2017, ketika sekitar 200.000 komputer terpengaruh di lebih dari 150 negara. Wabah ini memiliki dampak besar di beberapa industri dan memiliki biaya global sekitar 6 miliar pound.

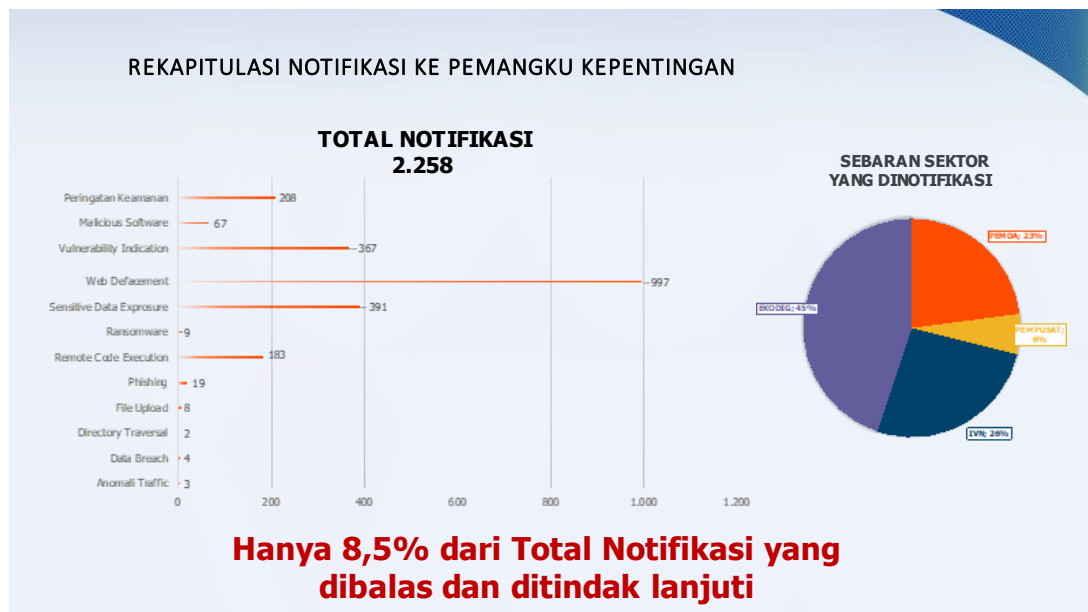
9. Serangan Siber di Hotel Marriott tidak diperhatikan selama bertahun-tahun

Serangan siber mengintai cukup lama ketika Marriott mengakuisisi grup Starwood Hotels, dan baru terungkap pada 2018. Namun, saat itu penyerang terus memiliki akses ke informasi pribadi tamu. Diperkirakan 339 juta tamu telah dikompromikan datanya. Hal ini menyebabkan pengawas privasi data Inggris mendenda Hotel Marriott sebesar 18,4 juta pound.

10. Kebocoran kata sandi terbesar RockYou2021

Dilaporkan awal Juni ini bahwa kompilasi sekitar 8.4B kata sandi bocor. Sejauh ini kebocoran kata sandi terbesar dan disebut sebagai RockYou2021 mengacu pada pelanggaran data 2009 situs RockYou yang mengkompromikan sekitar 32 juta akun.

Tabel 5
Rekapitulasi Notifikasi ke Pemangku Kepentingan



Beberapa contoh kasus serangan siber di Indonesia

1. Tahun 2021 terjadi cukup banyak kasus kebocoran data di Indonesia. Tercatat setidaknya ada delapan kasus kebocoran data di Indonesia selama tahun 2021. Salah satu yang paling heboh adalah beredarnya sertifikat vaksin Jokowi di media sosial. Kebocoran data ini berasal dari pihak luar, seperti Facebook. Sementara dari pihak dalam negeri, ada enam kasus kebocoran data yang terjadi. Berikut kasus kebocoran data di Indonesia selama 2021:
 - a. Facebook (April 2021)
 - b. BPJS Kesehatan (Mei 2021)
 - c. BRI Life (Juli 2021)
 - d. eHAC (Agustus 2021)
 - e. Sertifikat Vaksin Jokowi (September 2021)
 - f. KPAI (Oktober 2021)

- g. Bank Jatim (Oktober 2021)
 - i. Database Polri (November 2021)
2. Pada Kamis 20 Januari 2022 telah terjadi kebocoran data Bank Indonesia yang dilakukan oleh akun Geng ransomware Conti. Diungkapkan bahwa data BI yang dibobol 838 file sebesar 487,09 MB dan perangkat PC BI yang diretas hanya 16 unit. Pada hari Senin 24 Januari kebocoran data milik BI itu dikabarkan oleh salah satu platform intelijen bernama Dark Tracer lewat Twitter jumlahnya bertambah mencapai 74GB. Jumlah perangkat milik BI yang diretas meningkat menjadi 237 unit.
 3. Terakhir yang paling membuat heboh di bulan September 2022 adalah kasus peretasan yang dilakukan oleh Hacker yang menamakan dirinya Bjorka. Bjorka berhasil meretas 3 jenis data rahasia, di antaranya 150 juta data penduduk Indonesia, data 1,3 miliar pengguna SIM card, hingga Surat Rahasia BIN ke Presiden Joko Widodo (Jokowi). Disamping itu juga data pribadi beberapa pejabat negara.

Badan Siber dan Sandi Negara juga tidak luput dari upaya serangan siber, diketahui bahwa

1. Pada Rabu tanggal 20 Oktober 2021, situs www.pusmanas.bssn.go.id diretas, dengan tampilan "Hacked by theMx0nday". Ternyata, pelaku yang diduga asal Brasil itu membalas dendam karena hacker Indonesia juga meretas website negara Brasil.

2. Pada Senin tanggal 31 Januari 2022 Situs Jaringan Dokumentasi dan Informasi Hukum (JDIH) milik Badan Siber dan Sandi Negara (BSSN) diduga mengalami kebocoran data. Kabar kebocoran data itu disampaikan oleh akun @darkTracer di Twitter. Nama file yang ada dalam data yang dibocorkan dan dibagikan p0L1cy di RaidForums mengindikasikan data ini milik JDIH BSSN.

H. Kondisi awal

1. Terbentuknya organisasi BSSN.

Badan Siber dan Sandi Negara (BSSN) merupakan instansi pemerintah yang bergerak di bidang keamanan informasi dan keamanan siber, yang didirikan berdasarkan Peraturan Presiden (Perpres) Nomor 53 Tahun 2017 tanggal 19 Mei 2017. Kemudian dirubah dengan Perpres Nomor 133 tahun 2017 tanggal 16 Desember 2017. Dan organisasi mulai efektif berjalan pada pertengahan tahun 2018.

BSSN merupakan penguatan atas badan yang sebelumnya telah ada, yakni Lembaga Sandi Negara dan Direktorat Keamanan Informasi, Direktorat Jenderal Aplikasi Informatika, Kementerian Komunikasi dan Informatika. Dengan dibentuknya BSSN, berbagai tugas dan fungsi yang sebelumnya diemban oleh berbagai Lembaga di atas dilaksanakan oleh BSSN.

Pembentukan BSSN sebagai penguatan atas lembaga yang sebelumnya telah ada didorong oleh kemajuan teknologi komunikasi dan informasi yang turut membawa risiko dan

ancaman penyalahgunaan terhadapnya yang kian hari kian canggih dan kompleks. Tantangan keamanan siber saat ini semakin besar karena perkembangan Internet of Things dan terkoneksiya lembaga dan unit dari segala bidang, baik publik maupun swasta.

2. Validasi organisasi BSSN.

Pada 13 April 2021, Presiden Joko Widodo menetapkan Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara. Dengan Perpres yang baru ini, terjadi perubahan kembali dalam struktur organisasi BSSN. Ini tentunya berpengaruh terhadap kebijakan dan peraturan-peraturan yang ada, perlu diperbarui atau dibuat lagi.

3 Evaluasi SPBE

Sesuai dengan Peraturan Presiden Nomor 95 Tahun 2018, Sistem Pemerintahan Berbasis Elektronik (SPBE) sebagai inisiasi KemenpanRB dalam mewujudkan tata kelola Teknologi Informasi dan Komunikasi (TIK) yang bersih, efektif, transparan dan akuntabel, mengharuskan seluruh Instansi Pusat dan Daerah untuk melakukan upaya – upaya sebagaimana yang tertera pada Domain SPBE. Badan Siber dan Sandi Negara (BSSN) dalam hal ini selaku pengguna SPBE, perlu melakukan hal yang menjadi fokus SPBE salah satunya adalah pada domain Manajemen SPBE terkait Tingkat Kematangan Penerapan Manajemen Risiko SPBE.

Pada Permenpan RB Nomor 59 Tahun 2020 tentang Pemantauan Dan Evaluasi Sistem Pemerintahan Berbasis

Elektronik, pada Domain Manajemen SPBE dijelaskan bahwa salah satu aspek manajemen yang dihitung tingkat kematangannya adalah Tingkat Kematangan Manajemen Risiko. Manajemen Risiko itu sendiri menurut Permenpan RB Nomor 5 Tahun 2020 adalah Manajemen Risiko SPBE adalah pendekatan sistematis yang meliputi proses, pengukuran, struktur, dan budaya untuk menentukan tindakan terbaik terkait Risiko SPBE.

4. Sumber daya penanganan Manajemen Risiko.

Komposisi pegawai BSSN saat ini khususnya di Pusdatik yang terbatas dan belum didukung dengan kompetensi dalam penanganan manajemen risiko keamanan siber, disamping itu juga belum didukung dengan kelengkapan sarana prasarana sumber daya pendukung penilaian risiko siber, yang masih dalam tahap pengembangan/pembangunan dengan berubahnya organisasi.

Tabel 6
Daftar pegawai, aplikasi, perangkat dan Security Perimeter

NO	URAIAN	JUMLAH	KETERANGAN
1	Pegawai BSSN	1418	
	Pegawai Pusdatik	83	
	Pegawai yang telah mendapat pelatihan risk management	1	
2	Aplikasi Existing	328	
	Aplikasi On	142	
	Aplikasi Off	186	
3	Perangkat Data Center	46	
	a.Power PLN	2	2770 kW
	b.Trafo	2	3150 kW
	c.Genset	2	1250 kW
	d.Fuel tank	4	2 x15000 ltr
			2 x 1000 ltr

NO	URAIAN	JUMLAH	KETERANGAN
	e.Cooling	8	unit PAC (untuk Datahall, UPS)
	f.UPS	8	unit UPS 300 kVA (Cooling)
	g.Rak Server	20	rak
4	Security Perimeter		
	a.Anti DDOS, Network Firewall, Publisher		
	b.NVR & CCTV	13	titik
	c.Access Control	15	titik

5. Identifikasi masalah.

Identifikasi masalah dalam Proyek Perubahan ini dilakukan menggunakan analisis USG (*Urgency, Seriousness, Growth*). Analisis USG adalah salah satu metode skoring untuk menyusun urutan prioritas isu yang harus diselesaikan. Pada tahap ini masing-masing masalah dinilai tingkat risiko dan dampaknya dengan cara pemberian skor. Penyelesaian dilakukan dengan menggunakan Skala Likert 1-5 (5=Sangat besar, 4=Besar, 3=Sedang, 2=Kecil, 1=Sangat kecil). Masalah yang memiliki total skor tertinggi merupakan masalah yang harus diprioritaskan untuk diselesaikan.

- a. *Urgency*. Seberapa mendesak isu tersebut harus dibahas dikaitkan dengan waktu yang tersedia serta seberapa keras tekanan waktu tersebut untuk memecahkan masalah yang menyebabkan isu tadi.
- b. *Seriousness*. Seberapa serius isu tersebut perlu dibahas dikaitkan dengan akibat yang timbul dengan penundaan pemecahan masalah yang menimbulkan isu tersebut atau akibat yang menimbulkan masalah-masalah lain kalau masalah penyebab isu tidak dipecahkan. Perlu dimengerti bahwa dalam

keadaan yang sama, suatu masalah yang dapat menimbulkan masalah lain adalah lebih serius bila dibandingkan dengan suatu masalah lain yang berdiri sendiri.

- c. *Growth*. Seberapa kemungkinan-kemungkinannya isu tersebut menjadi berkembang dikaitkan kemungkinan masalah penyebab isu akan makin memburuk kalau dibiarkan.

Tabel 7
Analisis USG

No.	Isu Strategis	U	S	G	Jumlah Skor	Peringkat	Fakta
1.	Pelaksanaan manajemen risiko siber telah efektif dilaksanakan dalam mengantisipasi serangan siber dan kebocoran data dengan menggunakan pedoman yang telah ditetapkan	5	5	5	15	1	- Pelaksanaan penilaian serangan siber belum dapat dilaksanakan secara optimal. - Belum ada peraturan yang dijadikan pedoman, termasuk SOP dan petunjuk teknis.
2.	Sumber daya BSSN sudah mencukup untuk melaksanakan kegiatan penilaian risiko saat ini	5	4	4	13	2	Sumber daya manusia yang telah memiliki kompetensi dalam penilaian risiko masih sedikit dan belum terdukung dengan adanya sarana prasana yang memadai
3.	Penilaian risiko keamanan siber telah dilaksanakan secara berkesinambungan.	4	4	4	12	3	Penilaian risiko keamanan siber belum dapat dilaksanakan secara berkesinambungan karena terkendala peraturan dan sumber daya yang masih terbatas

Berdasarkan hasil analisis USG yang disajikan dalam Tabel 7, maka masalah yang diprioritaskan untuk diselesaikan adalah melakukan perbaikan terhadap pelaksanaan manajemen risiko keamanan siber di BSSN melalui pembuatan peraturan, SOP, Petunjuk teknis dan peningkatan kompetensi pegawai serta sarana prasarana pendukung, yang selanjutnya akan ditindaklanjuti dengan mengimplementasikan penilaian keamanan siber tersebut sebagai upaya untuk meningkatkan tata kelola pelaksanaan SPBE di lingkungan BSSN.

Berdasarkan analisis kondisi diatas dapat disimpulkan bahwa:

1. Manajemen Risiko Keamanan Siber belum dapat dilaksanakan secara optimal sebagai alat ukur untuk penilaian SPBE di BSSN, sehingga perlu ditingkatkan.
2. Belum ada peraturan Kepala yang dapat dijadikan pedoman bagi Tim Penilai untuk melaksanakan penilaian risiko keamanan siber di BSSN.
3. Belum ada standar operasional prosedur dalam melakukan penilaian risiko (risk assessment).
4. Belum ada petunjuk teknis dalam melakukan penilaian risiko (risk assessment).
5. Pegawai yang memiliki kemampuan dan ketrampilan dalam penilaian risiko masih terbatas/sedikit.
6. Sarana Prasarana pendukung kegiatan penilaian risiko belum terpenuhi.

7. Pemahaman pegawai secara umum terkait penilaian risiko masih kurang.

I. Kondisi yang Diharapkan (Kondisi Ideal)

Kondisi yang diharapkan adalah sebagai berikut:

1. Tidak terjadi lagi kasus serangan siber / kebocoran data khususnya di lingkungan BSSN.
2. Kegiatan manajemen dan penilaian risiko SPBE dapat dilaksanakan secara rutin dan berkelanjutan di lingkungan BSSN.
3. Jumlah pegawai yang memiliki kompetensi dalam hal manajemen dan penilaian risiko keamanan siber terpenuhi dan meningkat.
4. Tersedianya sarana prasana pendukung untuk penilaian risiko keamanan siber secara memadai.
5. Meningkatnya Pemahaman pegawai secara umum terkait penilaian risiko.

J. Gap yang muncul berdasarkan kondisi awal dan kondisi yang diharapkan

Kondisi Pembentukan organisasi yang masih baru dan adaya validasi organisasi setelahnya, dimana organisasi masih mencari bentuk yang efektif dan efisien dalam operasional kegiatannya, sehingga alat kelengkapan organisasi dan peraturan belum ada / belum mendukung seluruhnya.

Perubahan organisasi juga mengakibatkan tidak optimalnya kinerja pegawai karena diklat belum dipersiapkan dan kurangnya sarana prasana terkait.

K. Gagasan Proyek Perubahan

Berdasarkan analisis kondisi di atas, gagasan yang ditawarkan untuk menyelesaikan masalah tersebut adalah Optimalisasi Pusdatik Dalam Melakukan Manajemen Risiko SPBE di Lingkungan Badan Siber dan Sandi Negara, yaitu dengan cara :

1. Pembuatan Piranti Lunak (kebijakan) berupa :
 - Peraturan Kepala Badan Siber dan Sandi Negara tentang Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik.
 - Standar Operasional Prosedur Penilaian Risiko (Risk Assesment)
 - Petunjuk Tekhnis Penilaian Risiko (Risk Assesment)
2. Peningkatan kompetensi pegawai sebagai Tim Risk Assesment
3. Pemenuhan sarana prasarana Tim Risk Assesment
4. Sosialisasi tentang budaya Kamsiber (Keamanan Siber) kepada pegawai

L. Strategi untuk mewujudkan gagasan

Dalam upaya untuk melakukan Optimalisasi Pusdatik Dalam Melakukan Manajemen Risiko SPBE di lingkungan BSSN dengan mempertimbangkan kondisi saat ini dan kondisi yang diharapkan, maka dilakukan analisis SOAR.

Analisis SOAR (Strength, Opportunities, Aspirations, Results) dikembangkan oleh Stavros dkk pada tahun 2003. Analisis SOAR sebagai alternatif terhadap analisis SWOT. Model SOAR mengubah analisis SWOT, yang sudah sangat mapan, dalam hal faktor-faktor kekurangan (*weakness*) internal organisasi serta ancaman (*threats*) eksternal yang dihadapinya ke dalam faktor-faktor aspirasi (*aspiration*) yang dimiliki organisasi serta hasil (*results*) terukur yang ingin dicapai. Analisis SOAR terdiri atas empat elemen sebagai berikut:

1. *Strength* (S) merupakan segala hal yang menjadi kekuatan dan kemampuan terbesar yang dimiliki, berupa aset baik aset yang berwujud maupun aset yang tidak berwujud yang mampu mendukung keberlangsungan usaha. Kekuatan akan terus dikembangkan demi kemajuan organisasi di masa depan. Dalam hal ini *strength* (S) yang dimiliki BSSN adalah: (1) adanya landasan hukum yang kuat bagi BSSN sebagai penyelenggara keamanan siber, (2) rata-rata latar belakang Pendidikan pegawai BSSN di bidang IT.
2. *Opportunities* (O) merupakan bagian dari lingkungan eksternal yang harus di analisis agar mudah memahami apa yang harus dilakukan agar dapat dimanfaatkan. Peluang akan memberikan manfaat bagi organisasi jika organisasi tersebut mampu meraih peluang tersebut dengan cepat dan tepat. Dalam kaitan ini, *opportunities* (O) yang dimiliki BSSN adalah: (1) dorongan dari

- Pimpinan BSSN untuk meningkatkan keamanan siber (2) dukungan dari para pemangku kepentingan.
3. *Aspirations* (A) merupakan harapan, visi dan misi yang ingin dicapai guna membentuk kepercayaan diri terhadap produk, pasar dan hal apapun yang dikerjakan demi mencapai visi yang diharapkan sehingga munculah perasaan positif dan semangat dalam meningkatkan kinerja serta pelayanan. Dalam hal ini *aspirations* (A) BSSN adalah: (1) Terciptanya kebijakan pimpinan berupa peraturan, Standar Operasional Prosedur dan Petunjuk Teknis dalam penilaian risiko, (2) Meningkatnya kompetensi dan kemampuan pegawai khususnya tim penilai risiko keamanan, (3) Terdukungnya sarana prasana penilaian risiko yang memadai.
4. *Results* (R) merupakan hasil-hasil yang ingin dicapai dalam perencanaan strategis, guna mengetahui sejauh mana pencapaian dari tujuan yang telah disepakati bersama. Dalam hal ini *results* (R) yang diharapkan dapat tercapai oleh BSSN adalah: (1) Terwujudnya manajemen SPBE yang baik di BSSN, (2) Meningkatnya kepercayaan stakeholder dalam beraktifitas di ruang siber secara aman.

Analisis SOAR BSSN dalam upaya meningkatkan keamanan siber melalui penilaian risiko keamanan siber disajikan dalam Tabel 8.

Tabel 8

Analisis SOAR

ANALISIS SOAR	STRENGTHS (S) - Adanya landasan hukum yang kuat bagi BSSN sebagai penyelenggara keamanan siber - Rata-rata latar belakang pegawai di bidang IT	OPORTUNITIES (O) - Dorongan dari Pimpinan BSSN untuk terus meningkatkan keamanan siber - Dukungan dari para pemangku kepentingan
ASPIRATIONS (A) - Terciptanya kebijakan pimpinan berupa perturan, SOP dan Juknis dalam penilaian risiko - Meningkatnya kompetensi dan kemampuan pegawai khususnya tim penilai risiko keamanan - Terdukungnya sarana prasana penilaian risiko yang memadai	S+A Dengan adanya landasan hukum yang kuat bagi BSSN sebagai penyelenggara keamanan siber dan rata-rata latar belakang pendidikan pegawai di bidang IT, maka akan dapat mempermudah dalam menyusun kebijakan pimpinan berupa perturan, SOP dan Juknis dalam penilaian risiko, lebih mudah dalam meningkatnya kompetensi dan kemampuan pegawai khususnya tim penilai risiko keamanan serta mudah mendapatkan dukungan sarana prasana penilaian risiko yang memadai	O+A Dengan adanya dorongan dari Pimpinan BSSN untuk terus meningkatkan keamanan siber dan dukungan dari para pemangku kepentingan, maka akan dapat mempermudah dalam menyusun kebijakan pimpinan berupa perturan, SOP dan Juknis dalam penilaian risiko, lebih mudah dalam meningkatnya kompetensi dan kemampuan pegawai khususnya tim penilai risiko keamanan serta mudah mendapatkan dukungan sarana prasana penilaian risiko yang memadai
RESULTS (R) - Terwujudnya manajemen SPBE yang baik di BSSN - Meningkatnya kepercayaan stakeholder dalam beraktifitas di ruang siber secara aman	S+R Dengan adanya landasan hukum yang kuat bagi BSSN sebagai penyelenggara keamanan siber dan rata-rata latar belakang pendidikan pegawai di bidang IT, maka dapat mewujudkan manajemen SPBE yang baik di BSSN yang pada akhirnya dapat meningkatkan kepercayaan stakeholder dalam beraktifitas di ruang siber secara aman	O+R Dengan adanya dorongan dari Pimpinan BSSN untuk terus meningkatkan keamanan siber dan dukungan dari para pemangku kepentingan, maka dapat mewujudkan manajemen SPBE yang baik di BSSN yang pada akhirnya dapat meningkatkan kepercayaan stakeholder dalam beraktifitas di ruang siber secara aman

Berdasarkan analisis SOAR yang disajikan dalam tabel di atas, maka strategi yang dipilih adalah :

Dengan adanya landasan hukum yang kuat bagi BSSN sebagai penyelenggara keamanan siber dan rata-rata latar belakang pendidikan pegawai di bidang IT, serta dengan adanya dorongan dari Pimpinan BSSN untuk terus meningkatkan keamanan siber dan dukungan dari para pemangku kepentingan, maka dapat

membantu dalam menyusun kebijakan pimpinan berupa peraturan, SOP dan Juknis dalam penilaian risiko, lebih mudah dalam meningkatnya kompetensi / kemampuan pegawai khususnya tim penilai risiko keamanan serta mudah mendapatkan dukungan sarana prasana penilaian risiko yang memadai, sehingga dapat mewujudkan manajemen SPBE yang baik di BSSN, yang pada akhirnya dapat meningkatkan kepercayaan stakeholder dalam beraktifitas di ruang siber secara aman.

M. Ruang Lingkup Proyek Perubahan

Proyek Perubahan ini difokuskan pada penilaian risiko Keamanan Siber. Melalui penilaian tersebut dapat diketahui dimensi-dimensi strategis yang harus dianalisis, dievaluasi dan ditingkatkan guna meningkatkan kepercayaan masyarakat. Adapun ruang lingkup proyek perubahan ini meliputi:

1. Pembuatan Draft Peraturan Kepala Badan Siber dan Sandi Negara tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik.
2. Pembuatan Rancangan Standar Operasional Prosedur Penilaian Risiko (Risk Assesment).
3. Pembuatan Rancangan Petunjuk Teknis Risiko (Risk Assesment).
4. Pelatihan peningkatan kompetensi pegawai sebagai Tim Risk Assesment.

5. Sosialisasi Draft Peraturan Kepala Badan Siber dan Sandi Negara tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik.
6. Pemenuhan sarana prasarana pendukung kegiatan Tim Risk Assesment.

N. Perspektif Baru dalam Proyek Perubahan

Penilaian Risiko Keamanan Siber sebagai bagian dari upaya peningkatan kepercayaan kepada para pemangku kepentingan dalam beraktivitas di ruang Siber dalam mewujudkan manajemen Sistem Pemerintahan Berbasis Elektronik yang baik.

III. TUJUAN DAN MANFAAT

A. Tujuan

1. Tujuan Jangka Panjang

Terciptanya Sistem Pemerintahan Berbasis Elektronik yang baik yang dibuktikan dengan meningkatnya nilai indeks SPBE BSSN, sehingga akan meningkatkan reputasi BSSN serta meningkatkan kepercayaan pemangku kepentingan kepada BSSN.

2. Tujuan Jangka Menengah

Tujuan jangka menengah yang ingin dicapai dari pelaksanaan Proper ini adalah:

- a. Meningkatkan kemampuan anggota BSSN dalam penilaian risiko keamanan siber.

- b. Tersedianya sarana dan prasana pendukung kegiatan tim penilai risiko keamanan siber
- c. Terukurnya manajemen risiko keamanan siber di BSSN.

3. Tujuan Jangka Pendek

Tujuan jangka pendek yang ingin dicapai dari pelaksanaan Proper ini adalah:

- a. Penyelesaian Draft Peraturan Kepala Badan Siber dan Sandi tentang Manajemen Risiko Keamanan Sistem Pemerintahan Berbasis Elektronik.
- b. Terbentuknya Rancangan Standar Operasional Prosedur Penilaian Risiko (Risk Assesment).
- c. Terbentuknya Rancangan Petunjuk Teknis Penilaian Risiko (Risk Assesment).
- d. Terpenuhinya sebagian sarana prasana pendukung kegiatan Tim penilai risiko.
- e. Meningkatnya kompetensi dan kemampuan pegawai dalam melakukan penilaian risiko keamanan siber.
- 6) Tersosialisasikannya Draft Peraturan Kepala Badan Siber dan Sandi tentang Manajemen Risiko Keamanan Sistem Pemerintahan Berbasis Elektronik kepada pihak internal.

B. Manfaat

1. Manfaat bagi Pihak Internal

Manfaat pelaksanaan Proper ini bagi pihak internal adalah sebagai berikut:

- a. Memberikan panduan bagi tim penilai risiko dalam melakukan manajemen risiko keamanan siber;
- b. Meningkatkan kemampuan dan kompetensi pegawai khususnya dalam melakukan penilaian risiko keamanan siber

2. Manfaat bagi Pihak Eksternal

Manfaat pelaksanaan Proyek perubahan ini bagi pihak eksternal adalah sebagai berikut:

- a. Memberikan gambaran pentingnya menjaga keamanan siber di wilayah kerjanya sehingga menjadi budaya dalam aktivitas pekerjaan sehari-hari.
- b. Memberikan kepastian dan rasa aman dalam penggunaan sistem teknologi informasi dan komunikasi tiap tiap satuan kerja dari kemungkinan terjadinya ancaman serangan siber;

IV. OUTPUT DAN OUTCOME

A. Output

1. Jangka Pendek

- a. Draft Peraturan Kepala Badan Siber dan Sandi Negara tentang Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik.
- b. Rancangan kerangka Standar Operasional Prosedur Penilaian Risiko Keamanan (Risk Assesment).
- c. Rancangan kerangka Petunjuk Tekhnis Penilaian Risiko Keamanan (Risk Assesment).

- d. Hasil pelatihan peningkatan kemampuan terhadap pegawai tentang penilaian risiko keamanan.
- e. Hasil sosialisasi Draft Peraturan Kepala Badan Siber dan Sandi Negara tentang Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik.
- f. Ajuan penambahan sarana prasarana dasar bagi tim penilai risiko.

2. Jangka Menengah

- a. Hasil revisi harmonisasi draft Peraturan Kepala Badan Siber dan Sandi Negara tentang Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik.
- b. Dokumen pendaftaran draft peraturan pada kementerian hukum dan HAM.
- c. Standar Operasional Prosedur Penilaian Risiko Keamanan
- d. Petunjuk Tekhnis Penilaian Risiko Keamanan
- e. Ajuan Sarana dan Prasana pendukung kegiatan tim penilai risiko keamanan siber (lanjutan).
- f. Ajuan Pelatihan peningkatan kemampuan pegawai dalam penilaian risiko tahap 2.

3. Jangka Panjang

- a. Penerbitan Peraturan Kepala Badan Siber dan Sandi Negara tentang Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik.
- b. Hasil sosialisasi dan implementasi ke pihak eksternal.
- c. Penambahan sarana prasarana tim penilai (lanjutan).

B. Outcome

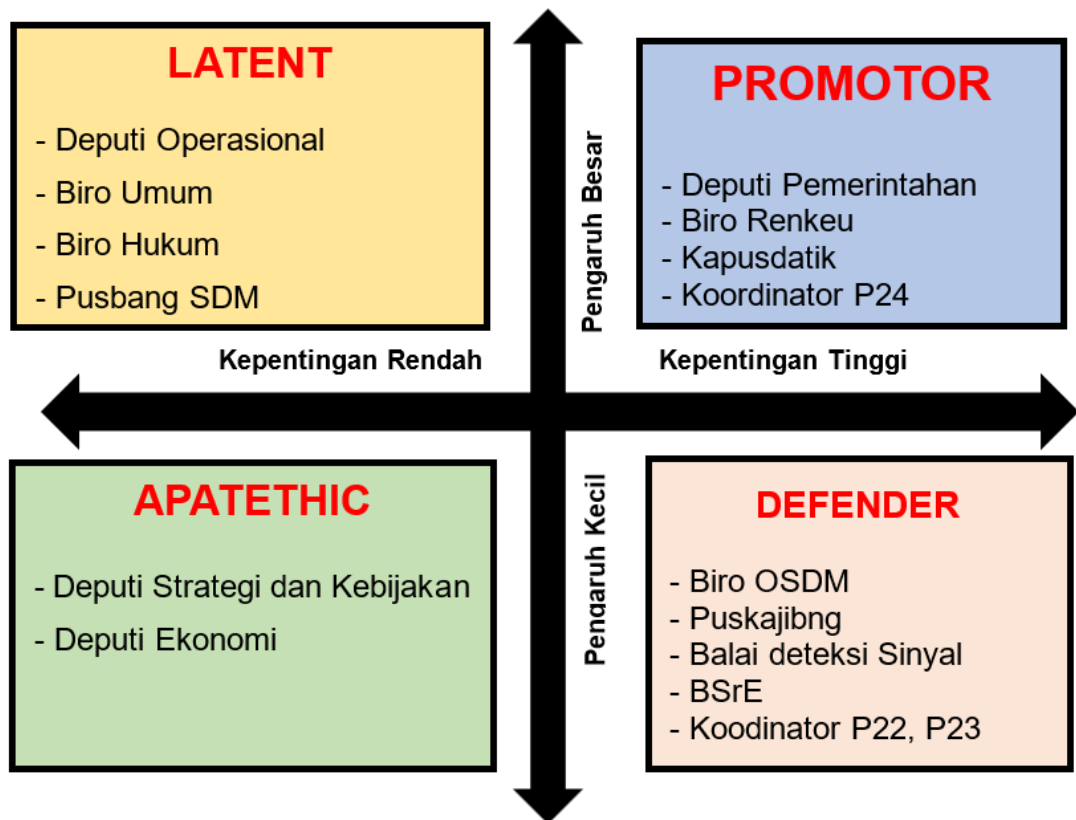
Peraturan Kepala Badan Siber dan Sandi tentang Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik dibuat untuk dijadikan sebagai pedoman dalam manajemen risiko keamanan siber yang dilakukan secara terus menerus dan berkesinambungan, sehingga dapat menjadi langkah strategis untuk meningkatkan kepercayaan kepada para pemangku kepentingan dalam beraktivitas dan bertransaksi di ruang Siber dalam rangka mewujudkan manajemen Sistem Pemerintahan Berbasis elektronik yang baik.

V. IDENTIFIKASI STAKEHOLDER

Stakeholder adalah semua pihak baik yang berada di dalam maupun di luar organisasi, termasuk individu atau kelompok yang memiliki legitimasi, kekuasaan, dan kepentingan dalam suatu organisasi.

Stakeholder dapat dikelompokkan ke dalam: (1) Stakeholder utama merupakan stakeholder yang memiliki kaitan kepentingan secara langsung dengan suatu kebijakan, program, dan proyek. Mereka harus ditempatkan sebagai penentu utama dalam proses pengambilan keputusan; (2) Stakeholder pendukung (sekunder) adalah stakeholder yang tidak memiliki kaitan kepentingan secara langsung terhadap suatu kebijakan, program, dan proyek, tetapi memiliki kepedulian (concern) sehingga mereka turut berpengaruh terhadap sikap masyarakat; dan (3) Stakeholder kunci merupakan stakeholder yang memiliki kewenangan secara legal dalam hal pengambilan keputusan.

Gambar 2. Pemetaan Stakeholder



Dalam Proyek Perubahan ini stakeholder dikelompokkan berdasarkan pengaruh/kekuasaan dan kepentingan yang dimilikinya, yaitu:

1. Promotor, yaitu stakeholder yang memiliki kepentingan tinggi dan pengaruh besar/tinggi terhadap Proyek Perubahan. Stakeholder yang termasuk ke dalam kategori Promoter meliputi:

- Promotor 1 : Deputi Pemerintahan.
- Promotor 2 : Biro Renkeu.
- Promotor 3 : Kapusdatik.
- Promotor 4 : Koordinator risiko dan kerentanan

Strategi komunikasi yang akan dibangun adalah koordinasi, konsultasi, diskusi dan sosialisasi.

2. Defender, yaitu stakeholder yang memiliki kepentingan tinggi dan pengaruh kecil/rendah terhadap Proyek Perubahan. Stakeholder yang termasuk ke dalam kategori Defender meliputi:

- Defender 1: Biro OSDM.
- Defender 2: Puskajibang.
- Defender 3: Balai Deteksi Sinyal.
- Defender 4: Balai Sertifikasi Elektronik
- Defender 5: Koordinator Sistem Aplikasi dan Lisensi
- Defender 6: Koordinator Infrastruktur dan jaringan

Strategi komunikasi yang akan dibangun adalah koordinasi dan sosialisasi.

3. Latent, yaitu stakeholder yang memiliki kepentingan kecil/rendah dan pengaruh besar/tinggi terhadap Proyek Perubahan. Stakeholder yang termasuk ke dalam kategori Latent meliputi:

- Latent 1: Deputi Operasional Keamanan Siber dan Sandi.
- Latent 2: Biro Hukum dan Komunikasi Publik
- Latent 3: Biro OSDM.
- Latent 4: Pusbang SDM.

Strategi komunikasi yang akan dibangun adalah koordinasi, diskusi dan sosialisasi.

4. Apatethis, yaitu stakeholder yang memiliki kepentingan kecil/rendah dan pengaruh kecil/rendah terhadap Proyek Perubahan. Stakeholder yang termasuk ke dalam kategori Latent meliputi:

- Apatethis 1: Deputi Strategi dan Kebijakan.
- Apatethis 2: Deputi Ekonomi.

Strategi komunikasi yang akan dibangun adalah sosialisasi berupa informasi, persuasif, publikatif, promosi dan komitmen.

VI. POTENSI RISIKO DAN RENCANA MITIGASI

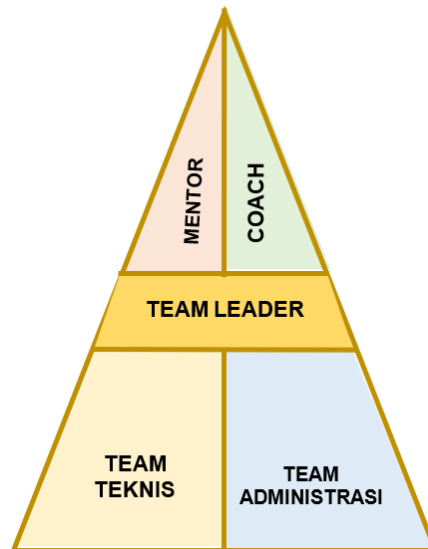
Tabel 9
Potensi Risiko dan Rencana Mitigasi

No.	POTENSI RISIKO	RENCANA MITIGASI
1.	Internal: - Pergantian Pimpinan; - Mutasi pegawai efektif. - Ego sektoral antar bagian atau kelompok fungsi	Internal: - Menerapkan Manajemen Pengetahuan sebagai kontrol pergantian pimpinan atau mutasi pegawai efektif yang terjadi - Sosialisasi atau penyampaian mengenai manfaat dan tujuan dari manajemen risiko untuk mengurai ego sektoral antar fungsi;
2.	Eksternal: - Pemahaman terkait manajemen Risiko SPBE yang tidak merata - Ego Sektoral antar unit kerja	Eksternal: - Sosialisasi kebijakan manajemen risiko, SOP dan petunjuk teknis kepada seluruh pemangku kepentingan - Sosialisasi atau penyampaian mengenai manfaat dan tujuan dari manajemen risiko untuk mengurai ego sektoral unit kerja

VII. ORGANISASI TIM EFEKTIF

Dalam proyek perubahan ini mencoba menyajikan organisasi proyek perubahan yang agile, dimana terdiri dari mentor, coach, project leader, tim efektif sebagai berikut:

Gambar 3. Tim Efektif



Deskripsi dari masing-masing komponen Tim Efektif sebagaimana tersebut dalam Tabel 7 di bawah ini :

Tabel 10

Tata Kelola Proyek Perubahan

No.	Kedudukan	Nama	Peranan
1.	Mentor	Brigjen TNI Ferdinand Mahulette, SE Kapusdatik BSSN	1. Memberikan persetujuan Proposal Proyek Perubahan. 2. Memberikan bimbingan, arahan dalam merumuskan dan mengimplementasikan Proyek Perubahan. 3. Memberikan bimbingan mengatasi kendala, selama berlangsungnya proses implementasi Proyek Perubahan.

			4. Memantau perkembangan pelaksanaan Proyek Perubahan dengan meminta progress report.
2.	Coach	Buridan Ali Junjuran, SH, MSi Widya Iswara Lembaga Administrasi Negara	1. Memantau kegiatan peserta selama pelaksanaan Proyek Perubahan. 2. Melakukan koordinasi dengan mentor, membantu peserta apabila mengalami permasalahan selama pelaksanaan Proyek Perubahan. 3. Memberikan masukan kepada peserta terkait usulan proyek perubahan yang dirumuskan pada agenda aktualisasi kepemimpinan. 4. Memberikan feedback, laporan perkembangan implementasi proyek perubahan yang disampaikan peserta bimbingan minimal seminggu sekali. 5. Menjadi counsellor saat peserta kesulitan.
3.	Project Leader	Rakhmat Damdami, SAP, MSi Kabagum Pusdatik BSSN	1. Merencanakan Proyek Perubahan serta berkonsultasi dengan Mentor dan Coach. 2. Melaksanakan, mengendalikan Proyek Perubahan. 3. Mengkoordinasikan stakeholder terkait. 4. Memberikan motivasi kepada Tim. 5. Membuat Rencana Proyek Perubahan dan Laporan Proyek Perubahan.
4.	Wakil Project Leader	Adi Nugroho, S.ST, S.Kom	1. Menyusun rencana kerja Proyek Perubahan. 2. Menyusun jadwal pelaksanaan Proyek Perubahan.

			3. Mengendalikan kegiatan Proyek Perubahan. 4. Mengendalikan Tim Pengawasan, monitoring dan evaluasi (monev) dan team pengelolah pengaduan. 5. Mengidentifikasi, mempersiapkan kebutuhan perlengkapan Proyek Perubahan. 6. Melakukan koordinasi stakeholder terkait. 7. Melaksanakan tugas tambahan yang diarahkan oleh Project Leader.
5.	Tim Teknis	1. James Leonardo, S.ST 2. Noor Hafidz S.ST 3. Agung Widodo, SE 4. Muhammad Dwison Alizah, S.Tr.Tp 5. Agung Nursilo S.ST, MT 6. Thoriq Rahmat Hidayat, S.Tr.Tp 7. Fitri Ariani, S.Sos 8. Anis Nurul Hanifah, A.Md	1. Menyelenggarakan rapat/diskusi Proyek Perubahan. 2. Mempersiapkan bahan rapat/diskusi Proyek Perubahan. 3. Membuat laporan hasil rapat Proyek Perubahan. 4. Mendokumentasikan kegiatan Proyek Perubahan. 5. Menangani surat masuk dan surat keluar. 6. Membuat laporan dan evaluasi progres Proyek Perubahan. 7. Melaksanakan tugas-tugas tambahan yang diarahkan oleh Project Leader. 8. Menyusun laporan-laporan terkait pelaksanaan Proyek Perubahan.
6.	Tim Administrasi	1. Muhammad 2. Cut Ageng Sulistyowati, S.Kom 3. Suri Suryani	1. Mendokumentasikan seluruh kegiatan Proyek Perubahan. 2. Menyiapkan bahan sosialisasi.

VIII. ANGGARAN

Proses pembuatan proyek perubahan ini tidak menggunakan anggaran DIPA BSSN, akan tetapi sepenuhnya menggunakan dana pribadi dari peserta PKN, karena kegiatan diklat PKN ini tidak masuk dalam DIPA rutin untuk pembuatan proyek perubahan. Namun demikian untuk keberlanjutan dari implementasi proyek perubahan seperti pengadaan peralatan bagi tim penilai risiko akan diusulkan menggunakan DIPA BSSN pada tahun anggaran berikutnya.

BAB II

IMPLEMENTASI PROYEK PERUBAHAN

I. CAPAIAN TAHAPAN RENCANA STRATEGIS

Sebagai implementasi dari Rencana Proyek Perubahan, telah dilakukan langkah-langkah strategis sesuai dengan rencana proyek perubahan yang telah disusun sebelumnya. Pada dasarnya rencana proyek perubahan telah dicapai berdasarkan hasil capaian milestone kegiatan dan outputnya pada Tahapan jangka pendek. Beberapa hal yang telah dicapai utamanya pencapaian jangka pendek antara lain tahapan sebagai berikut :

1. Permohonan ijin dan dukungan kepada Pimpinan.

Pada hari Senin tanggal 12 September 2022 siswa PKN II atas nama AKBP Rakhmat Damdami menghadap Wakil Kepala Badan Siber dan Sandi Negara (Waka BSSN) Komisaris Jenderal Polisi Drs. Luki Hermawan, Msi, menyampaikan maksud dan tujuan terkait penugasan peserta PKN II dalam pembuatan Proyek Perubahan yang berjudul “Optimalisasi Pusdatik Dalam Melakukan Manajemen Risiko Sistem Pemerintah Berbasis Elektronik di Lingkungan Badan Siber dan Sandi Negara”.

Mendengar maksud dan tujuan tersebut, Waka BSSN memberikan arahan dan dukungannya sebagai berikut :

Bahwa seperti kita ketahui bahwa akhir akhir ini banyak terjadi kasus kasus serangan siber ataupun kebocoran data. Hal ini sangat

berbahaya bagi keamanan negara maupun data pribadi setiap warga negara yang dapat disalahgunakan oleh oknum oknum yang tidak bertanggung jawab, baik untuk kepentingan pribadi dengan tujuan mendapatkan sejumlah imbalan materi ataupun dengan tujuan untuk mengacaukan stabilitas negara yang dapat dilakukan oleh state actor baik dari dalam maupun luar negeri.

Oleh karena itu perlindungan terhadap sistem elektronik suatu institusi termasuk BSSN adalah sangat penting, dengan cara melakukan manajemen risiko sistem pemerintahan berbasis elektronik. Dengan demikian dapat diketahui dengan segera kerentanan atau kerawanan pada sistem elektronik tersebut, dan dapat segera dilakukan perbaikan ataupun penguatan.

Pada kesempatan ini Waka BSSN berharap agar proyek perubahan ini dapat segera diterapkan dan memberikan dampak yang positif bagi organisasi BSSN ke depannya.

Sebagai bentuk dukungan, Waka BSSN memberikan akses seluas luasnya semua sumber daya yang ada ke setiap unit kerja dalam rangka pengumpulan data.



Selanjutnya pada hari dan tanggal yang sama 12 September 2022 siswa PKN II atas nama AKBP Rakhmat Damdami menghadap Kepala Pusat Data dan Teknologi Informasi Komunikasi (Kapusdatik), Brigadir Jenderal TNI Ferdinand Mahulette, SE, sekaligus bertindak sebagai mentor Siswa PKN, menyampaikan maksud dan tujuan terkait penugasan peserta PKN II dalam pembuatan Proyek Perubahan, dimana dalam salah tahap awal pelaksanaannya adalah dengan pembentukan tim efektif.

Kapusdatik sangat memberikan dukungan dalam pembuatan proyek perubahan ini, karena Sejak terbentuknya BSSN tahun 2017, efektif beroperasi pertengahan 2018 dan pernah mengalami reorganisasi tahun 2021, masih banyak kekurangan alat kelengkapan organisasi termasuk di dalamnya adalah peraturan peraturan. Ini sangat mempengaruhi tugas pokok di BSSN, khususnya kami di Pusdatik, tidak dapat melaksanakan salah satu fungsi yang ada di kami yaitu manajemen risiko sebagai suatu upaya untuk mencegah terjadinya upaya serangan siber ataupun kebocoran data.

Tidak adanya peraturan ini juga menyebabkan kami kesulitan untuk mencapai nilai indeks nilai SPBE BSSN yang telah menjadi target yang telah ditentukan. Oleh karena itu dengan langkah optimalisasi Pusdatik melalui pembuatan peraturan ini diharapkan juga dapat mengangkat indeks SPBE BSSN yang setiap tahun dilakukan evaluasi oleh Kemenpan RB.

Dalam proyek perubahan ini Kapusdatik menyarankan tidak hanya terbatas pada pembuatan Peraturan Kepala saja namun juga SOP dan petunjuk Teknis untuk pelaksanaannya, sehingga Ketika Peraturan tersebut disahkan, pegawai yang masuk dalam Tim Penilai dapat segera melaksanakan tugasnya karena sudah dilengkapi dengan peraturan, SOP dan Petunjuk Teknis. Tentu sebelumnya mereka juga dibekali terlebih dahulu dengan pelatihan untuk peningkatan kemampuan dan juga dukungan sarana prasana terkait.

Terakhir, Kapusdatik berharap proyek perubahan ini dapat segera diterapkan dan saya dukung untuk keberlanjutannya ke depan dalam mensukseskan visi dan misi BSSN.

Terkait dengan pembentukan Tim Efektif, arahan dari Kapusdatik adalah agar dilaksanakan rapat dengan staf Pusdatik untuk dapat disampaikan maksud dan tujuan tersebut kepada pegawai yang akan dilibatkan dalam pembuatan proyek perubahan tersebut.



2. Pembentukan Tim Efektif.

Pada tanggal 13 September 2022, dilaksanakan rapat di lingkungan Pusdatik BSSN yang dipimpin langsung oleh Bapak Kapusdatik. Rapat awal ini diadakan dalam rangka mendukung tugas pembuatan implementasi Proyek Perubahan dari peserta PKN II Angkatan XVIII tahun 2022 atas nama AKBP Rakhmat Damdami NRP. 74050727, dengan judul Proyek Perubahan adalah “Optimalisasi Pusdatik Dalam Melakukan Manajemen Risiko Sistem Pemerintah Berbasis Elektronik di Lingkungan Badan Siber dan Sandi Negara”. Pada rapat dijelaskan tentang rencana pembentukan Tim Efektif dan tugas dari masing-masing pegawai yang ditunjuk dalam Tim Efektif.

Tujuan kegiatan ini adalah untuk membantu peserta PKN dalam mengimplementasikan proyek perubahan. Kegiatan ini dapat dilaksanakan dengan lancar tanpa adanya kendala dan kesulitan, dan 100% tujuan kegiatan. Hasil kegiatan berupa pembagian tugas dalam rangka mendukung implementasi proyek perubahan terkait pelaksanaan proyek perubahan.

Susunan Tim Efektif dan peranannya sebagai berikut :

1. Project Leader, yaitu Rakhmat Damdami, SAP, MSi, dengan tugas :
 - Merencanakan Proyek Perubahan serta berkonsultasi dengan Mentor dan Coach.
 - Melaksanakan, mengendalikan Proyek Perubahan.
 - Mengkoordinasikan stakeholder terkait.

- Memberikan motivasi kepada Tim.
 - Membuat Rencana Proyek Perubahan dan Laporan Proyek Perubahan.
2. Wakil Project Leader, yaitu Adi Nugroho, S.ST, S.Kom, dengan tugas :
- Menyusun rencana kerja Proyek Perubahan.
 - Menyusun jadwal pelaksanaan Proyek Perubahan.
 - Mengendalikan kegiatan Proyek Perubahan.
 - Mengendalikan Tim Pengawasan, monitoring dan evaluasi (monev) dan team pengelolah pengaduan.
 - Mengidentifikasi, mempersiapkan kebutuhan perlengkapan Proyek Perubahan.
 - Melakukan koordinasi stakeholder terkait.
 - Melaksanakan tugas tambahan yang diarahkan oleh Project Leader.
3. Tim Teknis, terdiri dari :
- James Leonardo, S.ST
 - Noor Hafidz S.ST
 - Agung Widodo, SE
 - Muhammad Dwison Alizah, S.Tr.Tp
 - Agung Nursilo S.ST, MT
 - Thoriq Rahmat Hidayat, S.Tr.Tp
 - Fitri Arian, S.Sos
 - Anis Nurul Hanifah, A.Md
- Dengan tugas

- Menyelenggarakan rapat/diskusi Proyek Perubahan.
- Mempersiapkan bahan rapat/diskusi Proyek Perubahan.
- Membuat laporan hasil rapat Proyek Perubahan.
- Mendokumentasikan kegiatan Proyek Perubahan.
- Menangani surat masuk dan surat keluar.
- Membuat laporan dan evaluasi progres Proyek Perubahan.
- Melaksanakan tugas-tugas tambahan yang diarahkan oleh Project Leader.
- Menyusun laporan-laporan terkait pelaksanaan Proyek Perubahan.

4. Tim Administrasi, terdiri dari :

- 1. Muhammad
- 2. Cut Ageng Sulistyowati, S.Kom
- 3. Suri Suryani

Dengan tugas :

- Mendokumentasikan seluruh kegiatan Proyek Perubahan.
- Menyiapkan bahan sosialisasi.



Pada tanggal 14 September 2022, telah diterbitkan Surat Perintah Tim Efektif yang di tanda-tangani oleh Bapak Kapusdatik, dalam rangka mendukung tugas pembuatan implementasi Proyek Perubahan dari peserta PKN II Angkatan XVIII tahun 2022 atas nama AKBP Rakhmat Damdami NRP. 74050727, dengan judul Proyekk Perubahan adalah “Optimalisasi Pusdatik Dalam Melakukan Manajemen Risiko Sistem Pemerintah Berbasis Elektronik di Lingkungan Badan Siber dan Sandi Negara”.



BADAN SIBER DAN SANDI NEGARA
Jalan Raya Muchtar No.70, Kel. Duren Mekar, Kec. Bojongsari, Depok 16518
Telepon (021) 77973360, Faksimile (021) 78844104, (021) 77973579
Website : <https://bssn.go.id>, E-mail : bssn@bssn.go.id

SURAT PERINTAH
NOMOR : 23/P2KP.07.01/09/2022

Menimbang : bahwa dalam rangka mendukung pelaksanaan kegiatan Pelatihan Kepemimpinan Nasional (PKN) Tingkat II angkatan XVIII tahun 2022, dipandang perlu mengeluarkan surat perintah bagi Pegawai Badan Siber dan Sandi Negara;

Dasar : 1. Surat Perintah Kaproli Nomor : Sprin/1718/VII/DIK.2.5/2022 tanggal 15 Juli 2022 perihal Perintah mengikuti Pelatihan Kepemimpinan Nasional Tingkat II Angkatan XVIII tahun 2022 di Pusdikmin Lemdiklat Polri;
2. Surat Kaproli Nomor : B/5806/VII/DIK.2.5/2022/SSDM tanggal 15 Juli 2022 perihal Penghadapan Peserta Pelatihan Kepemimpinan Nasional Tingkat II Angkatan XVIII tahun 2022;
3. Program Kerja Kepala Pusat Data dan Teknologi Komunikasi Informasi Tahun Anggaran 2022.

Memberi Perintah

Kepada : Pegawai Negeri Sipil Badan Siber dan Sandi Negara yang nama namanya tersebut dalam lajur dua lampiran Surat Perintah ini.

Untuk : 1. Di samping melaksanakan tugas dan jabatan sehari-hari, ditunjuk sebagai tim efektif untuk mendukung pembuatan Proyek Perubahan PKN Tingkat II angkatan XVIII tahun 2022 a.n. AKBP Rakhmat Damdami S.A.P. M.Si., NRP 74050727 selaku Kepala Bagian Umum, Pusat Data dan TIK BSSN terkait pelaksanaan proyek perubahan dengan judul “Optimalisasi Pusdatik Dalam Melakukan Manajemen Risiko Sistem Pemerintah Berbasis Elektronik di Lingkungan Badan Siber dan Sandi Negara”;
2. Melaksanakan perintah ini dengan sebaik-baiknya dan penuh tanggung jawab;
3. Membuat laporan setelah melaksanakan kegiatan dimaksud.

Depok, 14 September 2022

Kepala Pusat Data dan Teknologi Informasi Komunikasi



Tembusan :

1. Kepala Badan Siber dan Sandi Negara;
2. Wakil Kepala BSSN;
3. Plt. Sekretaris Utama;
4. Inspektur;
5. Kepala Biro Perencanaan dan Keuangan;
6. Plt. Kepala Biro Organisasi dan Sumber Daya Manusia.

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Badan Sertifikasi Elektronik (BSE-E), Badan Siber dan Sandi Negara

BADAN SIBER DAN SANDI NEGARA

LAMPIRAN SURAT PERINTAH
NOMOR : 23/P2KP.07.01/09/2022
TANGGAL : 14 September 2022

DAFTAR NAMA TIM EFEKTIF DALAM Mendukung Pembuatan Proyek Perubahan PKN TINGKAT II Angkatan XVIII Tahun 2022

NO	NAMA	NIP/NRP	PANGKAT/GOL. RUANG	JABATAN	JABATAN DALAM TIM PROYEK PERUBAHAN
1	Rakhmat Damdami, M.Si.	74050727	Ajun Komisaris Besar Polisi	Kepala Bagian Umum, Pusat Data dan TIK	Project Leader
2	Adi Nugroho, S.ST., S.Kom	19841229 200312 1 007	Penata (IIIC)	Sandiman Madja	Wakil Project Leader
3	James Leonardo, S.ST.	19840114 200312 1 005	Penata Tk. I (IIB)	Penata Hubungan Masyarakat Muda	
5	Noor Hafidz, S.ST.	19840709 200501 1 001	Penata Tk. I (IIB)	Penata Komputer Muda	
6	Agung Witoko, S.E.	19820604 200212 1 003	Penata (IIC)	Manggota Informatika Ahli Muda	
7	Muhammad Dwison Alisah, S.Tr.TP	19850115 201611 1 001	Penata Muda (IIB)	Penata Komputer Pertama	
8	Agung Nurullo, S.S.T., M.T.	19870705 200701 1 002	Penata (IIC)	Penata Komputer Muda	Tim Teknis
9	Thoriq Rakhmat Hidayat, S.Tr.TP	19840913 201712 1 001	Penata Muda (IIB)	Manggota Informatika Ahli Pertama	
10	Fah Anan, S.Sos.	19760624 200212 2 002	Penata Muda (IIB)	Pengelola BAH	
11	Aria Nurul Hudaib, A.Md.	19960226 201902 2 001	Pengantar (IIC)	Penata Komputer Pelaksana	Tim Administrasi
12	Muhammad	19760512 199812 1 001	Penata Muda Tk. I (IIB)	Sandiman Pelaksanaan Lanjutan	
13	Cid Ageng Sukhtyewati, S.Kom.	19871208 2021 2405	PPNPN	Asisten Pengelola Data Perkantoran	
14	Suri Suryati	19910426 2019 2267	PPNPN	Asisten Pengelola Data Perkantoran	

Kepala Pusat Data dan Teknologi Informasi Komunikasi



Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Badan Sertifikasi Elektronik (BSE-E), Badan Siber dan Sandi Negara

2. Pengajuan Sarana Prasarana Pendukung

Pada tanggal 19 September 2022, dibuat nota dinas pengajuan peralatan sarana prasarana dalam rangka mendukung kegiatan manajemen penilaian risiko yang dibuat oleh Kepala Bagian Umum (Kabagum) Pusdatik kepada Kapusdatik dan nota dinas pengajuan dari Kapusdatik kepada Kepala Biro Umum (Karoum) BSSN.

BADAN SIBER DAN SANDI NEGARA
NOTA DINAS
NOMOR : 507/P2/KP.07.01/05/2022

Yth : Kepala Pusat Data dan Teknologi Informasi Komunikasi
Dari : Kepala Bagian Umum Pusdatik
Hal : Permohonan Fasilitas Sarana Prasarana Pendukung Kegiatan Manajemen Penilaian Risiko SPBE
Lampiran : 1 (satu) berkas
Tanggal : 19 September 2022

1. Dasar:

a. Surat Perintah Kapri Nomor Sprin/1718/VII/DIK.2.5/2022 tanggal 15 Juli 2022 perihal Perintah mengikuti Pelatihan Kepemimpinan Nasional Tingkat II Angkatan XVIII tahun 2022 di Pusdikmin Lemdiklat Polri;

b. Surat Kapri Nomor B/5806/VII/DIK.2.5/2022/SSDM tanggal 15 Juli 2022 perihal Penghadapan Peserta Pelatihan Kepemimpinan Nasional Tingkat II Angkatan XVIII tahun 2022;

c. Surat Perintah Nomor 23/P2/KP.07.01/09/2022 tanggal 14 September 2022 tentang Tim efektif untuk mendukung pembuatan Proyek Perubahan PKN Tingkat II angkatan XVIII tahun 2022 a.n. AKBP Rahmat Dandami S.A.P. M.Si., NRP 74050727 selaku Kepala Bagian Umum, Pusat Data dan TIK BSSN terkait pelaksanaan proyek perubahan dengan judul "Optimalisasi Pusdatik Dalam Melakukan Manajemen Risiko Sistem Pemerintah Berbasis Elektronik di Lingkungan Badan Siber dan Sandi Negara.

2. Merujuk dasar tersebut diatas, bersama ini dengan hormat disampaikan permohonan Fasilitas Sarana Prasarana Pendukung Kegiatan Manajemen Penilaian Risiko SPBE.

3. Demikian disampaikan, atas perhatian dan perkenan Bapak diucapkan terima kasih.



Tembusan :

1. Kepala Badan Siber dan Sandi Negara;

2. Wakil Kepala Badan Siber dan Sandi Negara;

3. Pjt. Sekretaris Utama;

4. Inspektorat.

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE) Badan Siber dan Sandi Negara

3. Pembuatan Draft Peraturan Kepala Badan Siber dan Sandi Negara tentang Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik.

Pada tanggal 19 September 2022, dibuat surat undangan kepada Tim Efektif dalam rangka rapat pembahasan penyusunan draft Peraturan Kepala Badan Siber dan Sandi Negara tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik di lingkungan Badan Siber dan Sandi Negara.

BADAN SIBER DAN SANDI NEGARA

Nomor : 506/P2/KH.01.02/09/2022
Sifat : Biasa
Lampiran : Satu Berkas
Hal : Undangan Penyusunan Peraturan tentang Pedoman Manajemen Risiko

Depok, 19 September 2022

Yth. Daftar Undangan Terlampir di -
Tempat

1. Dasar:

a. Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara;

b. Surat Perintah Kapri Nomor Sprin/1718/VII/DIK.2.5/2022 tanggal 15 Juli 2022 perihal Perintah mengikuti Pelatihan Kepemimpinan Nasional Tingkat II Angkatan XVIII tahun 2022 di Pusdikmin Lemdiklat Polri;

c. Surat Kapri Nomor B/5806/VII/DIK.2.5/2022/SSDM tanggal 15 Juli 2022 perihal Penghadapan Peserta Pelatihan Kepemimpinan Nasional Tingkat II Angkatan XVIII tahun 2022;

d. Surat Perintah Nomor 23/P2/KP.07.01/09/2022 tanggal 14 September 2022 tentang Tim efektif untuk mendukung pembuatan Proyek Perubahan PKN Tingkat II angkatan XVIII tahun 2022 a.n. AKBP Rahmat Dandami S.A.P. M.Si., NRP 74050727 selaku Kepala Bagian Umum, Pusat Data dan TIK BSSN terkait pelaksanaan proyek perubahan dengan judul "Optimalisasi Pusdatik Dalam Melakukan Manajemen Risiko Sistem Pemerintah Berbasis Elektronik di Lingkungan Badan Siber dan Sandi Negara.

2. Merujuk dasar tersebut diatas, bersama ini kami mengundang Bapak/Ibu untuk hadir dalam Penyusunan Peraturan tentang Pedoman Manajemen Risiko yang dilaksanakan pada:

Hari/Tanggal : Rabu, 21 September 2022
Waktu : 09.30 s.d. selesai
Tempat : Ruang Rapat Pusdatik Lt. 6, Gedung D4, Kantor Sawangan

3. Demikian disampaikan, atas perhatiannya dan kerjanya samanya diucapkan terima kasih.



Tembusan :

1. Kepala Badan Siber dan Sandi Negara;

2. Wakil Kepala Badan Siber dan Sandi Negara;

3. Pjt. Sekretaris Utama;

4. Inspektorat.

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE) Badan Siber dan Sandi Negara

Lampiran 1 Surat Undangan
Nomor : 506/P2/KH.01.02/09/2022
Tanggal : 19 September 2022

DAFTAR UNDANGAN

1. Rahmat Dandami S.A.P. M.Si., selaku Kepala Bagian Umum Pusdatik;
2. James Leonardo, S.ST., selaku Koordinator Fungsi Pengembangan Sistem Dan Pengujian Data Pusdatik;
3. Noor Hafidz, S.ST., selaku Koordinator Fungsi Operasi Dan Layanan TIK;
4. Adi Nugroho, S.ST., S.Kom selaku Koordinator Fungsi Manajemen Risiko Dan Kelengkapan TIK;
5. Agung Nurrozi, S.ST., M.T., selaku Subkoordinator Manajemen Sistem Informasi dan Teknologi, Kelompok/Fungsi Pengembangan Sistem dan Pengolahan Data, Pusdatik;
6. Muhammad Dwison Alzahr, S.Tr.PP, selaku Subkoordinator Tatakelola dan Kepatuhan Keamanan Sistem Informasi dan TIK, Kelompok/Fungsi Manajemen Risiko dan Kelengkapan TIK;
7. Agung Widada, S.E., selaku Subkoordinator Operasional dan Pemngaman Pensaadran, Kelompok/Fungsi Manajemen Risiko dan Kelengkapan TIK;
8. Thoriq Rahmat Hidayat, S.Tr.PP, selaku Manggala Informaka Ahli Pertama, Kelompok/Fungsi Manajemen Risiko dan Kelengkapan TIK;
9. Anis Nasir Vindah, A.Mi., selaku Pranata Komputer Pelaksana, Kelompok/Fungsi Operasi dan Layanan TIK;
10. Muhammad, Sandiman Pelaksana Lanjutan, Kelompok/Fungsi Bagian Umum Pusdatik;
11. Fitri Ariani, S.Sos., Pengelola BMN, Kelompok/Fungsi Bagian Umum Pusdatik;
12. Cut Ageng Sulhiyowati S.Kom., Asisten Pengelola Data Perkantoran, Kelompok/Fungsi Bagian Umum Pusdatik;
13. Suri Suryani, Asisten Pengelola Data Perkantoran, Kelompok/Fungsi Bagian Umum Pusdatik.

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE) Badan Siber dan Sandi Negara

Pada hari Rabu tanggal 21 September 2022, dilaksanakan rapat Tim Efektif untuk melakukan pembahasan penyusunan draft Peraturan Kepada Badan Siber dan Sandi Negara tentang Pedoman Manajemen Risiko Sistim Pemerintahan Berbasis Elektronik di lingkungan Badan Siber dan Sandi Negara, yang dipimpin oleh Project Leader Perubahan yaitu AKBP Rakhmat Damdami.



Pada hari Kamis tanggal 6 Oktober 2022, dilaksanakan rapat Tim Efektif untuk melakukan finalisasi pembahasan penyusunan draft Peraturan Kepada Badan Siber dan Sandi Negara tentang Pedoman Manajemen Risiko Sistim Pemerintahan Berbasis Elektronik di lingkungan Badan Siber dan Sandi Negara, yang

dipimpin oleh Project Leader Perubahan yaitu AKBP Rakhmat Damdami.

BADAN SIBER DAN SANDI NEGARA

Nomor : 575/P2/KH.01.02/10/2022
Sifat : Biasa
Lampiran : Satu Berkas
Hal : Undangan Finalisasi Penyusunan Draft Peraturan
Kepada Badan Siber dan Sandi Negara

Depok, 3 Oktober 2022

Lampiran I Surat Undangan
Nomor : 575/P2/KH.01.02/10/2022
Tanggal : 3 Oktober 2022

DAFTAR UNDANGAN

Yth. Daftar Undangan Terlampir
di –
Tempat

1. Dasar :
 - a. Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara;
 - b. Surat Perintah Kapoli Nomor Sprin/1718/VI/DIK.2.5/2022 tanggal 15 Juli 2022 perihal Perintah mengikuti Pelatihan Kepemimpinan Nasional Tingkat II Angkatan XVIII tahun 2022 di Pusdikmin Lemdiklat Polri;
 - c. Surat Kapoli Nomor B/S806/VI/DIK.2.5/2022/SSDM tanggal 15 Juli 2022 perihal Penghadapan Peserta Pelatihan Kepemimpinan Nasional Tingkat II Angkatan XVIII tahun 2022;
 - d. Surat Perintah Nomor 23/P2/KP.07.01/09/2022 tanggal 14 September 2022 tentang Tim efektif untuk mendukung pembuatan Proyek Perubahan PKN Tingkat II angkatan XVIII tahun 2022 a.n. AKBP Rakhmat Damdami S.A.P. M.Si., NRP 74050727 selaku Kepala Bagian Umum, Pusat Data dan TIK BSSN terkait pelaksanaan proyek perubahan dengan judul "Optimalisasi Pusdatik Dalam Melakukan Manajemen Risiko Sistem Pemerintah Berbasis Elektronik di Lingkungan Badan Siber dan Sandi Negara.
2. Merujuk dasar tersebut diatas, bersama ini kami mengundang Bapak/Ibu untuk hadir dalam Undangan Melakukan Finalisasi Penyusunan Draft Peraturan Kepada Badan Siber dan Sandi Negara tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik di Lingkungan Badan Siber dan Sandi Negara, yang dilaksanakan pada:
Hari/Tanggal : Kamis, 6 Oktober 2022
Waktu : 09.00 s.d. selesai
Tempat : Ruang Rapat Pusdatik Lt. 6, Gedung D4, Kantor BSSN Sawangan
3. Demikian disampaikan, atas perhatiannya dan kerja samanya diucapkan terima kasih.



Terbuan :

1. Kepala Badan Siber dan Sandi Negara;
2. Wakil Kepala Badan Siber dan Sandi Negara;
3. Plt. Sekretaris Utama;
4. Inspektorat.

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE) Badan Siber dan Sandi Negara

1. Rakhmat Damdami S.A.P. M.Si., selaku Kepala Bagian Umum Pusdatik;
2. James Leonardo, S.ST., selaku Koordinator Fungsi Pengembangan Sistem Dan Pengolahan Data, Pusdatik;
3. Noor Hafidz, S.ST., selaku Koordinator Fungsi Operasi Dan Layanan TIK;
4. Adi Nugroho, S.ST., S.Kom selaku Koordinator Fungsi Manajemen Risiko Dan Kelangsungan TIK;
5. Agung Nursilo, S.S.T., M.T., selaku Subkoordinator Manajemen Sistem Informasi dan Teknologi, Kelompok/Fungsi Pengembangan Sistem dan Pengolahan Data, Pusdatik;
6. Muhammad Dwison Alizah, S.Tr.TP, selaku Subkoordinator Tatakelola dan Kepatuhan Keamanan Sistem Informasi dan TIK, Kelompok/Fungsi Manajemen Risiko dan Kelangsungan TIK;
7. Agung Widodo, S.E., selaku Subkoordinator Operasional dan Pengamanan Persandian, Kelompok/Fungsi Manajemen Risiko dan Kelangsungan TIK;
8. Thoriq Rahmat Hidayat, S.Tr.TP, selaku Manggala Informatika Ahli Pertama, Kelompok/Fungsi Manajemen Risiko dan Kelangsungan TIK;
9. Anis Nurul Hanifah, A.Md., selaku Pranata Komputer Pelaksana, Kelompok/Fungsi Operasi dan Layanan TIK;
10. Muhammad, Sandiman Pelaksana Lanjutan, Kelompok/Fungsi Bagian Umum Pusdatik;
11. Fitri Aniani, S.Sos., Pengelola BMN, Kelompok/Fungsi Bagian Umum Pusdatik;
12. Cut Ageng Sulistyowati S.Kom., Asisten Pengelelola Data Perkantoran, Kelompok/Fungsi Bagian Umum Pusdatik;
13. Surti Suryani, Asisten Pengelelola Data Perkantoran, Kelompok/Fungsi Bagian Umum Pusdatik.

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE) Badan Siber dan Sandi Negara



4. Pembuatan Standar Operasional Prosedur Penilaian Risiko Keamanan (Risk Assessment).

Pada hari Rabu tanggal 12 Oktober 2022, dilaksanakan rapat Tim Efektif untuk melakukan pembahasan penyusunan Standar Operasional Prosedur (SOP) tentang Penilaian Risiko (Risk Assesment) Sistem Pemerintahan Berbasis Elektronik di lingkungan Badan Siber dan Sandi Negara, yang dipimpin oleh Project Leader Perubahan yaitu AKBP Rakhmat Damdami.

BADAN SIBER DAN SANDI NEGARA

Nomor : 576/P2/KH.01.02/10/2022
Sifat : Biasa
Lampiran : Satu Berkas
Hal : Undangan Pembahasan Penyusunan Standar Operasional Prosedur (SOP) tentang Penilaian Risiko (Risk Assesment) SPBE di Lingkunga BSSN

Depok, 10 Oktober 2022

Yth. Daftar Undangan Terlampir
di –
Tempat

1. Dasar :
 - a. Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara;
 - b. Surat Perintah Kapri Nomor Sprin/1718/VII/DIK.2.5/2022 tanggal 15 Juli 2022 perihal Perintah mengikuti Pelatihan Kepemimpinan Nasional Tingkat II Angkatan XVIII tahun 2022 di Pusdikmin Lemdiklat Polri;
 - c. Surat Kapri Nomor B/5806/VII/DIK.2.5/2022/SSDM tanggal 15 Juli 2022 perihal Penghadapan Peserta Pelatihan Kepemimpinan Nasional Tingkat II Angkatan XVIII tahun 2022;
 - d. Surat Perintah Nomor 23/P2/KP.07.01/09/2022 tanggal 14 September 2022 tentang Tim efektif untuk mendukung pembuatan Proyek Perubahan PKN Tingkat II angkatan XVIII tahun 2022 a.n. AKBP Rakhmat Damdami S.A.P. M.Si., NRP 74050727 selaku Kepala Bagian Umum, Pusat Data dan TIK BSSN terkait pelaksanaan proyek perubahan dengan judul "Optimalisasi Pusdatik Dalam Melakukan Manajemen Risiko Sistem Pemerintah Berbasis Elektronik di Lingkungan Badan Siber dan Sandi Negara.
2. Merujuk dasar tersebut diatas, bersama ini kami mengundang Bapak/Ibu untuk hadir dalam Undangan Pembahasan Penyusunan Standar Operasional Prosedur (SOP) tentang Penilaian Risiko (Risk Assesment) Sistem Pemerintahan Berbasis Elektronik di Lingkungan Badan Siber dan Sandi Negara yang dilaksanakan pada:
Hari/Tanggal : Rabu, 12 Oktober 2022
Waktu : 09.30 s.d. selesai
Tempat : Ruang Rapat Pusdatik Lt. 6, Gedung D4, Kantor BSSN Sawangan
3. Demikian disampaikan, atas perhatiannya dan kerja samanya diucapkan terima kasih.



Tembusan :

1. Kepala Badan Siber dan Sandi Negara;
2. Wakil Kepala Badan Siber dan Sandi Negara;
3. Plt. Sekretaris Utama;
4. Inspektorat.

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE) Badan Siber dan Sandi Negara

Lampiran | Surat Undangan
Nomor : 576/P2/KH.01.02/10/2022
Tanggal : 10 Oktober 2022

DAFTAR UNDANGAN

1. Rakhmat Damdami S.A.P. M.Si., selaku Kepala Bagian Umum Pusdatik;
2. James Leonardo, S.ST., selaku Koordinator Fungsi Pengembangan Sistem Dan Pengolahan Data, Pusdatik;
3. Noor Hafidz, S.ST., selaku Koordinator Fungsi Operasi Dan Layanan TIK;
4. Adi Nugroho, S.ST., S.Kom selaku Koordinator Fungsi Manajemen Risiko Dan Kelangsungan TIK;
5. Agung Nursilo, S.S.T., M.T., selaku Subkoordinator Manajemen Sistem Informasi dan Teknologi, Kelompok/Fungsi Pengembangan Sistem dan Pengolahan Data, Pusdatik;
6. Muhammad Dwison Alizah, S.Tr.TP, selaku Subkoordinator Tatakelola dan Kepatuhan Keamanan Sistem Informasi dan TIK, Kelompok/Fungsi Manajemen Risiko dan Kelangsungan TIK;
7. Agung Widodo, S.E., selaku Subkoordinator Operasional dan Pengamanan Persandian, Kelompok/Fungsi Manajemen Risiko dan Kelangsungan TIK;
8. Thoriq Rahmat Hidayat, S.Tr.TP, selaku Manggala Informatika Ahli Pertama, Kelompok/Fungsi Manajemen Risiko dan Kelangsungan TIK;
9. Anis Nurul Hanifah, A.Md., selaku Pranata Komputer Pelaksana, Kelompok/Fungsi Operasi dan Layanan TIK;
10. Muhammad, Sandiman Pelaksana Lanjutan, Kelompok/Fungsi Bagian Umum Pusdatik;
11. Fitri Ariani, S.Sos., Pengelola BMN, Kelompok/Fungsi Bagian Umum Pusdatik;
12. Cut Ageng Sulistyowati, S.Kom., Asisten Pengelola Data Perkantoran, Kelompok/Fungsi Bagian Umum Pusdatik;
13. Suri Suryani, Asisten Pengelola Data Perkantoran, Kelompok/Fungsi Bagian Umum Pusdatik.

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE) Badan Siber dan Sandi Negara



5. Pembuatan Petunjuk Teknis Penilaian Risiko Keamanan (Risk Assesment).

Pada hari Kamis tanggal 20 Oktober 2022, dilaksanakan rapat Tim Efektif untuk melakukan pembahasan penyusunan Petunjuk Teknis tentang Penilaian Risiko (Risk Assesment) Sistem Pemerintahan Berbasis Elektronik di lingkungan Badan Siber dan Sandi Negara, yang dipimpin oleh Project Leader Perubahan yaitu AKBP Rakhmat Damdami.

BADAN SIBER DAN SANDI NEGARA

Nomor : 577/P2/KH.01.02/10/2022
Sifat : Biasa
Lampiran : Satu Berkas
Hal : Undangan Pembahasan Penyusunan Petunjuk Teknis tentang Penilaian Risiko (Risk Assesment) SPBE di Lingkungan BSSN

Depok, 17 Oktober 2022

Lampiran I Surat Undangan
Nomor : 577/P2/KH.01.02/10/2022
Tanggal : 20 Oktober 2022

DAFTAR UNDANGAN

Yth. Daftar Undangan Terlampir
di –
Tempat

- Dasar :
 - Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara;
 - Surat Perintah Kapoli Nomor Sprin/1718/VII/DIK.2.5/2022 tanggal 15 Juli 2022 perihal Perintah mengikuti Pelatihan Kepemimpinan Nasional Tingkat II Angkatan XVIII tahun 2022 di Pusdikmin Lemdiklat Polri;
 - Surat Kapoli Nomor B/5806/VII/DIK.2.5/2022/SSDM tanggal 15 Juli 2022 perihal Penghadapan Peserta Pelatihan Kepemimpinan Nasional Tingkat II Angkatan XVIII tahun 2022;
 - Surat Perintah Nomor 23/P2/KP.07.01/09/2022 tanggal 14 September 2022 tentang Tim efektif untuk mendukung pembuatan Proyek Perubahan PKN Tingkat II angkatan XVIII tahun 2022 a.n. AKBP Rakhmat Damdami S.A.P, M.Si., NRP 74050727 selaku Kepala Bagian Umum, Pusat Data dan TIK BSSN terkait pelaksanaan proyek perubahan dengan judul "Optimalisasi Pusdatik Dalam Melakukan Manajemen Risiko Sistem Pemerintah Berbasis Elektronik di Lingkungan Badan Siber dan Sandi Negara.
- Merujuk dasar tersebut diatas, bersama ini kami mengundang Bapak/Ibu untuk hadir dalam Undangan Pembahasan Penyusunan Petunjuk Teknis tentang Penilaian Risiko (Risk Assesment) Sistem Pemerintahan Berbasis Elektronik di Lingkungan Badan Siber dan Sandi Negara yang dilaksanakan pada:
Hari/Tanggal : Kamis, 20 Oktober 2022
Waktu : 09.00 s.d. selesai
Tempat : Ruang Rapat Pusdatik Lt. 6, Gedung D4, Kantor BSSN Sawangan
- Demikian disampaikan, atas perhatiannya dan kerja samanya diucapkan terima kasih.



Tembusan :

- Kepala Badan Siber dan Sandi Negara;
- Wakil Kepala Badan Siber dan Sandi Negara;
- Pt. Sekretaris Utama;
- Inspektorat.

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE) Badan Siber dan Sandi Negara

- Rakhmat Damdami S.A.P, M.Si., selaku Kepala Bagian Umum Pusdatik;
- James Leonardo, S.ST., selaku Koordinator Fungsi Pengembangan Sistem Dan Pengolahan Data, Pusdatik;
- Noor Hafidz, S.ST., selaku Koordinator Fungsi Operasi Dan Layanan TIK;
- Adi Nugroho, S.ST., S.Kom selaku Koordinator Fungsi Manajemen Risiko Dan Kelangsungan TIK;
- Agung Nursilo, S.S.T., M.T., selaku Subkoordinator Manajemen Sistem Informasi dan Teknologi, Kelompok/Fungsi Pengembangan Sistem dan Pengolahan Data, Pusdatik;
- Muhammad Dwison Alizah, S.Tr.TP, selaku Subkoordinator Tatakelola dan Kepatuhan Keamanan Sistem Informasi dan TIK, Kelompok/Fungsi Manajemen Risiko dan Kelangsungan TIK;
- Agung Widodo, S.E., selaku Subkoordinator Operasional dan Pengamanan Persandian, Kelompok/Fungsi Manajemen Risiko dan Kelangsungan TIK;
- Thoriq Rahmat Hidayat, S.Tr.TP, selaku Manggala Informatika Ahli Pertama, Kelompok/Fungsi Manajemen Risiko dan Kelangsungan TIK;
- Anis Nurul Hanifah, A.Md., selaku Pranata Komputer Pelaksana, Kelompok/Fungsi Operasi dan Layanan TIK;
- Muhammad, Sandiman Pelaksana Lanjutan, Kelompok/Fungsi Bagian Umum Pusdatik;
- Fitri Ariani, S.Sos., Pengelola BMN, Kelompok/Fungsi Bagian Umum Pusdatik;
- Cut Ageng Sulistyowati S.Kom., Asisten Pengelelel Data Perkantoran, Kelompok/Fungsi Bagian Umum Pusdatik;
- Suri Suryani, Asisten Pengelelel Data Perkantoran, Kelompok/Fungsi Bagian Umum Pusdatik.

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE) Badan Siber dan Sandi Negara



6. Peningkatan kemampuan terhadap pegawai tentang penilaian risiko keamanan.

Pada hari Kamis tanggal 27 Oktober 2022, dilaksanakan pelatihan dasar dalam rangka pemahaman peningkatan kemampuan Penilaian Risiko (Risk Assessment) Sistem Pemerintahan Berbasis Elektronik di lingkungan Badan Siber dan Sandi Negara.



BADAN SIBER DAN SANDI NEGARA
Jalan Raya Meduri No.76, Kel. Duren Mekar, Kec. Bulevar, Depok 16518
Telepon (021) 77973366, Faksimile (021) 7844104, (021) 77973579
Website : <https://bsn.go.id>, E-mail : humas@bsn.go.id

SURAT PERINTAH
NOMOR : 26/P2/DL.01.02/10/2022

Merimbang : bahwa sehubungan pelaksanaan kegiatan Pelatihan Dasar Dalam Rangka Peningkatan Pemahaman dan Kemampuan Penilaian Risiko (Risk Assessment) Sistem Pemerintahan Berbasis Elektronik di Lingkungan Badan Siber dan Sandi Negara, perlu dikeluarkan Surat Perintah bagi Pegawai Negeri Sipil Badan Siber dan Sandi Negara;

Dasar : 1. Surat Keputusan Negara Republik Indonesia Nomor B/5805/VII/DK.2.5/2022/SSDM tanggal 15 Juli 2022 perihal Pemanggilan Peserta PKN Tingkat II Angkatan XVIII Tahun Anggaran 2022;
2. Program Kerja Kepala Pusat Data dan Teknologi Informasi Komunikasi;
3. Perimbangan Pimpinan;

Memberi Perintah

Kepada : Pegawai Negeri Sipil Badan Siber dan Sandi Negara yang namanya tersebut dalam lajur dua Lampiran Surat Perintah ini.

Untuk : 1. Melaksanakan Pelatihan Dasar Dalam Rangka Peningkatan Pemahaman dan Kemampuan Penilaian Risiko (Risk Assessment) Sistem Pemerintahan Berbasis Elektronik di Lingkungan Badan Siber dan Sandi Negara pada tanggal 27 Oktober 2022 di Kantor BSSN, Sawangan;
2. Melaksanakan perintah ini dengan sebaik-baiknya dan penuh tanggung jawab;
3. Membuat laporan setelah melaksanakan kegiatan dimaksud.

Depok, 24 Oktober 2022

a.n. Kepala Badan Siber dan Sandi Negara

Kepala Pusat Data dan Teknologi Informasi Komunikasi



Tembusan :
1. Kepala Badan Siber dan Sandi Negara;
2. Wakil Kepala BSSN;
3. Deputi Bidang Operasi Keamanan Siber dan Sandi;
4. Inspektur;
5. Kepala Biro Organisasi dan Sumber Daya Manusia.

Dokumen ini telah diandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Badan Sertifikasi Elektronik (BSE) Badan Siber dan Sandi Negara

BADAN SIBER DAN SANDI NEGARA

LAMPIRAN SURAT PERINTAH
NOMOR : 26/P2/DL.01.02/10/2022
TANGGAL : 24 Oktober 2022

DAFTAR NAMA PERSONIL PELAKSANA KEGIATAN PELATIHAN DASAR DALAM RANGKA PENINGKATAN PEMAHAMAN DAN KEMAMPUAN PENILAIAN RISIKO (RISK ASSESSMENT) SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN BSSN				
1 NO	2 NAMA	3 NIP.	4 PANGKAT/GOL. RUANG	5 JABATAN
1.	Reno Ramdano, S.T.TP	19910410 201012 1 001	Penata (IIIc)	Analisis Sistem Informasi dan Jaringan, Kelompok/Fungsi Manajemen Risiko dan Kelengkapan TIK pada Pusat Data dan Teknologi Informasi Komunikasi
2.	Muhammad	19780512 199812 1 001	Penata Muda Tk. I (IIIb)	Sandimen Pelaksana Layanan, Kelompok/Fungsi Layanan Tata Usaha Bagian Umum pada Pusat Data dan Teknologi Informasi Komunikasi
3.	Afonso Brolin Sihite, S.Tr.TP	19940717 201611 1 001	Penata Muda Tk. I (IIIb)	Analisis Sistem Informasi dan Jaringan, Kelompok/Fungsi Manajemen Risiko dan Kelengkapan TIK pada Pusat Data dan Teknologi Informasi Komunikasi
4.	Ahmad Farid, S.Tr.TP	19930207 201412 1 002	Penata Muda Tk. I (IIIb)	Sandimen Pertama, Kelompok/Fungsi Manajemen Risiko dan Kelengkapan TIK pada Pusat Data dan Teknologi Informasi Komunikasi
5.	Muhammad Dwison Alizah, S.Tr.TP	19950115 201611 1 001	Penata Muda (IIIa)	Pranata Komputer Pertama, Kelompok/Fungsi Manajemen Risiko dan Kelengkapan TIK pada Pusat Data dan Teknologi Informasi Komunikasi
6.	Gagas Paras Mulati, S.Tr.Kom	19970321 201912 1 001	Penata Muda (IIIa)	Analisis Sistem Informasi dan Jaringan, Kelompok/Fungsi Manajemen Risiko dan Kelengkapan TIK pada Pusat Data dan Teknologi Informasi Komunikasi
7.	Rico Budiyanto, A.Md.	19880129 201902 1 001	Pengatur (IIIC)	Pranata Komputer Pelaksana, Kelompok/Fungsi Operasi dan Layanan TIK pada Pusat Data dan Teknologi Informasi Komunikasi

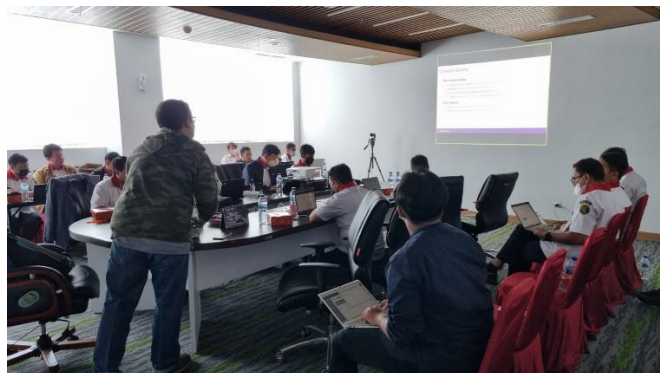
Dokumen ini telah diandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Badan Sertifikasi Elektronik (BSE) Badan Siber dan Sandi Negara

NO. 1	NAMA 2	NP. 3	PANGKAT/GOV. RUANG 4	JABATAN 5
8.	Gilang Triptari, A.Md.	1980013 201902 1 005	Pengantar (III)	Plarata Komputer Pribadi, Kelompok/Fungsi Manajemen Risiko dan Kelengkapan TK pada Pusat Data dan Teknologi Informasi Komunikasi
9.	Muhammad Luthi, A.Md.M.	19861028 201902 1 002	Pengantar (III)	Plarata Komputer Pribadi, Kelompok/Fungsi Manajemen Risiko dan Kelengkapan TK pada Pusat Data dan Teknologi Informasi Komunikasi
10.	Habibi Nersyia Khira, A.Md.	19940102 201902 1 006	Pengantar (III)	Plarata Komputer Pribadi, Kelompok/Fungsi Operasi dan Layanan TK pada Pusat Data dan Teknologi Informasi Komunikasi
11.	Muhammad Khairul Muttaqin, A.Md.	19861004 201902 1 002	Pengantar (III)	Plarata Komputer Pribadi, Kelompok/Fungsi Manajemen Risiko dan Kelengkapan TK pada Pusat Data dan Teknologi Informasi Komunikasi
12.	Eko Sanif Puayho, S.Kom.	19800810 202203 1 002	CPNS (IIIa)	Audit Sistem Informasi dan Jaringan (Cabin Praktek Komputer Aik Permana), Kelompok/Fungsi Manajemen Risiko dan Kelengkapan TK pada Pusat Data dan Teknologi Informasi Komunikasi
13.	Lingga Maulana Kurniawan, S.Kom.	19900420 202203 1 002	CPNS (IIIa)	Audit Deteksi Keamanan Siber, Kelompok/Fungsi Manajemen Risiko dan Kelengkapan TK pada Pusat Data dan Teknologi Informasi Komunikasi
14.	Bayu Ake Candra, S.Kom.	19861018 202203 1 001	CPNS (IIIa)	Audit Identifikasi Kerentanan Siber, Kelompok/Fungsi Manajemen Risiko dan Kelengkapan TK pada Pusat Data dan Teknologi Informasi Komunikasi
15.	Tri Ragi Mulyanti, A.Md.	19910802 202203 1 001	CPNS (IIIa)	Pengelolaan Sistem Informasi, Kelompok/Fungsi Manajemen Risiko dan Kelengkapan TK pada Pusat Data dan Teknologi Informasi Komunikasi
16.	Duhann Awahni, A.Md.Kom.	19880811 202203 1 001	CPNS (IIIa)	Pengelola Data Keamanan Siber dan Sandi, Kelompok/Fungsi Manajemen Risiko dan Kelengkapan TK pada Pusat Data dan Teknologi Informasi Komunikasi

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Badan Sertifikasi Elektronik (BS-E) Badan Siber dan Sandi Negara

NO. 1	NAMA 2	NP. 3	PANGKAT/GOV. RUANG 4	JABATAN 5
17.	Imam Muhammad Nurul Huda, A.Md.	19890707 202203 1 001	CPNS (IIIa)	Pengelola Data Keamanan Siber dan Sandi, Kelompok/Fungsi Manajemen Risiko dan Kelengkapan TK pada Pusat Data dan Teknologi Informasi Komunikasi
18.	Irfan Jafar, A.Md.	19961029 202203 1 001	CPNS (IIIa)	Pengelola Data Keamanan Siber dan Sandi, Kelompok/Fungsi Manajemen Risiko dan Kelengkapan TK pada Pusat Data dan Teknologi Informasi Komunikasi
19.	Agung Wibisono, A.Md.	19950906 202203 1 002	CPNS (IIIa)	Pengelola Data Keamanan Siber dan Sandi, Kelompok/Fungsi Manajemen Risiko dan Kelengkapan TK pada Pusat Data dan Teknologi Informasi Komunikasi
20.	Boma Indra Gunawan, S.T.	19961011 202203 1 001	CPNS (IIIa)	Audit Perilaku Siber, Kelompok/Fungsi Pengendalian Sistem dan Pengelolaan Data pada Pusat Data dan Teknologi Informasi Komunikasi

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Badan Sertifikasi Elektronik (BS-E) Badan Siber dan Sandi Negara



7. Pada hari Jumat tanggal 28 Oktober 2022, dilaksanakan Forum Grup Diskusi untuk melakukan pembahasan penyusunan tentang Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik di lingkungan Badan Siber dan Sandi Negara, dengan mengundang perwakilan pejabat di lingkungan Badan Siber dan Sandi Negara.

BADAN SIBER DAN SANDI NEGARA

Nomor : 574/P2/KH.01.02/10/2022
 Sifat : Biasa
 Lampiran : Satu Berkas
 Hal : Undangan FGD Diskusi tentang Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik di Lingkungan BSSN

Depok, 24 Oktober 2022

Lampiran I Surat Undangan
 Nomor : 574/P2/KH.01.02/09/2022
 Tanggal : 30 September 2022

DAFTAR UNDANGAN

Yth. Daftar Undangan Terlampir
 di - Tempat

1. Dasar :
 - a. Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara;
 - b. Surat Perintah Kepala Nomor Sprin/1718/VII/DK.2.5/2022 tanggal 15 Juli 2022 perihal Perintah mengikuti Pelatihan Kepemimpinan Nasional Tingkat II Angkatan XVIII tahun 2022 di Pusdikmin Lemdiklat Polri;
 - c. Surat Keputusan Nomor B/S600/VII/DK.2.5/2022/SSDM tanggal 15 Juli 2022 perihal Penghadapan Peserta Pelatihan Kepemimpinan Nasional Tingkat II Angkatan XVIII tahun 2022;
 - d. Surat Perintah Nomor 23/P2/KP.07.01/09/2022 tanggal 14 September 2022 tentang Tim efektif untuk mendukung pembuatan Proyek Perubahan PKN Tingkat II angkatan XVIII tahun 2022 a.n. AKBP Rakhmat Damdami S.A.P. M.Si., NRP 74050727 selaku Kepala Bagian Umum, Pusat Data dan TIK BSSN terkait pelaksanaan proyek perubahan dengan judul "Optimalisasi Pusatdata Dalam Melakukan Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik di Lingkungan Badan Siber dan Sandi Negara.
2. Mengingat dasar tersebut diatas, bersama ini kami mengundang Bapak/Ibu untuk hadir dalam FGD Diskusi tentang Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik di Lingkungan BSSN yang dilaksanakan pada:

Hari/Tanggal : Jumat, 28 Oktober 2022
 Waktu : 09.00 s.d. selesai
 Tempat : Aula dr. Roebiono Kertopati, Kantor BSSN Sawangan
3. Demikian disampaikan, atas perhatiannya dan kerja samanya diucapkan terima kasih.



- Tembusan :
1. Kepala Badan Siber dan Sandi Negara;
 2. Wakil Kepala Badan Siber dan Sandi Negara;
 3. Pj. Sekretaris Utama;
 4. Inspektur.

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE) Badan Siber dan Sandi Negara

1. 1 (satu) orang perwakilan dari Biro Perencanaan dan Keuangan;
2. 1 (satu) orang perwakilan dari Biro Organisasi dan SDM;
3. 1 (satu) orang perwakilan dari Biro Hukum dan Komunikasi Publik;
4. 1 (satu) orang perwakilan dari Biro Umum;
5. 1 (satu) orang perwakilan dari Direktorat Strategi Keamanan Siber dan Sandi;
6. 1 (satu) orang perwakilan dari Direktorat Kebijakan Tata Kelola Keamanan Siber dan Sandi;
7. 1 (satu) orang perwakilan dari Direktorat Kebijakan Teknologi Keamanan Siber dan Sandi;
8. 1 (satu) orang perwakilan dari Direktorat Kebijakan Sumber Daya Manusia Keamanan Siber dan Sandi;
9. 1 (satu) orang perwakilan dari Direktorat Operasi Keamanan Siber;
10. 1 (satu) orang perwakilan dari Direktorat Operasi Keamanan dan Pengendalian Informasi;
11. 1 (satu) orang perwakilan dari Direktorat Operasi Sandi;
12. 1 (satu) orang perwakilan dari Direktorat Keamanan Siber dan Sandi Pemerintah Pusat;
13. 1 (satu) orang perwakilan dari Direktorat Keamanan Siber dan Sandi Pemerintah Daerah;
14. 1 (satu) orang perwakilan dari Direktorat Keamanan Siber dan Sandi Pembangunan Manusia;
15. 1 (satu) orang perwakilan dari Direktorat Keamanan Siber dan Sandi Keuangan, Perdagangan dan Pariwisata;
16. 1 (satu) orang perwakilan dari Direktorat Keamanan Siber dan Sandi Energi dan Sumber Daya Alam;
17. 1 (satu) orang perwakilan dari Direktorat Keamanan Siber dan Sandi Teknologi Informasi dan Komunikasi, Media, dan Transportasi;
18. 1 (satu) orang perwakilan dari Direktorat Keamanan Siber dan Sandi Industri;
19. 1 (satu) orang perwakilan dari Inspektur;
20. 1 (satu) orang perwakilan dari Pusat Pengkajian dan Pengembangan Teknologi Keamanan Siber dan Sandi;
21. 1 (satu) orang perwakilan dari Pusat Pengembangan Sumber Daya Manusia;
22. Tim Efektif Proper.

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE) Badan Siber dan Sandi Negara



8. Sosialisasi kepada personel mengenai Draft Peraturan Kepala Badan Siber dan Sandi Negara tentang Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik di lingkungan internal.

Pada hari Selasa tanggal 1 Nopember 2022, dilaksanakan sosialisasi terhadap draft Peraturan Kepala Badan Siber dan Sandi Negara tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik di lingkungan Badan Siber dan Sandi Negara, yang dipimpin oleh Project Leader Perubahan yaitu AKBP Rakhmat Damdami.

Disamping itu sosialisasi juga dilakukan secara informal / spontan dengan mengumpulkan pegawai, lewat zoom dan juga disampaikan melalui kesempatan pada apel pagi.

BADAN SIBER DAN SANDI NEGARA

Nomor : 578/P2/KH.01.02/10/2022
Sifat : Biasa
Lampiran : Satu Berkas
Hal : Undangan Sosialisasi terhadap Draft Peraturan Kepala Badan Siber dan Sandi Negara tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik di Lingkungan Badan Siber dan Sandi Negara

Depok, 28 Oktober 2022

Lampiran I Surat Undangan
Nomor : 578/P2/KH.01.02/10/2022
Tanggal : 28 Oktober 2022

DAFTAR SURAT UNDANGAN

1. 3 orang staf Sekretaris Utama;
2. 3 orang staf Deputy Bidang Strategi dan Kebijakan Keamanan Siber dan Sandi;
3. 3 orang staf Deputy Bidang Operasi Keamanan Siber dan Sandi;
4. 3 orang staf Deputy Bidang Keamanan Siber Dan Sandi Pemerintahan dan Pembangunan Manusia;
5. 3 orang staf Deputy Bidang Keamanan Siber dan Sandi Perekonomian.

Yth. Daftar Undangan Terlampir

di -
Tempat

1. Dasar :

- a. Peraturan Badan Siber dan Sandi negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara;
 - b. Surat Perintah Kapoti Nomor Sprin/1718/VII/DIK.2.5/2022 tanggal 15 Juli 2022 perihal Perintah mengikuti Pelatihan Kepemimpinan Nasional Tingkat II Angkatan XVIII tahun 2022 di Pusdikmin Lemdiklat Polri;
 - c. Surat Kapoti Nomor B/5806/VII/DIK.2.5/2022/SSDM tanggal 15 Juli 2022 perihal Penghadapan Peserta Pelatihan Kepemimpinan Nasional Tingkat II Angkatan XVIII tahun 2022;
 - d. Surat Perintah Nomor 23/P2/KP.07.01/09/2022 tanggal 14 September 2022 tentang Tim efektif untuk mendukung pembuatan Proyek Perubahan PKN Tingkat II angkatan XVIII tahun 2022 a.n. AKBP Rakhmat Dandani S.A.P. M.Si., NRP 74050727 selaku Kepala Bagian Umum, Pusat Data dan TIK BSSN terkait pelaksanaan proyek perubahan dengan judul "Optimalisasi Pusat Data Dalam Melakukan Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik di Lingkungan Badan Siber dan Sandi Negara.
2. Merujuk dasar tersebut diatas, bersama ini kami mengundang Bapak/Ibu untuk hadir dalam Sosialisasi terhadap Draft Peraturan Kepala Badan Siber dan Sandi Negara tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik di lingkungan Badan Siber dan Sandi Negara yang dilaksanakan pada:
- Hari/Tanggal : Selasa, 1 November 2022
Waktu : 09.00 s.d selesai
Tempat : Ruang Rapat Lt. 2, Gedung D4, Kantor BSSN Sawangan

3. Demikian disampaikan, atas perhatiannya dan kerja samanya diucapkan terima kasih.



Tembusan :

1. Kepala Badan Siber dan Sandi Negara;
2. Wakil Kepala Badan Siber dan Sandi Negara;
3. Pti. Sekretaris Utama;
4. Inspektorat.

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE) Badan Siber dan Sandi Negara

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE) Badan Siber dan Sandi Negara





9. Penerimaan peralatan sarana prasarana dasar bagi tim Penilai Risiko.

Pada hari Rabu tanggal 2 Nopember 2022, telah diterima 3 unit komputer untuk mendukung kegiatan tim penilai risiko, yaitu :

- 2 unit komputer Windows dari Biro Umum dimanfaatkan untuk kegiatan manajemen adminitrasi.
- 1 unit komputer Mac dari Pusdatik untuk mendukung kegiatan registrasi penerimaan laporan.



10. Analisa dan Evaluasi

Pada hari Rabu tanggal 2 Nopember 2022, dilaksanakan Analisa dan evaluasi pelaksanaan implementasi proyek perubahan Optimalisasi Pusdatik Dalam Melakukan Manajemen Risiko Sistem Pemerintah Berbasis Elektronik di Lingkungan Badan Siber dan Sandi Negara yang dipimpin oleh Kapusdatik selaku Mentor yaitu Brigadir Jenderal Ferdinand Mahulette, SE.

BADAN SIBER DAN SANDI NEGARA

Nomor : 579/P2/KH.01.02/10/2022
Sifat : Biasa
Lampiran : Satu Berkas
Hal : Undangan Analisa dan Evaluasi

Depok, 28 Oktober 2022

Lampiran I Surat Undangan
Nomor : 579/P2/KH.01.02/10/2022
Tanggal : 28 Oktober 2022

Yth. Daftar Undangan Terlampir
di –
Tempat

1. Dasar :
 - a. Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara;
 - b. Surat Perintah Kapro Nomor Spriv/1718/VII/DK.2.5/2022 tanggal 15 Juli 2022 perihal Perintah mengikuti Pelatihan Kepemimpinan Nasional Tingkat II Angkatan XVIII tahun 2022 di Pusdatik Lemdiklat Polri;
 - c. Surat Kaproli Nomor B/5806/VII/DK.2.5/2022/SSDM tanggal 15 Juli 2022 perihal Penghadapan Peserta Pelatihan Kepemimpinan Nasional Tingkat II Angkatan XVIII tahun 2022;
 - d. Surat Perintah Nomor 23/P2/KP.07.01/09/2022 tanggal 14 September 2022 tentang Tim efektif untuk mendukung pembuatan Proyek Perubahan PKN Tingkat II angkatan XVIII tahun 2022 a.n. AKBP Rakhmat Dardani S.A.P. M.Si. NRP 74050727 selaku Kepala Bagian Umum, Pusat Data dan TIK BSSN terkait pelaksanaan proyek perubahan dengan judul "Optimalisasi Pusdatik Dalam Melakukan Manajemen Risiko Sistem Pemerintah Berbasis Elektronik di Lingkungan Badan Siber dan Sandi Negara.
2. Menunjuk dasar tersebut diatas, bersama ini kami mengundang Bapak/Ibu untuk hadir dalam Analisa dan Evaluasi Pelaksanaan Implementasi Proyek Perubahan Optimalisasi Pusdatik Dalam Melakukan Manajemen Risiko Sistem Pemerintah Berbasis Elektronik di Lingkungan Badan Siber dan Sandi Negara yang dilaksanakan pada:
Hari/Tanggal : Rabu, 2 November 2022
Waktu : 09.30 s.d. selesai
Tempat : Ruang Rapat Pusdatik Lt. 6, Gedung D4, Kantor Sawangan
3. Demikian disampaikan, atas perhatiannya dan kerja samanya diucapkan terima kasih.



Tembusan :

1. Kepala Badan Siber dan Sandi Negara;
2. Wakil Kepala Badan Siber dan Sandi Negara;
3. Plt. Sekretaris Utama;
4. Inspektoral.

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Badan Sertifikasi Elektronik (BSrE) Badan Siber dan Sandi Negara

DAFTAR UNDANGAN

1. Rakhmat Dardani S.A.P. M.Si., selaku Kepala Bagian Umum Pusdatik;
2. James Leonardo, S.ST., selaku Koordinator Fungsi Pengembangan Sistem Dan Pengolahan Data, Pusdatik;
3. Noor Hafidz, S.ST., selaku Koordinator Fungsi Operasi Dan Layanan TIK;
4. Adi Nugroho, S.ST., S.Kom selaku Koordinator Fungsi Manajemen Risiko Dan Kelangsungan TIK;
5. Agung Nursilo, S.S.T., M.T., selaku Subkoordinator Manajemen Sistem Informasi dan Telekom, Kelompok/Fungsi Pengembangan Sistem dan Pengolahan Data, Pusdatik;
6. Muhammad Desion Alizah, S.Tr.TP, selaku Subkoordinator Tatakelola dan Kepatuhan Keamanan Sistem Informasi dan TIK, Kelompok/Fungsi Manajemen Risiko dan Kelangsungan TIK;
7. Agung Widodo, S.E., selaku Subkoordinator Operasional dan Pengamanan Persandian, Kelompok/Fungsi Manajemen Risiko dan Kelangsungan TIK;
8. Thong Rahmat Hidayat, S.Tr.TP, selaku Manggota Informatika Ahli Pertama, Kelompok/Fungsi Manajemen Risiko dan Kelangsungan TIK;
9. Anis Nurul Hanifah, A.Md., selaku Pranata Komputer Pelaksana, Kelompok/Fungsi Operasi dan Layanan TIK;
10. Muhammad, Sandiman Pelaksana Lanjutan, Kelompok/Fungsi Bagian Umum Pusdatik;
11. Fitri Ariani, S.Sos., Pengelola BMN, Kelompok/Fungsi Bagian Umum Pusdatik;
12. Cui Ageng Sulistyowati S.Kom., Asisten Pengelola Data Perkantoran, Kelompok/Fungsi Bagian Umum Pusdatik;
13. Suri Suryani, Asisten Pengelola Data Perkantoran, Kelompok/Fungsi Bagian Umum Pusdatik.

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Badan Sertifikasi Elektronik (BSrE) Badan Siber dan Sandi Negara





II. DESKRIPSI KEPEMIMPINAN STRATEGIS

A. Membangun Integritas dan Akuntabilitas Kinerja Organisasi

Pusdatik BSSN yang diberi tugas dan fungsi di dalam internal BSSN untuk melaksanakan perencanaan, pelaksanaan, evaluasi dan pelaporan di bidang data dan teknologi informasi komunikasi, harus melakukan terobosan-terobosan untuk melaksanakan tugas dan fungsi yang sudah diamanatkan. Dalam fungsi manajemen penilaian risiko dituntut untuk dilaksanakan dengan baik. Karena merupakan salah satu pelayanan untuk dapat memastikan keamanan dari perangkat teknologi informasi yang ada, dalam mencapai visi, misi dan tujuan telah ditetapkan sasaran strategis dengan pengukuran Indikator Kinerja Utama (IKU), maka perlu adanya pembenahan dengan melakukan manajemen risiko SPBE melalui pembuatan peraturan yang baku. Peraturan tersebut tentunya akan mempermudah pegawai penilai risiko untuk melaksanakan tugasnya, memberi kejelasan dan kepastian kepada stakeholder, memudahkan pemantauan dan pengendalian oleh pimpinan. Adanya peraturan ini merupakan salah satu menjaga

integritas pegawai. Untuk membangun integritas dan akuntabilitas dalam meningkatkan kinerja organisasi diperlukan :

1. Etika seorang pemimpin

Pemimpin yang dalam hal ini adalah Project Leader (Peserta PKN) harus menjadi role model, dengan mengimplementasikan dalam organisasinya Kode Etik dan Kode Perilaku yang berlaku, mengimplementasikan nilai-nilai organisasi, selalu berkomunikasi dengan pegawai yang dibentuk dalam tim tata efektif, bersama-sama dengan tim efektif untuk menyelesaikan masalah, konsisten dalam berpendapat dan mengambil keputusan selalu mengumpulkan bukti-bukti dan masukan dari pejabat dan pegawai lainnya.

2. Melakukan Pengawasan aktif

Agar integritas dan akuntabilitas kinerja organisasi selalu terjaga, dilakukan pengawasan yang aktif yaitu dengan melakukan pengawasan dan pengendalian dalam pelaksanaan aksi perubahan, dengan menerapkan Sistem Pengendalian Intern Pemerintah. Selain itu juga melakukan pengawasan langsung ke lapangan, mendengarkan masukan stakeholder dan meneliti setiap laporan yang masuk dengan melibatkan pegawai yang menangani.

3. Menempatkan orang-orang yang tepat

Agar aksi perubahan tersebut dapat berjalan lancar, maka diperlukan pegawai yang akan melaksanakan aksi perubahan yang kompeten, berperilaku yang baik, professional, bekerja

keras dan ikhlas serta mempunyai budaya kerja yang tinggi. Selain itu juga mempunyai komitmen yang tinggi dalam penerapan pengendalian terhadap masalah yang ada. Pegawai yang kriterianya seperti tersebut, maka dimasukkan dalam tim efektif.

4. Melakukan proses internalisasi yang efektif

Dalam rangka membangun integritas dan akuntabilitas telah dilakukan memberikan pengarahan dalam beberapa kegiatan dan melalui arahan dalam apel terhadap Perilaku staf pegawai agar menekankan Kerjasama, Akuntabilitas, Melayani, Inovasi, Disiplin, Jujur, Pioner dan Tanggung jawab. Selain itu juga ditetapkan apa yang menjadi hak dan kewajiban pegawai, benturan kepentingan, menciptakan lingkungan kerja yang kondusif, pengelolaan dan pengamanan informasi, bagaimana hubungan dengan pemangku kepentingan, hubungan dengan sesama pegawai.

B. Pengelolaan Budaya Kerja

Dalam rangka melaksanakan tugas dan fungsi di Pusdatik BSSN, seorang pemimpin harus berkomitmen untuk melaksanakan etos kerja yang sudah ditetapkan di lingkungan organisasinya. Diperlukan komitmen yang kuat antara Pemimpin dan Pegawai dalam mewujudkan visi dan misi yang sudah ditetapkan dalam organisasinya. Untuk menciptakan budaya kerja tersebut perlu dibangun kesadaran pegawai bahwa seluruh pegawai mempunyai peran yang sama, dapat melakukan komunikasi yang efektif dan

efisien yang dapat menciptakan suasana yang menggembirakan atau kondusif. Selain itu Pegawai juga harus dipersiapkan untuk bisa beradaptasi dengan perubahan-perubahan yang ada. Dengan adanya perubahan budaya kerja yang awalnya dilakukan manual dan sekarang dilakukan dengan digital, tentunya perlu dilakukan bimtek atau training. Peran dari seorang Pemimpin diperlukan untuk dapat mewujudkan budaya kerja yang sudah ditetapkan. Dengan adanya aksi perubahan di Pusdatik BSSN, dimana harus merubah budaya kerja yang awalnya manual menjadi digital, maka perlu dibangun dan dikelola budaya kerja yang sudah dilaksanakan dengan :

1. Memberikan penghargaan/Apresiasi kepada Pegawai.

Dalam rangka mewujudkan visi dan misi organisasi, maka peran pegawai sangat berarti. Karena Pegawai yang akan melaksanakan untuk mencapai visi dan misi organisasi. Dengan adanya aksi perubahan ini, tentunya yang sangat berperan dalam aksi perubahan tersebut adalah para pegawai di Pusdatik. Setiap tahun Pusdatik sudah melaksanakan pemberian reward kepada Pegawai Terbaik.

2. Memberi Pelatihan atau Bimbingan Teknis.

Agar Pegawai yang melaksanakan tugas pelayanan jasa dapat mengerti dan melaksanakan perubahan dengan adanya aksi perubahan, maka diberi penjelasan dengan melakukan rapat koordinasi. Selain itu juga dilakukan bimtek dan training bagi pegawai yang akan ditugaskan sebagai penilai risiko SPBE

3. Memberikan sikap yang positif.

Dengan adanya aksi perubahan ini tentunya perlu dilakukan pendekatan kepada pegawai penilai risiko, agar mereka dapat berpikir positif dengan adanya aksi perubahan ini. Dengan adanya aksi perubahan ini, sering dilakukan diskusi, sehingga semua pegawai merasa mendapat peran penting juga dalam meningkatkan kinerja organisasi.

4. Manajemen waktu yang baik

Agar pegawai bisa melaksanakan tugas dan mencapai kinerja individu, maka didorong untuk memanfaatkan waktu dengan baik. Waktu di kantor digunakan untuk melaksanakan tugas yang diberikan dan tidak menunda-nunda pekerjaan. Dengan adanya pemanfaatan waktu yang baik, akan menghasilkan pekerjaan yang optimal sesuai SOP bahkan lebih cepat.

C. Membangun Jejaring dan Kolaborasi

Dalam rangka implementasi aksi perubahan, perlu diidentifikasi stakeholder yang akan berpengaruh untuk kelancaran pelaksanaan aksi perubahan. Untuk kelancaran pelaksanaan aksi perubahan ini pendekatan yang akan dibangun dikelompokkan menjadi stakeholder primer dan sekunder. Bagi stakeholder primer yang sangat berpengaruh terhadap kelancaran proyek perubahan akan intensif dilakukan koordinasi. Dan untuk mempermudah membangun kolaborasi, maka stakeholder primer dibentuk Tim Efektif Proyek Perubahan sesuai Surat Perintah Kepala Pusdatik Nomor : 23/P2/KP.07.01/09/2022 tanggal 14 September 2022.

Untuk membangun jejaring dan kolaborasi dalam meningkatkan kinerja organisasi diperlukan :

1. Membangun komunikasi yang efektif.

Agar pegawai penilai risiko dapat melaksanakan aksi perubahan dengan baik, maka selalu dilakukan komunikasi dengan diskusi bersama untuk mendengarkan tanggapan atas aksi perubahan, mendengarkan kendala yang dihadapi.

2. Mendengarkan informasi dan masukan.

Agar dapat membuat keputusan yang dapat diterima oleh bawahan, maka seorang pemimpin harus mau mendengarkan apa yang menjadi keluhan dan masukan dari bawahan, sehingga berimbang informasi yang diterima.

3. Menyampaikan isi pesan secara verbal dan nonverbal

Ketepatan penggunaan bahasa verbal dan nonverbal makin membuat komunikasi menjadi efektif serta mempermudah proses penerimaan dan pemaknaan pesan oleh lawan bicara.

4. Memperkirakan waktu terbaik untuk mendengar dan berbicara

Dikutip dari buku *Developing Interpersonal Skills* (Mengembangkan Keterampilan Antarpribadi) (2021) karya Muhammad Basri Wello dan Lely Novia, membangun komunikasi yang efektif membutuhkan peran dari kedua belah pihak, yakni komunikator dan komunikan. Saat komunikator berbicara, hendaknya komunikan mendengar dan memahami isi pesan yang disampaikan. Begitu pula ketika komunikan menanggapi pesan, komunikator hendaknya memperhatikan.

III. IMPLEMENTASI STRATEGI MARKETING

A. Dukungan/Peta Stakeholder

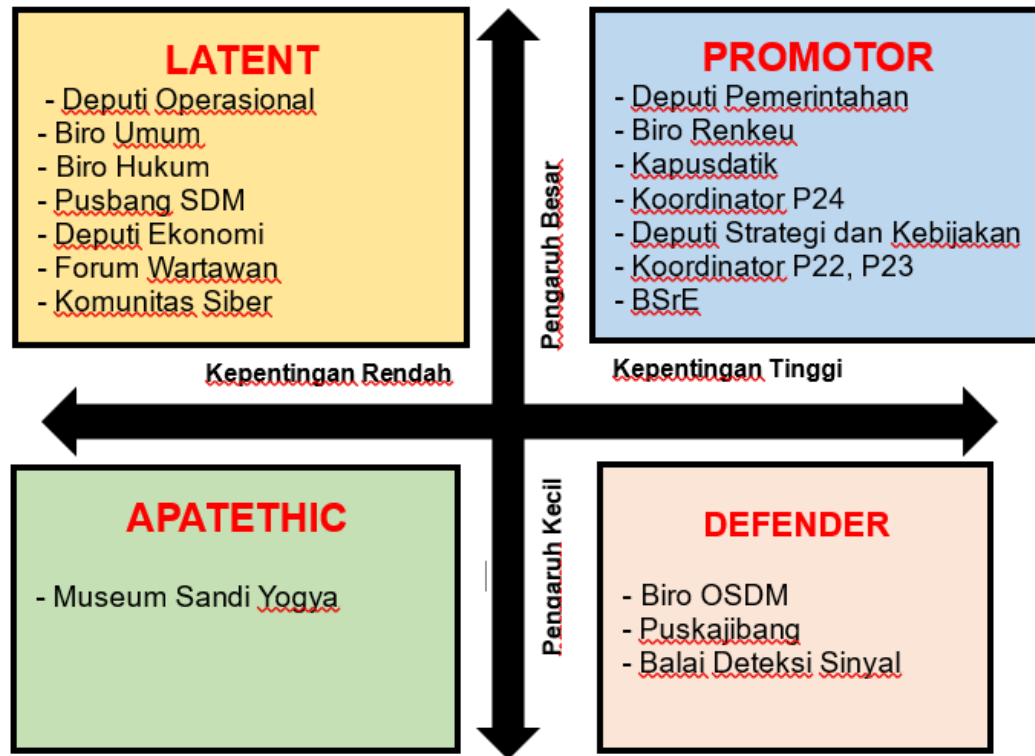
Pendekatan dilakukan kepada semua stakeholder dengan berbagai strategi yang efektif. Berbagai pendekatan telah dilakukan dengan memperhatikan peran dan tugas masing-masing stakeholder, antara lain:

1. Promoters, pendekatan yang dilakukan :
 - Meningkatkan Koordinasi dan konsultasi yang intens;
 - Melibatkan promotor dalam pengambilan keputusan dalam perencanaan, pelaksanaan dan evaluasi;
2. Defenders, pendekatan yang dilakukan;
 - Melaksanakan koordinasi dan komunikasi yang intens;
 - Meningkatkan motivasi dan kompetensi.;
 - Memberikan apresiasi atas upaya-upaya yang telah dilakukan.
 - Memberikan kesempatan untuk terlibat dalam pelaksanaan kegiatan lembaga, seperti menjadi narasumber.
 - Sebagai unsur kolaborasi untuk proyek perubahan.
3. Latens, pendekatan yang dilakukan;
 - Meningkatkan koordinasi dan komunikasi yang intens;
 - Membangun kerjasama dalam penyusunan peraturan;
 - Dilibatkan aktif dalam kegiatan sosialisasi;
4. Apathetics, pendekatan yang dilakukan;
 - Dilibatkan dalam perencanaan dan pelaksanaan tahapan kegiatan.

Dari berbagai upaya yang dilakukan di atas, telah terjadi pergeseran peta stakeholder ke arah positif, baik ke arah Promoters maupun

Defenders serta penambahan stakeholder baru pada Latent. Perubahan peta stakeholder dapat dilihat pada tabel berikut:

Gambar 4. Perubahan Peta Stakeholder



Dari hasil strategi komunikasi yang dijalankan maka terdapat pergeseran dalam peta stakeholder, yaitu :

1. Deputi Strategi dan Kebijakan yang semula Apatethis berubah menjadi Promoter. Hal ini karena pembuatan peraturan dan kebijakan merupakan salah satu tupoksi yang dijalankan dalam kedeputian ini. Oleh karena itu maka Deputi Strategi dan Kebijakan memberikan dukungan atas keberhasilan dan keberlanjutan dari proyek perubahan ini.
2. Deputi Ekonomi yang semula Apatethis berubah menjadi Latent. Hal ini karena Deputi bidang Ekonomi banyak berhubungan dengan pelaku pelaku ekonomi, dimana sangat memerlukan

keamanan siber demi terciptanya iklim investasi yang aman, oleh karena itu berharap Proyek Perubahan ini dapat ditindaklanjuti untuk kegiatan eksternal.

3. Balai Sertifikasi Elektronik yang semula Defender berubah menjadi Promoter. Hal ini karena Balai Sertifikasi Elektronik berkepentingan terhadap sertifikat elektronik dan tanda tangan elektronik, yang mana dalam kegiatannya tidak dapat terputus oleh adanya gangguan serangan siber, sebab ini bersifat pelayanan publik terhadap keabsahan dokumen dokumen elektronik yang telah diterapkan di beberapa kementerian/Lembaga dan pemerintah daerah
4. Koordinator P22 (pengembangan sistem dan pengolahan data) dan Koordinator P23 (operasi dan layanan TIK) yang semula Defender berubah menjadi Promoter. Hal ini karena di P22 sangat berhubungan erat dengan banyak sistem aplikasi yang perlu diamankan, demikian pula di P23 dimana banyak perangkat keras dan server yang menjadi tanggung jawabnya yang tentu juga rawan terhadap terjadinya serangan siber.
5. Kemudian yang baru masuk mengisi ke Peta Apatethic adalah Museum Sandi Yogya, tentu ini memberikan pengaruh yang bagus karena museum Yogya sebagai salah satu tujuan wisata Pendidikan, banyak dikunjungi oleh masyarakat umum, sehingga dapat menjadi sarana promosi terhadap keamanan siber.

6. Selanjutnya ada Forum wartawan dan komunitas siber yang juga perlu untuk digandeng sebagai stakeholder. Forum Wartawan adalah pihak yang paling cepat menyampaikan berita apabila terjadi serangan siber atau kebocoran data, oleh karena itu dapat dijadikan sebagai stakeholder untuk dapat menyampaikan pandangan tulisannya dalam hal manajemen risiko dalam kesempatan pemberitaan tersebut. Demikian juga halnya dengan Komunitas Siber, mereka sering menjadi narasumber ataupun memberikan pendapat melalui media terkait dengan keamanan data dan informasi. Keduanya meskipun memiliki kepentingan yang kecil dalam hal ini akan tetapi memiliki pengaruh yang sangat besar terhadap pemberitaan dan pembentukan opini, sehingga dapat membantu memberikan edukasi dan pemahaman tentang keamanan siber secara lebih luas dan ilmiah.

B. Diseminasi Dan Publikasi

Berikut merupakan pendekatan marketing yang akan dilakukan dalam proyek perubahan ini, melalui pendekatan marketing ini diharapkan pelaksanaan Proyek Perubahan dapat berjalan efektif dan efisien.

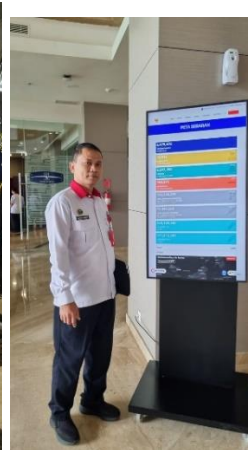
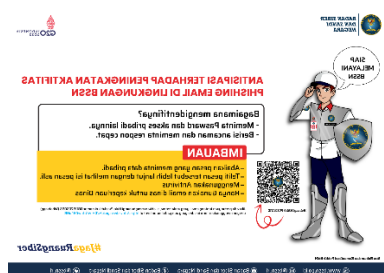
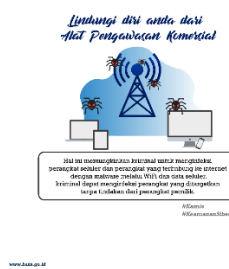
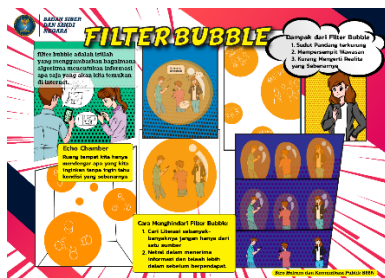
1. **Customer.** Customer merupakan elemen yang paling penting dalam pemasaran sektor publik, karena customer merupakan awal dan akhir dari proses pemberian layanan. Dalam proyek

perubahan ini yang menjadi customer adalah seluruh Satuan Kerja di BSSN dan seluruh Pegawai di BSSN.

2. **Place.** Place atau tempat merupakan elemen rigid dalam manajemen pemasaran, dikarenakan sifatnya tetap dan sulit untuk diubah. Dalam proyek perubahan ini yang menjadi place atau tempat adalah seluruh lingkungan kerja di kantor BSSN, yaitu Jakarta, Sawangan, Sentul dan Batam.
3. **Product.** Produk dalam proyek perubahan ini adalah Draft Peraturan Kepala BSSN tentang Manajemen Risiko Keamanan Siber, Standar Operasional Prosedur dan Petunjuk Teknis Penilaian Risiko Keamanan Siber.
4. **Price.** Price atau harga dapat diartikan sebagai pengorbanan waktu dan pikiran yang dikeluarkan untuk terlaksananya Proper ini, karena secara anggaran belum didukung oleh DIPA BSSN untuk saat ini, sehingga menggunakan daya usaha semampunya. Namun demikian untuk ke depan dalam hal pengadaan dukungan sarana prasana akan diajukan melalui anggaran DIPA BSSN tahun berikutnya.
5. **Promotion.** Merupakan elemen akhir yang mendukung pelaksanaan proyek perubahan ini. Kegiatan promotion dilaksanakan melalui sosialisasi hasil pelaksanaan Proper baik secara langsung maupun tidak langsung. Untuk promosi antara lain :

a. Pembuatan Brosur / Leaflet / Banner

Proyek perubahan ini bertujuan untuk mengamankan data, jaringan dan perangkat siber di BSSN, sehingga dalam pemasarannya dilakukan dalam bentuk brosur / leaflet / banner baik cetak maupun digital yang disebarluaskan kepada seluruh stakeholders terkait.

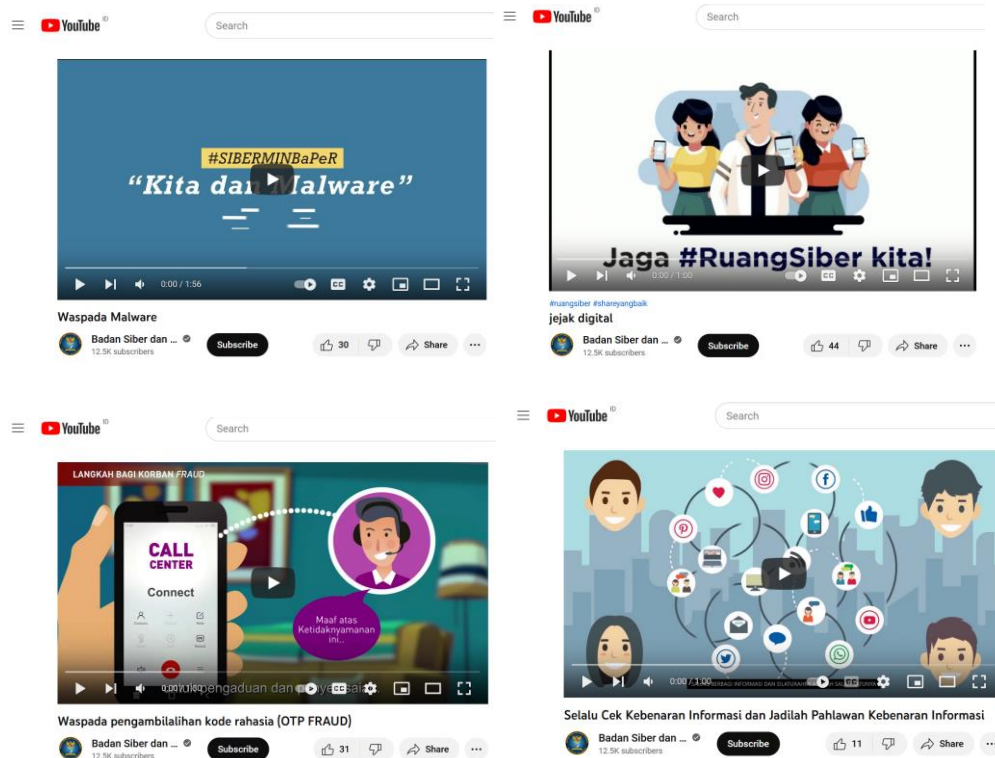




b. Media Sosial dan Web

Media sosial menggunakan akun Instagram dan website resmi BSSN baik yang dikelola oleh Pusdatik sendiri maupun melalui Biro Hukum dan Komunikasi Publik, diantaranya ;

- Edukasi masyarakat di <https://bssn.go.id/masyarakat-umum/>
- Publikasi di <https://bssn.go.id/publikasi/>
- Himbauan Keamanan di <https://bssn.go.id/security-advisory/>
- <https://www.youtube.com/watch?v=2br8En8jCwE>
- <https://www.youtube.com/watch?v=LHBqXoSmkTg>
- <https://www.youtube.com/watch?v=0Af52D3PfVA>
- <https://www.youtube.com/watch?v=txgABjX1ef4>
- <https://www.youtube.com/watch?v=PQTMcpW02D8>
- <https://www.youtube.com/watch?v=d8iM6XliW04>
- https://www.youtube.com/watch?v=_LYyINB9jFM&t=3s



IV. KEBERLANJUTAN PROYEK PERUBAHAN

A. Dukungan Mentor untuk keberlanjutan Proyek Perubahan

Kapusdatik BSSN selaku mentor dari peserta PKN II atas nama Rakhmat Damdami, sangat mendukung gagasan proyek perubahan ini yang berjudul Optimalisasi Pusdatik Dalam Melakukan Manajemen Risiko Sistem Pemerintah Berbasis Elektronik di Lingkungan Badan Siber dan Sandi Negara.

Karena Sejak terbentuknya BSSN tahun 2017, efektif beroperasi pertengahan 2018 dan pernah mengalami reorganisasi tahun 2021, masih banyak kekurangan alat kelengkapan organisasi termasuk di dalamnya adalah peraturan peraturan. Ini sangat mempengaruhi tugas pokok di BSSN, khususnya di lingkungan Pusdatik, tidak dapat melaksanakan salah satu fungsi yang ada di

kami yaitu manajemen risiko sebagai suatu upaya untuk mencegah terjadinya upaya serangan siber ataupun kebocoran data.

Tidak adanya peraturan ini, menyebabkan Pusdatik kesulitan untuk mencapai nilai indeks nilai SPBE BSSN yang telah menjadi target yang telah ditentukan. Oleh karena itu dengan langkah optimalisasi Pusdatik melalui pembuatan peraturan ini diharapkan juga dapat mengangkat indeks SPBE BSSN yang setiap tahun dilakukan evaluasi oleh Kemenpan RB.

Dalam proyek perubahan ini Kapusdatik BSSN selaku mentor menyarankan tidak hanya terbatas pada pembuatan Peraturan Kepala saja namun juga SOP dan petunjuk Teknis untuk pelaksanaannya, sehingga Ketika Peraturan tersebut disahkan, pegawai yang masuk dalam Tim Penilai dapat segera melaksanakan tugasnya karena sudah dilengkapi dengan peraturan, SOP dan Petunjuk Teknis. Tentu sebelumnya mereka juga dibekali terlebih dahulu dengan pelatihan untuk peningkatan kemampuan dan juga dukungan sarana prasana terkait.

Untuk kedepannya pimpinan akan mengajukan perangkat dalam penilaian risiko ini melalui anggaran organisasi baik melalui APBN maupun melalui pinjaman dalam dan luar negeri.

Oleh karena itu Kapusdatik BSSN sekaligus Mentor dari Siswa berharap proyek perubahan ini dapat segera diterapkan dan saya dukung untuk keberlanjutannya ke depan dalam mensukseskan visi dan misi BSSN.

B. Rencana Implementasi Jangka Menengah dan Jangka Panjang

Tujuan utama yang akan dicapai dalam Proyek Perubahan ini adalah terwujudnya manajemen risiko sistem pemerintahan berbasis elektronik di lingkungan BSSN melalui pembuatan Peraturan Kepala BSSN tentang Manajemen Risiko, pembuatan SOP Penilaian Risiko dan Petunjuk Teknis Penilaian Risiko. Setelah Peraturan ini terbentuk maka penerapannya menjadi sangat penting dalam mewujudkan tujuan dan manfaat Proyek Perubahan ini.

Pada implementasi proyek perubahan ini tujuan jangka pendek telah pembuatan Draft Peraturan Kepala BSSN tentang Manajemen Risiko.

Untuk mencapai tujuan jangka menengah, maka Peraturan Kepala BSSN tentang Manajemen Risiko ini akan dilakukan harmonisasi di Biro Hukum BSSN, untuk selanjutnya dapat diajukan pengesahannya kepada Kementerian Hukum dan HAM pada implementasi jangka Panjang berikutnya.

Pada implementasi jangka menengah ini juga direncanakan akan diusulkan perangkat utama untuk melakukan penilaian risiko melalui anggaran DIPA BSSN, sehingga diharapkan pada implementasi jangka Panjang, perangkat tersebut dapat tersedia dan dapat segera digunakan.

Selanjutnya pada implementasi jangka Panjang, diharapkan Draft Peraturan Kepala BSSN tentang Manajemen Risiko ini telah disetujui dan ditanda tangani, untuk kemudian dapat segera

diterapkan dan dijadikan pedoman bagi pegawai BSSN khususnya personil Pusdatik yang membidangi manajemen risiko untuk dapat melaksanakan tugas fungsinya secara optimal.

V. IMPLEMENTASI SOLUSI TERHADAP KENDALA

Selama pelaksanaan proyek perubahan jangka pendek terdapat beberapa kendala yang dihadapi, baik itu kendala internal maupun kendala eksternal yang tentunya berpotensi menghambat pelaksanaan dan tercapainya tujuan proyek perubahan. Kendala-kendala tersebut dapat diuraikan sebagai berikut :

A. Kendala Internal

- Keterbatasan waktu tim efektif dalam pelaksanaan proyek perubahan karena tumpang tindih dengan pekerjaan lainnya;
- Jumlah pegawai yang memiliki spesialisasi dalam manajemen risiko masih sangat sedikit;
- Resistensi dari pegawai lama yang disebabkan masih dalam paradigma lama;
- Pergantian Pimpinan;
- Mutasi pegawai efektif.
- Ego sektoral antar bagian atau kelompok fungsi

B. Kendala Eksternal

- Rencana pelaksanaan kegiatan Konferensi Tingkat Tinggi G20 yang menjadikan fokus seluruh stakeholders lebih ditujukan pengamanan IT / Siber di lokasi secara khususnya.
- Pemahaman terkait manajemen Risiko SPBE yang tidak merata

- Ego Sektoral antar unit kerja

Dalam menyikapi kendala, baik internal maupun eksternal dapat dilakukan beberapa hal sehingga proyek perubahan dapat mencapai target capaiannya sesuai dengan yang direncanakan:

1. Pembagian dan manajemen waktu dan tugas antara pelaksanaan kegiatan anggota tim efektif dan saling membackup bila ada permasalahan yang harus segera ditangani;
2. Strategi komunikasi, baik secara formal maupun informal, untuk menjaga keberlangsungan jejaring kerja. Penggunaan teknologi komunikasi seperti Whatsapp group sangat membantu dalam mengefektifkan koordinasi;
3. Terkait keterbatasan jumlah pegawai yang memiliki spesialisasi dalam penilaian risiko, diupayakan dengan melakukan pelatihan secara bertahap menyesuaikan kondisi;
4. Terkait dengan resistensi pegawai lama, dilakukan melalui dialog dan internalisasi yang dilakukan oleh internal Pusdatik baik secara formal maupun informal.
5. Menerapkan Manajemen Pengetahuan sebagai kontrol pergantian pimpinan atau mutasi pegawai efektif yang terjadi.
6. Sosialisasi atau penyampaian mengenai manfaat dan tujuan dari manajemen risiko untuk mengurai ego sektoral antar fungsi;
7. Sosialisasi kebijakan manajemen risiko, SOP dan petunjuk teknis kepada seluruh pemangku kepentingan.
8. Sosialisasi atau penyampaian mengenai manfaat dan tujuan dari manajemen risiko untuk mengurai ego sektoral unit kerja

VI. PEMBERDAYAAN ORGANISASI PEMBELAJARAN

Peter Senge mendefinisikan Learning organization adalah organisasi dimana pegawainya secara berkelanjutan mengembangkan kapasitasnya untuk mewujudkan hasil yang mereka inginkan, pola berfikir baru dan ekspansif ditumbuhkembangkan, keinginan bersama diberi ruang kebebasan dan pegawai secara terus menerus belajar bersama. Peter Sange juga mengatakan bahwa bekerja sebagai proses belajar berkelanjutan yang membentuk masa depan, bukan merupakan reaksi terhadap masa lampau. Sementara David Garvin mendefinisikan organisasi pembelajar sebagai organisasi yang mahir menciptakan, memperoleh, menginterpretasikan, mentransfer dan mempertahankan pengetahuan.

Pusdatik BSSN berusaha menerapkan learning organization dalam pencapaian tujuan organisasinya. Diantaranya dengan pembangunan proyek perubahan ini. Hal ini diawali dengan membangun komunikasi dengan seluruh unsur yang ada di internal Pusdatik BSSN untuk merumuskan apa yang akan dilakukan dan bagaimana mengerjakan apa yang dipahami. Rancangan Proyek Perubahan dikomunikasikan secara internal, diawali dengan pembentukan tim efektif hingga penyusunan Draft Peraturan, Standar Operasional Prosedur dan Petunjuk Teknis Manajemen Penilaian Risiko SPBE. Learning organization ditandai dengan adanya pengembangan yang terus-menerus melalui ide-ide baru, pengetahuan dan pemahaman yang baru, yang dipergunakan secara terus-menerus untuk mengantisipasi, berinovasi dan menemukan cara-cara baru yang lebih baik dalam mencapai tujuan

Proyek Perubahan ini. Dalam hal ini pencapaian tujuan Pusdatik BSSN menjadi organisasi yang adaptif dan pembelajar sebagai pengembangan fungsi Teknologi Informasi dan Komunikasi tidak hanya pada layanan data dan TIK saja tetapi juga menjamin keamanan dalam beraktivitas di ruang siber bagi pegawai BSSN. Hal ini ditandai dengan dilakukannya Manajemen dan Penilaian Risiko pada sistem pemerintahan berbasis Elektronik di BSSN. Koordinasi dengan setiap stakeholder baik internal maupun eksternal memperkaya pengetahuan project leader dan tim efektif sebagai upaya peningkatan peran Pusdatik dalam melakukan manajemen waktu yang lebih baik dalam pelaksanaan kegiatan anggota tim efektif secara lebih cepat dan akuntabel.

Setiap stakeholder baik internal maupun external memiliki ciri khas, kompetensi dan pengalaman masing masing. Dalam menjalankan sebuah proyek perubahan, kolaborasi adalah keharusan yang harus dilakukan agar mendapatkan segala kebaikan dari berbagai sumber. Komunikasi dengan stakeholder juga memiliki gaya yang berbeda, karena setiap stakeholder memiliki sifat yang beragam. Kejelasan dan keterbukaan informasi mempermudah setiap komunikasi dengan stakeholder.

Pada pelaksanaan proyek perubahan ini perlu adanya pemberdayaan organisasi pembelajaran yaitu :

1. Personal Mastery

Implementasi pedoman manajemen risiko mendorong penyelenggara sebagai personal (pegawai) untuk mengembangkan diri agar dapat melaksanakan manajemen risiko

sesuai pedoman yang ditetapkan. Peraturan, SOP dan Petunjuk Teknis yang baik dan terarah, akan memudahkan lembaga dalam melakukan evaluasi dan merencanakan pengembangan SDM bagi Tim Penilai Risiko yang lebih terarah dan tepat sasaran pada setiap pegawai. Penerapan teknologi dalam pedoman manajemen risiko juga mendorong personal pegawai untuk mengembangkan diri di bidang penguasaan teknologi. Hal-hal tersebut juga merubah paradigma pegawai dalam memberikan pelayanan prima kepada stakeholders.

2. Mental Models

Pengikutsertaan stakeholder dalam penyelenggaraan pelayanan publik di bidang manajemen risiko sebagaimana yang ditetapkan dalam Pedoman Pelayanan Publik mencakup keseluruhan proses penyelenggaraan Pelayanan Publik memberikan gambaran tentang kebutuhan setiap stakeholder. Survei kepuasan stakeholder secara berkala yang diatur dalam pedoman pelayanan memberikan gambaran kinerja lembaga dalam memberikan pelayanan manajemen risiko.

3. Shared Vision.

Penetapan pedoman manajemen risiko sebagai acuan dalam penyelenggaraan penilaian risiko sistem pemerintahan berbasis elektronik merupakan komitmen lembaga dalam mewujudkan visi bersama. Pedoman ini dijadikan sebagai acuan sehingga dapat menggerakkan organisasi pada tujuan bersama meskipun dengan

latar belakang, pendidikan, kesesuaian dan pengalaman yang berbeda.

4. Team Learning.

Implementasi Pedoman Manajemen Risiko yang telah ditetapkan mampu memotivasi pegawai sebagai penyelenggara layanan TIK untuk belajar secara adaptif, generative dan berkesinambungan. Layanan TIK dengan acuan pedoman yang jelas mendorong kemampuan organisasi untuk mensinergikan kegiatan team yang membentuk kebiasaan berbagi wawasan sehingga pembelajaran organisasi yang dilandasi wawasan pengetahuan dalam team menjadi sangat penting untuk meningkatkan kapasitas organisasi dalam menambah modal intelektualnya.

5. System Thinking.

Pedoman Manajemen Risiko yang dijalankan akan menghasilkan kinerja yang optimal karena mengatur hubungan kerja yang jelas antar divisi atau bagian. Kemampuan untuk membangun hubungan yang sinergis ini hanya akan dimiliki kalau semua anggota unit saling memahami pekerjaan unit lain dan memahami juga dampak dari kinerja unit yang dapat diraih, hal ini dapat diraih melalui implementasi pedoman yang telah ditetapkan.

Peran pemimpin sangat menentukan bagi pertumbuhan dan kelangsungan hidup suatu organisasi, termasuk dalam memberikan pengaruh terhadap perilaku bawahannya untuk mencapai tujuan organisasi.

Penerapan organisasi pembelajar di Pusdatik BSSN terkait implementasi proyek perubahan ini sudah dilakukan dengan baik, dan untuk meningkatkan kinerja organisasinya, perlu dilakukan beberapa langkah perbaikan pada sistem penyediaan informasi dan penyebaran informasi pembelajaran bagi seluruh anggota, mengoptimalkan kompetensi karyawan dengan memberikan penugasan khusus, meningkatkan kolaborasi dan pembelajaran tim, menjalin hubungan dan komunikasi yang baik dengan lingkungan eksternal dan internal, serta melakukan evaluasi terhadap langkah strategis yang diambil untuk mencapai target tujuannya.

Organisasi pembelajar memiliki pengaruh yang signifikan terhadap peningkatan kinerja organisasi. Kepemimpinan memiliki pengaruh yang signifikan terhadap terbentuknya organisasi pembelajar. Berbeda dengan budaya organisasi yang memiliki hubungan tidak signifikan dalam membentuk organisasi pembelajar. Kepemimpinan secara langsung tanpa melalui organisasi pembelajar memiliki hubungan yang negatif namun tidak signifikan dengan kinerja organisasi, sedangkan bila melalui organisasi pembelajar memiliki hubungan positif dan signifikan terhadap kinerja organisasi. Budaya organisasi tanpa melalui organisasi pembelajar memiliki hubungan negatif namun tidak signifikan dengan kinerja organisasi, namun bila melalui organisasi pembelajar, kinerja organisasi dapat ditingkatkan.

Strategi penting yang dilakukan untuk meningkatkan kinerja dalam proyek perubahan ini adalah mengadakan sistem evaluasi dan monitoring yang terukur serta rewards dan punishment yang transparan.

Direktur melakukan komunikasi terbuka dengan karyawan, pelanggan, pemerintah, untuk dapat mencapai tujuan. Pimpinan unit kerja juga melakukan mentoring kepada anggota timnya secara berjenjang, dan memasukkan proses belajar dan mengajar sebagai salah satu indikator penilaian kinerja. Strategi tersebut dilakukan melalui prinsip-prinsip organisasi pembelajar untuk mendorong peningkatan kinerja organisasi.

Beberapa hal yang dapat diambil dalam proses pembelajaran dalam implementasi proyek perubahan ini adalah sebagai berikut:

1. Pembelajaran tidak hanya dilakukan pada level individu dan tim, namun juga pada level organisasi. Pembelajaran bila diterapkan di kegiatan operasional harian akan mengubah cara pandang, pola pikir terhadap peluang perbaikan dan akhirnya dapat mendorong peningkatan efektivitas organisasi.
2. Pelatihan yang diberikan agar diterapkannya di pekerjaan sehari-hari serta dievaluasi efektifitas pelatihannya oleh atasan dan bagian kepegawaian. Untuk memotivasi karyawan dan menciptakan iklim pembelajaran berkelanjutan perlu diberikan juga penghargaan bagi anggota mencapai target belajarnya dan menjadi pengajar anggota lainnya, dengan memasukkan pengembangan kompetensi individu dan tim di dalam penilaian kinerja, termasuk kewajiban belajar melalui pelatihan, seminar, on the job training, rotasi dan mutasi, benchmarking, serta pemberian penugasan khusus.
3. Pemberdayaan pegawai dengan memberikan tugas khusus untuk menyelesaikan proyek proyek perbaikan di bidang proses kerja dan layanan penilaian risiko SPBE, akan membantu Pusdatik

menyelesaikan permasalahan dan hambatan yang dihadapi dalam mencapai tujuan organisasi.

4. Pemimpin yang memotivasi anggotanya untuk mau belajar secara berkelanjutan, melakukan monitoring terhadap target kerja yang diberikan kepada anggotanya, dan mengevaluasi serta mengembangkan sistem penilaian kinerja dapat membantu Pusdatik BSSN meningkatkan kinerja organisasi melalui organisasi pembelajar.
5. Evaluasi dan monitoring program kerja yang terukur serta menyediakan program reward dan punishment secara transparan terhadap hasil kerja yang dicapainya, perlu dilakukan secara konsisten untuk meningkatkan efektivitas pencapaian kinerja organisasi. Selanjutnya hasil evaluasi tersebut ditindaklanjuti dengan melakukan langkah perbaikan agar tercapai target bisnisnya, termasuk evaluasi terhadap penempatan orang yang tepat.
6. Pertemuan rutin dan keterbukaan informasi menjadi sangat penting dilakukan sebagai sarana untuk mendapatkan informasi dan komunikasi aktif dua arah. Penyediaan sistem informasi dapat berupa WA group discussion ataupun dalam bentuk juklak kerja yang disimpan dalam tempat yang mudah diakses oleh seluruh anggota baru maupun anggota lama. Pengaturan serah terima jabatan yang disamakan di setiap unit kerja akan memudahkan proses pertukaran informasi antara petugas lama dan petugas baru sebagai pengganti.

7. Kegiatan kebersamaan untuk mendorong keterbukaan, kebersamaan dan kesamaan persepsi dan kerjasama tim yang baik dapat dilakukan secara periodik, agar para pemimpin dan anggota lebih saling mengenal dan mengetahui apa yang menjadi harapan mereka dan mampu menyelaraskannya dengan tujuan organisasi yang diharapkan dari pihak pelanggan, masyarakat dan pemerintah daerah.

Output jangka pendek dari proyek perubahan ini adalah terbentuknya Draft Peraturan Kepala Badan Siber dan Sandi Negara tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik, serta Standar Operasional Prosedur dan Petunjuk Teknisnya.

Keberhasilan dari capaian output ini menunjukkan terimplementasikannya learning organization dengan sangat baik, antara lain:

- Memahami Tugas dan Fungsi Organisasi.
- Memahami Prinsip-Prinsip Sistem Manajemen Risiko.
- Memahami peran-peran para pihak dalam pelaksanaan manajemen risiko.
- Adaptif terhadap paradigma baru dan isu-isu strategis sistem pemerintahan berbasis elektronik.
- Mengoptimalkan semua potensi sumberdaya organisasi, memberikan challenge kompetensi pegawai untuk terus berkembang
- Menggalang dukungan semua pihak internal dan eksternal sesuai kapasitasnya.

Dan dari sisi pendekatan yang dilakukan dalam pelaksanaan proyek perubahan ini, maka ini memberikan lesson learnt bermakna antara lain prinsip Organisasi Pembelajaran, Organisasi Adaptif, Kepemimpinan Digital dan adanya dialog strategis.

VII. KONTRIBUSI MATA PELATIHAN PENDUKUNG

Salah satu mata pelatihan dalam PKN II adalah adanya materi pelatihan pilihan untuk menambah wawasan pengetahuan dan sebagai pendukung dalam pembuatan Laporan Proyek Perubahan. Sebagai mata pelatihan pendukung terkait dengan Proyek Perubahan ini, yang menitik beratkan pada manajemen risiko dan penilaian risiko maka penulis selama pembelajaran PKN II ini, mengambil beberapa mata pelatihan pilihan / pendukung yang dirasakan berkaitan secara signifikan maupun memperkaya wawasan tentang bagaimana manajemen risiko.

Adapun mata pelatihan pendukung yang diambil adalah sebagai berikut :

1. Certified Professional Risk Management

Membahas tentang bagaimana :

- a. Mengetahui ISO 31000:2018 sebagai salah satu Pedoman Internasional Penerapan Manajemen Risiko
- b. Refreshment/Knowledge Insight Manajemen Risiko
- c. Mengetahui Esensi Arsitektur Penerapan Manajemen Risiko



2. Certified Professional Governance, Risk Management & Compliance.

Membahas tentang bagaimana :

- ISO 37000:2020 (Pedoman Tata Kelola)
- ISO 31000:2018 (Pedoman Manajemen Risiko)
- ISO 37301:2021 (Compliance Management System)
- Definisi GRC
- Prinsip Tata Kelola Perusahaan
- Lingkup GRC
- Prinsip Kinerja Berprinsip
- GRC Capability Model – Komponen dan Elemen (Learn, Align, Perform & Review).
- Strategi GRC



3. Risk Management.

Membahas tentang bagaimana :

- Konsep Risiko based on ISO 31000:2018
- Manajemen Strategis
- Prinsip Manajemen Risiko based on ISO 31000:2018
- Kerangka Manajemen Risikoe
- Proses Manajemen Risiko based on ISO 31000:2018



4. Safety Management System

Membahasa tentang bagaimana :

- a. Memberikan pemahaman yang mendalam mengenai konsep dan pentingnya manajemen Keselamatan dari sudut pandang manajerial.
- b. Agar semua Stakeholder memahami pentingnya implementasi Safety Management system di semua lini serta membangun Safety awareness secara bersama – sama.
- c. Memahami minimum requirement implementasi Safety Management System supaya mudah diimplementasikan di perusahaan atau organisasi.
- d. Mengukur secara akurat sejauhmana sebuah perusahaan/ Organisasi sudah menerapkan konsep keselamatan (safety Performance Monitoring)



5. Enterprise Architecture

Membahas tentang Overview Enterprise Architecture dan Framework Enterprise Architecture, dimana Informasi Teknologi dalam Organisasi Modern,

- Sangat bergantung pada TI untuk operasional harian
- Menjalankan dan mengurus banyak sistem TI untuk mendukung proses bisnis
- Pengaruh TI pada model bisnis organisasi terus meningkat

- Peranan IT bergeser dari fungsi teknis dan pendukung menjadi fungsi strategis dan business-enabling
- Sistem informasi menjadi tulang punggung pada perubahan dan transformasi organisasi
- Investasi TI terus meningkat dari tahun ke tahun



6. Cyber Threats, Data Breach, and IT Risk Management

Struktur teknologi informasi di Indonesia mudah terserang oleh berbagai macam ancaman. Risiko ini terbukti dengan maraknya data data yang terbocorkan secara global untuk digunakan ilegal. Oleh karena itu perlunya kita untuk mengetahui kemungkinan ancaman dan risiko berbasis teknologi dan bagaimana cara untuk mengatasinya. Sistem manajemen risiko dapat memberikan pengamanan yang lebih terstruktur dan mudah untuk diterapkan.

Risiko dari sesuatu berbanding lurus dengan kemungkinan terjadinya dan dengan seberapa besar dampak jika risiko terjadi. Risiko bukan hanya berpeluang, tapi sudah sangat banyak risiko yang terwujud menjadi insiden. Dalam konteks teknologi informasi (TI), insiden-insiden menimbulkan dampak antara lain proses-proses dan layanan-layanan TI tidak lancar, terganggunya atau

berhentinya bisnis, kerugian finansial yang signifikan, corengnya citra organisasi, dan tidak tercapainya tujuan-tujuan



7. Mata Pelatihan lainnya sebagai penambah wawasan adalah :

- a. Seminar tentang Membangun Kerja Sama Yang Strategis Dengan Instansi Lain Untuk Menuju Polri Yang Presisi



- b. Workshop tentang Konseptualisasi dan Penyusunan Indeks Profesional Anggota Polri.



VIII. LESSON LEARNT (PEMBELAJARAN KEPEMIMPINAN)

Dalam rangka mewujudkan tujuan dari Proyek Perubahan, Project Leader menemukan adanya tantangan, baik yang datang dari internal maupun eksternal organisasi. Tantangan utama yang dihadapi adalah adanya kasus kebocoran data yang sedang trending yaitu Bjorka, sehingga hal ini cukup menyita energi dan waktu dari personil yang selama ini menangani keamanan siber, yang tentunya kebanyakan merupakan narasumber dalam penyusunan proyek perubahan ini. Disamping itu, adanya hajatan Nasional dimana Indonesia akan menyelenggarakan kegiatan G20, tentu memerlukan pengamanan ekstra terhadap seluruh jaringan teknologi, informasi dan komunikasi sehingga tidak akan mengganggu pelaksanaan jalannya kegiatan G20 tersebut. Personil yang terbatas, padatnya jadwal rapat baik dari internal maupun dari luar unit kerja, beberapa penugasan untuk mewakili pimpinan dalam beberapa forum atau event. Hal ini tentu memerlukan strategi mengatasi beberapa hambatan yang muncul supaya tantangan tersebut dapat dilaksanakan oleh project leader dan menjadi faktor kunci keberhasilan dalam sebuah organisasi. Beberapa strategi kepemimpinan digunakan (sifat tindakan yang mempunyai cakupan/lingkup dampak yang luas dalam organisasi) dan diharapkan tindakan tersebut menjadi pengungkit (leverage) bagi organisasi.

Seperti halnya pembentukan tim efektif : (1) Tim dibentuk untuk memecahkan setiap masalah yang bersifat jangka pendek, yang tidak mampu atau pun sulit dipecahkan oleh unit kerja, fungsi, dan peran kerja yang permanen dalam struktur organisasi. (2) Tim yang berkualitas

membutuhkan kombinasi keterampilan, pengalaman, emosional, pengetahuan, kecerdasan, dan energi yang saling bersinergi dan melengkapi. (3) Tim yang berkualitas akan selalu sadar bahwa keberadaan mereka di dalam tim adalah untuk mendukung semua unit kerja, peran kerja, fungsi kerja, dan aspek kerja di dalam struktur organisasi manajemen.

Selanjutnya pengungkit (leverage) adalah suatu tindakan sebagai dongkrak atau daya ungkit yaitu tindakan yang kecil, ringan tetapi mempunyai dampak luas pada organisasi dan mendorong organisasi pada level unggul dalam persaingan. Keberhasilan organisasi dalam mencapai kinerja organisasi bergantung pada faktor manajemen dan faktor manusia. Manusia sebagai performer dalam suatu organisasi/manajemen khususnya pada struktur organisasi profesional akan menjadi faktor kunci keberhasilan dalam suatu organisasi. Aspek kepemimpinan sumber daya manusia dalam suatu organisasi merupakan faktor kunci bagi kelangsungan aktivitas suatu organisasi karena pada hakekatnya di dalam organisasi itu sendiri terjadi proses kerjasama antar manusia untuk mencapai tujuan dari organisasi.

Begitu halnya dengan proses proyek perubahan strategi peningkatan pelayanan di bidang manajemen keamanan siber, faktor kunci keberhasilannya untuk mencapai kinerja organisasi yang efektif dan efisien dengan pelayanan publik yang lebih baik tertumpu pada kemauan untuk mewujudkan komitmen yang telah disepakati walaupun dengan kondisi jumlah personil yang terbatas tetapi dapat mewujudkan tujuan dari proyek perubahan ini.

Dari uraian yang telah di sampaikan pada bab sebelumnya, proyek perubahan ini memiliki tujuan untuk meningkatkan keamanan siber di lingkungan internal BSSN. Harapan yang ingin diwujudkan adalah semakin banyak stakeholder yang melakukan penilaian risiko keamanan siber di unit kerjanya masing-masing. Untuk semakin meningkatkan kebermanfaatannya bisa di ikuti kesimpulan dan rekomendasi di bawah ini.

Leasson Learn dari Proyek Perubahan “Optimalisasi Pusdatik Dalam Melakukan Manajemen Risiko Sistem Pemerintah Berbasis Elektronik di Lingkungan Badan Siber dan Sandi Negara” ini adalah :

- Cara berpikir lebih strategis
- Mampu menganalisa lingkungan dan pemetaan masalah
- Mampu memimpin staf yang memiliki keahlian yang beragam
- Mampu mengembangkan diri untuk menjadi lebih baik
- Mampu berkomunikasi lebih baik dengan atasan dan bawahan

BAB III

PENUTUP

I. SIMPULAN

1. Proyek perubahan ini berangkat dari permasalahan akibat rendahnya nilai indeks SPBE BSSN yang diberikan oleh KemenpanRB dan juga adanya kekhawatiran akibatnya banyaknya kasus serangan siber ataupun pencurian data yang terjadi akhir akhir ini terutama di lingkungan instansi pemerintahan.
2. Rendahnya nilai indeks SPBE ini salah satunya disebabkan karena Pusdatik BSSN belum dapat melakukan manajemen risiko SPBE di lingkungan BSSN. Pusdatik belum dapat melakukan kegiatan manajemen risiko karena belum didukung adanya aturan sebagai pijakannya. Oleh karena itu perlu upaya untuk mengoptimalkan fungsi Pusdatik dalam melakukan manajemen risiko.
3. Optimalisasi Fungsi Pusdatik BSSN dalam rangka melakukan manajemen risiko Sistem Pemerintahan Berbasis Elektronik ini di BSSN diwujudkan dalam bentuk penyusunan Peraturan Kepala BSSN tentang pedoman manajemen risiko SPBE, pembuatan Standar Operasional Prosedur dan Petunjuk Teknis tentang Penilaian Risiko serta dengan melakukan peningkatan kemampuan pegawai melalui pelatihan, penambahan sarana prasarana dan juga sosialisasi yang tepat sasaran kepada setiap stakeholder.
4. Keberhasilan pencapaian Jangka Pendek dalam implementasi Proyek Perubahan saat ini yaitu tercapainya pembentukan tim

efektif yang terdiri dari tim teknis dan tim administrasi, tersusunnya Draft Peraturan Kepala BSSN tentang pedoman manajemen risiko SPBE, pembuatan Standar Operasional Prosedur dan Petunjuk Teknis tentang Penilaian Risiko, Peningkatan kemampuan pegawai, Penambahan sarana prasarana dan sosialisasi.

5. Kegiatan implementasi Proyek Perubahanan ini dapat berjalan dengan baik dan lancar setelah mendapatkan materi materi pendukung dari widyaiswara, visitasi (study Banding), dukungan para stakeholder, tim efektif yang berintegritas dan memiliki kompetensi teknis dan dukungan dari mentor dan coach menjadi bagian yang terintegrasi dalam pencapaian implementasi proper ini

II. REKOMENDASI

1. Setiap proyek perubahan yang sifatnya jangka panjang memerlukan pendampingan-pendampingan sejak awal, baik sosialisasi dan advokasi demi kesuksesan dari program proyek perubahan. Terlebih lagi yang berhubungan dengan pembuatan peraturan yang terkait dengan sistem Teknologi Informasi dan Komunikasi yang akan berdampak kepada perubahan budaya kerja. Untuk itu Komunikasi dan koordinasi dengan setiap stakeholdres terkait harus tetap dipertahankan.
2. Proyek perubahan jangka pendek yang kiranya sudah berhasil dilakukan harus bisa dilanjutkan dengan capaian untuk jangka menengah dan jangka panjang. Kesemuanya harus didukung dengan anggaran yang jelas dan pembangunan Sumber Daya

Manusia pendukung serta persiapan budaya kerja yang baru tersebut.

3. Hal yang sering terlupakan dalam manajemen risiko sistem pemerintahan berbasis elektronik adalah pemastian agar Sumber Daya Manusia internal atau pihak yang diberi wewenang bisa memelihara sistem yang sudah terbangun melalui transfer knowledge. Sehingga sistem Teknologi Informasi dan Komunikasi tersebut akan terus berjalan dengan lebih baik dan terhindar dari upaya terjadinya serangan siber ataupun kebocoran data.

DAFTAR PUSTAKA

- Peraturan Presiden Nomor 53 tahun 2017 tanggal 23 Mei 2017 tentang Badan Siber dan Sandi Negara.
- Peraturan Presiden Nomor 133 tahun 2017 tanggal 16 Desember 2017 tentang Perubahan Atas Peraturan Presiden Nomor 53 tahun 2017 tentang Badan Siber dan Sandi Negara.
- Peraturan Presiden Nomor 28 tahun 2021 tentang Badan Siber dan Sandi Negara.
- Peraturan Badan Siber dan Sandi Negara Nomor 6 tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara.
- Peraturan Presiden Nomor 95 Tahun 2018, tentang Sistem Pemerintahan Berbasis Elektronik (SPBE).
- Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 59 Tahun 2020 tentang Pemantauan Dan Evaluasi Sistem Pemerintahan Berbasis Elektronik.
- Rencana Strategis (Renstra) Badan Siber dan Sandi Negara Tahun 2020-2024 yang memuat visi, misi, tujuan, kebijakan, program, dan kegiatan indikatif sesuai dengan tugas dan fungsi BSSN.
- Laporan Hasil Evaluasi Sistem Pemerintahan Berbasis Elektronik dari Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi tanggal 29 Desember 2021 tentang Indeks SPBE Tahun 2021 Badan Siber dan Sandi Negara.
- Stavros, J., Cooperrider, D., & Kelly, D. 2003. Strategic Inquiry - Appreciative intent : Inspirationto SOAR. Al Practioner.

- Peter Sange, 1990. The Fifth Discipline : The art, and Practice Learning Organization.
- Garvin, D.A, 1993. Building Learning Organization.
- Muhammad Basri Wello dan Lely Novia, 2021, Developing Interpersonal Skills (Mengembangkan Keterampilan Antarpribadi)
- Drs. Catur Sumar Sri Susatyo Dan Dr. Makhdum Priyatno, M.A, LAN Jakarta, 2021. Modul Resmi Pelatihan Kepemimpinan Nasional Tingkat II, Energi Kepemimpinan
- Drs. Wiryanta Muljono, Ma., Ph.D, LAN Jakarta, 2021, Modul Resmi Pelatihan Kepemimpinan Nasional Tingkat II, Kepemimpinan Digital
- Gatot Widayanto, LAN Jakarta, 2021, Modul Resmi Pelatihan Kepemimpinan Nasional Tingkat II, Kepemimpinan Kewirausahaan
- Dr. Hary Supriadi, S.H., M.A., LAN Jakarta, 2021, Modul Resmi Pelatihan Kepemimpinan Nasional Tingkat II, Organisasi Pembelajaran (Learning Organization)
- Tatang Muttaqin, Ph.D., LAN Jakarta, 2021. Modul Resmi Pelatihan Kepemimpinan Nasional Tingkat II, Manajemen Strategis Sektor Publik
- Dr. Hary Supriadi, S.H., M.A., LAN Jakarta, 2021. Modul Resmi Pelatihan Kepemimpinan Nasional Tingkat II, Marketing Sektor Publik
- Erna Irawati, S.Sos., M.Pol.Adm, LAN Jakarta, 2021. Modul Resmi Pelatihan Kepemimpinan Nasional Tingkat II, Isu Strategis
- Reghi Perdana, Sh, LLM, LAN Jakarta, 2021. Modul Resmi Pelatihan Kepemimpinan Nasional Tingkat II, Public Private Partnerships
- Erna Irawati, LAN Jakarta, 2021. Modul Resmi Pelatihan Kepemimpinan Nasional Tingkat II, Membuat Policy Brief Yang Efektif

- Modul Proyek Perubahan Pelatihan Kepemimpinan Nasional Tingkat II, Jakarta, 2021
- Prof. Dr. Eko Prasjo, Mag.rer.publ, Prenada Media Group, Jakarta, Memimpin Reformasi Birokrasi : Kompleksitas dan Dinamika Perubahan Birokrasi Indonesia.
- Priyantono Rudito, Ph.D dan Mardi F.N. Sinaga, MBA, Gramedia Jakarta, Digital Mastery : Membangun Kepemimpinan Digital untuk Memenangkan Era Disrupsi.
- John C. Maxwell, MIC Publishing, The Power of Your Leadership : Membuat Perbedaan Bersama Orang Lain.
- <https://pantura.inews.id/read/61805/10-serangan-cyber-terbesar-dalam-sejarah-ada-kasus-data-77-juta-pengguna-playstation-sony-hilang> tentang 10 Serangan Cyber Terbesar Dalam Sejarah, Ada Kasus Data 77 Juta Pengguna PlayStation Sony Hilang!
- <https://www.suara.com/tekno/2022/01/01/015822/daftar-kasus-kebocoran-data-di-indonesia-selama-2021-termasuk-sertifikat-vaksin-jokowi> tentang Daftar Kasus Kebocoran Data di Indonesia selama 2021, Termasuk Sertifikat Vaksin Jokowi
- <https://tekno.sindonews.com/read/585678/207/situs-bssn-diretas-hacker-amatir-pengamat-mike-tyson-ko-lawan-preman-pasar-1635732672> tentang Situs BSSN Diretas Hacker Amatir, Pengamat: Mike Tyson KO Lawan Preman Pasar
- <https://www.kompas.com/tren/read/2021/10/26/133000565/situs-milik-bssn-dibobol-peretas-ini-analisis-dan-saran-pengamat-siber?page=all> tentang Situs Milik BSSN Dibobol Peretas, Ini Analisis dan Saran Pengamat Siber
- <https://www.cnnindonesia.com/teknologi/20220201080620-185-753619/situs-bssn-diserang-lagi-data-jdih-bocor> tentang Situs BSSN Diserang Lagi, Data JDIH Bocor

- <https://tekno.kompas.com/read/2022/01/31/14505097/data-situs-jdih-bssn-diduga-bocor-dan-dibagikan-gratis-di-internet?page=all>. tentang Data Situs JDIH BSSN Diduga Bocor dan Dibagikan Gratis di Internet
- <https://www.cnnindonesia.com/teknologi/20220124163634-185-750569/kebocoran-data-bank-indonesia-belum-selesai-naik-jadi-74gb> tentang Kebocoran Data Bank Indonesia Belum Selesai, Naik Jadi 74GB
- <https://www.cnbcindonesia.com/tech/20220912164038-37-371426/hacker-bjorka-klaim-bobol-data-ri-datanya-asli> tentang Hacker Bjorka Klaim Bobol data RI, Datanya Asli?
- <https://www.beritasatu.com/news/977225/pemerintah-berupaya-jaga-data-pribadi-di-pusaran-bjorka> tentang Pemerintah Berupaya Jaga Data Pribadi di Pusaran Bjorka
- <https://www.liputan6.com/citizen6/read/5067854/11-fakta-hacker-bjorka-yang-retas-data-pemerintah-indonesia> tentang 11 Fakta Hacker Bjorka yang Retas Data Pemerintah Indonesia

LAMPIRAN-LAMPIRAN

LAMPIRAN 1

DRAFT PERATURAN

KEPALA BADAN SIBER DAN SANDI NEGARA

TENTANG MANAJEMEN RISIKO

SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK



DRAFT PERATURAN
KEPALA BADAN SIBER DAN SANDI NEGARA
TAHUN 2022

TENTANG
PEDOMAN MANAJEMEN RISIKO
SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK
BADAN SIBER DAN SANDI NEGARA

BAB I
PENDAHULUAN

A. Umum

Badan Siber dan Sandi Negara (BSSN) sebagai bagian dari institusi pemerintahan diberikan tugas pokok dan fungsi serta kewenangan untuk mengolaborasi dan elaborasikan seluruh sumber daya dalam rangka pengelolaan dan pengendalian ruang siber Indonesia, untuk maksud melindungi kedaulatan bangsa dan negara, terlebih seluruh warga negara Indonesia. Transformasi Lemsaneg menjadi BSSN tertuang dalam Peraturan Presiden Republik Indonesia Nomor 53 Tahun 2017 sebagaimana telah diubah dengan Peraturan Presiden Republik Indonesia Nomor 133 Tahun 2017 tentang Perubahan Atas Peraturan Presiden Nomor 53 Tahun 2017, yang kemudian diperbaharui kembali dengan Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara. Dalam rangka menjalankan tugas pokoknya untuk melakukan pengelolaan terhadap kebutuhan keamanan siber di tanah air, maka melalui Rencana Strategis BSSN tahun 2020-2024

dan Peraturan Kepala Badan Siber dan Sandi Negara Nomor 175.1 Tahun 2018 BSSN berkomitmen untuk melaksanakan layanan-layanan yang spesifik sesuai dengan strategi nasional yang telah ditetapkan.

Dalam pertumbuhannya pelaksanaan tugas BSSN melibatkan penyediaan layanan yang handal dan profesional terkait keamanan siber dan persandian negara. Namun demikian inovasi dan peningkatan dalam penyediaan layanan harus dilakukan secara berkelanjutan (*continual improvement*), tidak hanya untuk memenuhi kebutuhan namun juga untuk memberikan nilai (*value delivery*) bagi peri-kehidupan berbangsa dan bernegara. Layanan yang efektif dan efisien serta memenuhi ekspektasi pengguna merupakan suatu *objectives* yang menjadi acuan pengembangan kebijakan dan atau operasional. Integrasi Layanan Publik BSSN adalah inovasi dalam upaya pencapaian tujuan dimaksud.

B. Maksud dan Tujuan

1. Maksud

Maksud dari Pedoman Teknis Manajemen Risiko SPBE ini adalah untuk memberikan panduan bagi unit kerja di lingkungan Badan Siber dan Sandi Negara dalam melaksanakan Manajemen Risiko SPBE di lingkungannya.

2. Tujuan

- a. Meningkatkan kemungkinan pencapaian tujuan penerapan SPBE di unit kerja lingkup Badan Siber dan Sandi Negara;
- b. Memberikan dasar yang kuat untuk perencanaan dan pengambilan keputusan melalui penyajian informasi Risiko SPBE yang memadai di BSSN dalam penerapan SPBE;
- c. Meningkatkan optimalisasi pemanfaatan dan sumber daya SPBE di BSSN dalam penerapan SPBE;
- d. Meningkatkan kepatuhan terhadap peraturan dalam penerapan SPBE; dan
- e. Menciptakan budaya sadar Risiko SPBE bagi pegawai ASN di lingkungan BSSN.

C. Landasan Hukum

1. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 112);
2. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 5 Tahun 2020 tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik;
3. Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara;
4. Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara.

D. Manfaat Manajemen Risiko SPBE

1. Mewujudkan tata kelola pemerintahan yang efektif, efisien, transparan, dan akuntabel melalui penerapan SPBE di BSSN;
2. Mewujudkan penerapan SPBE yang terpadu di BSSN;
3. Meningkatkan kinerja pemerintahan di BSSN;
4. Meningkatkan reputasi dan kepercayaan pemangku kepentingan kepada BSSN; dan
5. Mewujudkan budaya kerja yang profesional dan berintegritas di BSSN.

E. Ruang Lingkup Manajemen Risiko SPBE

Ruang Lingkup Pedoman Manajemen Risiko SPBE yang menjadi fokus pembahasan mencakup:

1. Kerangka Kerja Manajemen Risiko SPBE;
2. Proses Manajemen Risiko SPBE;
3. Struktur Manajemen Risiko SPBE;
4. Budaya Sadar Risiko SPBE.

F. Pengertian Umum SPBE

1. Manajemen Risiko SPBE adalah pendekatan sistematis yang meliputi proses, pengukuran, struktur, dan budaya untuk menentukan tindakan terbaik terkait Risiko SPBE.

2. Risiko SPBE adalah peluang terjadinya suatu peristiwa yang akan mempengaruhi keberhasilan terhadap pencapaian tujuan penerapan SPBE.
3. Risiko SPBE Positif adalah peluang terjadinya suatu peristiwa yang akan meningkatkan keberhasilan terhadap pencapaian tujuan penerapan SPBE.
4. Risiko SPBE Negatif adalah peluang terjadinya suatu peristiwa yang akan menurunkan keberhasilan terhadap pencapaian tujuan penerapan SPBE.
5. Kategori Risiko SPBE adalah pengelompokan Risiko SPBE berdasarkan karakteristik penyebab Risiko SPBE yang menggambarkan seluruh jenis Risiko SPBE yang terdapat pada Instansi Pusat dan Pemerintah Daerah.
6. Area Dampak Risiko SPBE adalah pengelompokan area yang terkena dampak dari Risiko SPBE.
7. Kriteria Risiko SPBE adalah parameter atau ukuran secara kuantitatif atau kualitatif yang digunakan untuk menentukan Kriteria Kemungkinan Risiko SPBE dan Kriteria Dampak Risiko SPBE.
8. Kriteria Kemungkinan Risiko SPBE adalah besarnya peluang terjadinya suatu Risiko SPBE dalam periode tertentu.
9. Kriteria Dampak Risiko SPBE adalah besarnya akibat terjadinya suatu Risiko SPBE yang mempengaruhi sasaran SPBE.
10. Besaran Risiko SPBE adalah nilai Risiko SPBE yang dihasilkan dari proses analisis Risiko SPBE.
11. Level Risiko SPBE adalah pengelompokan Besaran Risiko SPBE yang mendeskripsikan tingkat Risiko SPBE.
12. Selera Risiko SPBE adalah penentuan Besaran Risiko SPBE di BSSN yang dapat diterima atau ditangani.
13. Program Kerja adalah rencana kegiatan yang disusun secara bersama untuk dilaksanakan dalam jangka waktu yang ditentukan berdasarkan peraturan yang berlaku guna mencapai tujuan organisasi.
14. Pengguna Layanan adalah merupakan individu, masyarakat, kelompok, organisasi pemerintah maupun swasta yang menggunakan layanan publik BSSN dalam melaksanakan kegiatan operasional.

15. Pemohon Layanan adalah merupakan individu, masyarakat, kelompok, atau organisasi pemerintah maupun swasta yang mengajukan permohonan layanan yang disediakan oleh BSSN.
16. Unit Layanan merupakan unit kerja yang memberikan pelayanan terhadap para stakeholder yang membutuhkan layanan publik BSSN.
17. Administrator Pengelola Administrasi Pelayanan (Admin Level 1) adalah pegawai yang melakukan pengelolaan permohonan layanan dan melakukan koordinasi dengan pemohon layanan.
18. Administrator Penyelenggara Pelayanan (Admin Level 2) adalah pejabat administrator atau pengawas yang melakukan persetujuan terhadap permohonan layanan publik dari pemohon layanan.

G. Sistematika Pedoman SPBE

Sistematika Pedoman Manajemen Risiko SPBE disusun dalam 5 (lima) bab, yaitu:

- Bab I Pendahuluan
Pendahuluan memuat latar belakang, maksud dan tujuan, manfaat, ruang lingkup, dan pengertian umum;
- Bab II Kerangka Kerja Manajemen Risiko SPBE
Memuat deskripsi komponen-komponen dasar yang menyusun kerangka kerja tersebut;
- Bab III Proses Manajemen Risiko SPBE
Memuat proses komunikasi dan konsultasi, penetapan konteks Risiko SPBE, penilaian Risiko SPBE, penanganan Risiko SPBE, pencatatan dan pelaporan, serta pemantauan dan evaluasi;
- Bab IV Struktur Manajemen dan Budaya Sadar Risiko SPBE
Memuat tugas dan fungsi dari struktur Manajemen Risiko SPBE dan pelaksanaan pembangunan budaya sadar Risiko SPBE; dan.
- Bab V Penutup
Memuat ringkasan pedoman Manajemen Risiko SPBE.

BAB II

KERANGKA KERJA MANAJEMEN RISIKO SPBE

Kerangka kerja Manajemen Risiko SPBE mendeskripsikan komponen dasar yang digunakan sebagai landasan penerapan Manajemen Risiko SPBE di BSSN. Tujuan dari kerangka kerja Manajemen Risiko SPBE adalah untuk membantu Instansi Pusat dan Pemerintah Daerah dalam mengintegrasikan Manajemen Risiko SPBE ke dalam kegiatan pelaksanaan tugas dan fungsi Instansi Pusat dan Pemerintah Daerah. Agar Manajemen Risiko SPBE dapat dilaksanakan dengan baik, Instansi Pusat dan Pemerintah Daerah dapat mengadopsi secara langsung atau memodifikasi kerangka kerja Manajemen Risiko SPBE ini sesuai dengan konteks internal dan eksternal di lingkungannya masing-masing.

Komponen dasar dari kerangka kerja ini terdiri atas prinsip mengenai peningkatan nilai dan perlindungan, kepemimpinan dan komitmen, serta proses dan tata kelola Manajemen Risiko SPBE sebagaimana terlihat pada Gambar 1.



Gambar 1. Kerangka Kerja Manajemen Risiko SPBE

A. Peningkatan Nilai dan Perlindungan

Prinsip utama dari penerapan Manajemen Risiko SPBE adalah menciptakan peningkatan nilai tambah dan perlindungan bagi BSSN dalam penerapan SPBE. Prinsip utama tersebut memiliki karakteristik sebagai berikut:

1. Terintegrasi, yaitu Manajemen Risiko SPBE merupakan serangkaian proses yang terintegrasi dengan proses pelaksanaan tugas dan fungsi BSSN;
2. Terstruktur dan komprehensif, yaitu Manajemen Risiko SPBE dibangun secara terstruktur, sistematis, dan menyeluruh untuk memberikan kontribusi terhadap efisiensi dan konsistensi hasil yang dapat diukur dalam peningkatan kualitas penerapan SPBE;
3. Dapat disesuaikan, yaitu kerangka kerja dan proses Manajemen Risiko SPBE dapat disesuaikan dengan konteks internal dan eksternal BSSN dalam penerapan SPBE;
4. Inklusif, yaitu Manajemen Risiko SPBE melibatkan semua pemangku kepentingan sesuai dengan pengetahuan, pandangan, dan persepsinya untuk membangun budaya sadar Risiko SPBE di BSSN;
5. Dinamis, yaitu Manajemen Risiko SPBE dapat dipergunakan untuk mengantisipasi dan merespon perubahan konteks BSSN dengan tepat dan sesuai waktu;
6. Informasi tersedia dan terbaik, yaitu informasi yang digunakan sebagai masukan dalam proses Manajemen Risiko SPBE didasarkan pada data historis, pengalaman, observasi, perkiraan, penilaian ahli, dan data dukung lain yang tersedia di BSSN;
7. Faktor manusia dan budaya, yaitu keberhasilan penerapan Manajemen Risiko SPBE di BSSN dipengaruhi oleh kapasitas, persepsi, kesungguhan, dan budaya kerja dari pegawai ASN yang terlibat dalam penerapan SPBE; dan
8. Perbaikan berkelanjutan, yaitu Manajemen Risiko SPBE senantiasa dikembangkan melalui strategi perbaikan manajemen secara berkelanjutan dan peningkatan kematangan penerapan Manajemen Risiko SPBE.

B. Kepemimpinan dan Komitmen

Pimpinan BSSN hendaknya menunjukkan kepemimpinan dan komitmen dalam penerapan kerangka kerja Manajemen Risiko SPBE melalui proses:

1. Integrasi

Kerangka kerja Manajemen Risiko SPBE hendaknya diintegrasikan dengan proses pelaksanaan tugas dan fungsi Instansi Pusat dan Pemerintah Daerah. Integrasi dapat dilakukan dengan memahami struktur dan konteks organisasi yang didasarkan pada tujuan, sasaran, dan kompleksitas organisasi.

Berdasarkan struktur dan konteks organisasi tersebut, tata kelola Manajemen Risiko SPBE perlu dibangun dengan menyusun struktur Manajemen Risiko SPBE beserta tugas-tugasnya untuk menjalankan, mengendalikan, dan melakukan pengawasan terhadap penerapan proses Manajemen Risiko SPBE dalam rangka mencapai sasaran dan target kinerja organisasi dalam penerapan SPBE.

2. Desain

Perancangan kerangka kerja Manajemen Risiko SPBE dilakukan dengan cara:

- a. Memahami struktur dan konteks organisasi termasuk tujuan, sasaran, dan kompleksitas organisasi;
- b. Mengekspresikan komitmen pimpinan terhadap penerapan kerangka kerja Manajemen Risiko SPBE dalam bentuk kebijakan, pernyataan, atau bentuk dukungan lainnya;
- c. Menetapkan kewenangan, tanggung jawab, dan akuntabilitas dari setiap peran di dalam kerangka kerja Manajemen Risiko SPBE;
- d. Menyediakan sumber daya yang diperlukan seperti SDM dan kompetensi, anggaran, proses dan prosedur, informasi dan pengetahuan, dan pelatihan; dan
- e. Membangun komunikasi dan konsultasi untuk efektivitas implementasi kerangka kerja Manajemen Risiko SPBE.

3. Implementasi

Kerangka kerja Manajemen Risiko SPBE diterapkan dengan melibatkan semua pemangku kepentingan di Instansi Pusat dan Pemerintah Daerah melalui penyusunan rencana, penyediaan sumber daya, pembuatan keputusan, dan pelaksanaan Manajemen Risiko SPBE.

4. Pemantauan dan Evaluasi

Untuk mengukur efektivitas implementasi kerangka kerja Manajemen Risiko SPBE, pimpinan Instansi Pusat dan Pemerintah Daerah perlu melakukan pemantauan dan evaluasi secara berkala untuk pengukuran kinerja dan kesesuaian kerangka kerja Manajemen Risiko SPBE terhadap tujuan dan sasaran SPBE.

5. Perbaikan

Hasil pemantauan dan evaluasi kerangka kerja Manajemen Risiko SPBE digunakan untuk melakukan perubahan dan perbaikan kerangka kerja Manajemen Risiko SPBE secara berkelanjutan sehingga kesesuaian, kecukupan, dan efektivitas dari kerangka kerja tersebut dapat ditingkatkan.

C. Proses dan Tata Kelola Manajemen Risiko SPBE

Proses Manajemen Risiko SPBE merupakan rangkaian proses yang sistematis dan menjadi bagian dari proses pelaksanaan tugas dan fungsi BSSN untuk pengambilan keputusan di tingkat strategis, operasional, dan pelaksanaan proyek. Proses Manajemen Risiko SPBE yang dilaksanakan oleh BSSN terdiri atas proses:

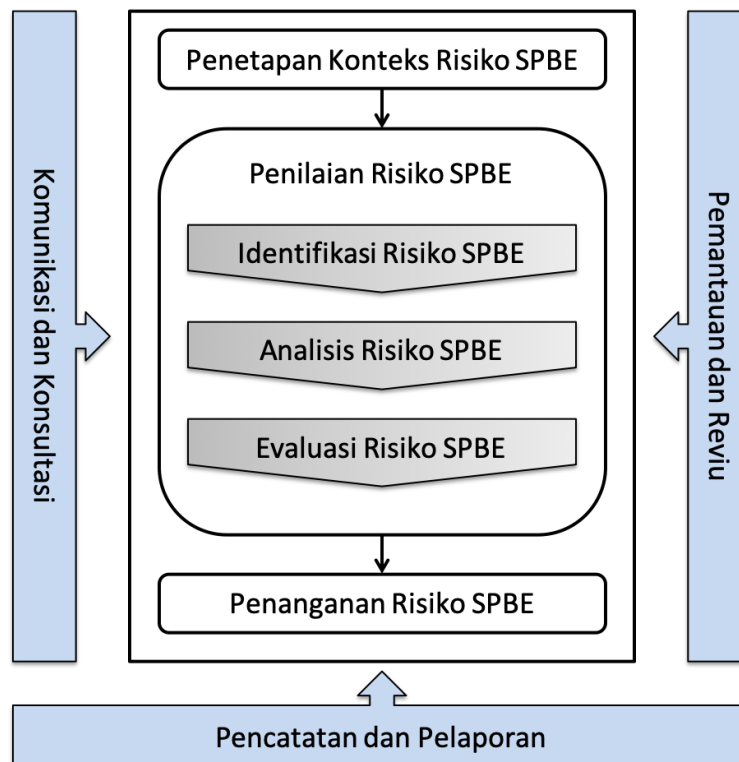
1. Komunikasi dan konsultasi;
2. Penetapan konteks Risiko SPBE;
3. Penilaian Risiko SPBE yang terdiri atas identifikasi Risiko SPBE, analisis Risiko SPBE, dan evaluasi Risiko SPBE;
4. Penanganan Risiko SPBE;
5. Pemantauan dan revidi;
6. Pencatatan dan pelaporan.

Sedangkan, tata kelola Manajemen Risiko SPBE merupakan mekanisme untuk mengatur kewenangan dan memastikan akuntabilitas pelaksanaan Manajemen Risiko SPBE di Instansi Pusat dan Pemerintah Daerah. Dalam hal ini, tata kelola Manajemen Risiko SPBE dibangun dengan menyusun struktur Manajemen Risiko SPBE dan membangun budaya sadar Risiko SPBE. Struktur Manajemen Risiko SPBE di Instansi Pusat dan Pemerintah Daerah sedikitnya terdiri atas fungsi yang terkait dengan strategi dan kebijakan, pelaksanaan, dan pengawasan Manajemen Risiko SPBE. Selain itu, budaya sadar Risiko SPBE perlu dibangun dan dikembangkan oleh BSSN melalui perencanaan, pelaksanaan, dan pemantauan dan evaluasi kegiatan budaya sadar Risiko SPBE.

BAB III

PROSES MANAJEMEN RISIKO SPBE

Proses Manajemen Risiko SPBE merupakan penerapan secara sistematis dari kebijakan, prosedur, dan praktik terhadap aktivitas komunikasi dan konsultasi, penetapan konteks, penilaian risiko (identifikasi risiko, analisis risiko, evaluasi risiko), penanganan risiko, pemantauan dan revidu, serta pencatatan dan pelaporan. Proses Manajemen Risiko SPBE diilustrasikan pada Gambar 2.



Gambar 2. Proses Manajemen Risiko

A. Komunikasi dan Konsultasi

Komunikasi dan konsultasi merupakan proses yang berkelanjutan dan berulang untuk menyediakan, membagikan, ataupun mendapatkan informasi dan menciptakan dialog dengan para pemangku kepentingan mengenai Risiko SPBE. Komunikasi dilakukan untuk meningkatkan kesadaran dan pemahaman mengenai Risiko SPBE. Sementara konsultasi dilakukan untuk mendapatkan umpan balik dan informasi dalam rangka mendukung pengambilan keputusan.

Bentuk kegiatan komunikasi dan konsultasi antara lain:

1. Rapat berkala, merupakan rapat yang diadakan secara rutin;
2. Rapat insidental, merupakan rapat yang diadakan sewaktu-waktu; dan
3. *Focus Group Discussion* (FGD), merupakan kelompok diskusi yang terarah untuk membahas topik tertentu

B. Penetapan Konteks Risiko SPBE

Penetapan konteks Risiko SPBE bertujuan untuk mengidentifikasi parameter dasar dan ruang lingkup penerapan Risiko SPBE yang harus dikelola dalam proses Manajemen Risiko SPBE. Tahapan penetapan konteks meliputi:

1. Inventarisasi Informasi Umum

Inventarisasi informasi umum bertujuan untuk mendapatkan gambaran umum mengenai unit kerja yang menerapkan Manajemen Risiko SPBE. Informasi yang dicantumkan meliputi nama Unit Pemilik Risiko (UPR) SPBE, tugas UPR SPBE, fungsi UPR SPBE, dan periode waktu pelaksanaan Manajemen Risiko SPBE dalam kurun waktu satu tahun. Informasi umum dituangkan ke dalam Formulir 2.1 seperti terlihat pada Tabel 1 di bawah ini.

Tabel 1

Contoh Pengisian Formulir 2.1 Informasi Umum

Informasi Umum	
Nama UPR SPBE	Deputi Bidang Kelembagaan dan Tata Laksana
Tugas UPR SPBE	Menyelenggarakan perumusan kebijakan serta koordinasi dan sinkronisasi pelaksanaan kebijakan di bidang kelembagaan dan ketatalaksanaan pemerintah
Fungsi UPR SPBE	1. perumusan kebijakan di bidang kelembagaan pemerintahan 2. perumusan kebijakan di bidang ketatalaksanaan pemerintahan, penyelenggaraan administrasi pemerintahan, dan pengembangan penerapan sistem pemerintahan berbasis elektronik
Periode Waktu	1 Januari - 31 Desember 2022

2. Identifikasi Sasaran SPBE

Identifikasi sasaran SPBE bertujuan untuk menentukan sasaran SPBE beserta indikator dan targetnya yang mendukung sasaran unit kerja sebagai UPR SPBE. Informasi yang dicantumkan meliputi:

- a. Sasaran UPR SPBE, diisi dengan sasaran unit kerja sebagai UPR SPBE yang tertuang dalam dokumen rencana strategis, rencana kerja, penetapan kinerja, atau dokumen perencanaan lainnya;
- b. Sasaran SPBE, diisi dengan sasaran SPBE yang mendukung sasaran UPR SPBE;
- c. Indikator Kinerja SPBE, diisi dengan indikator kinerja SPBE yang mendeskripsikan pencapaian sasaran SPBE; dan
- d. Target Kinerja SPBE, diisi dengan target kinerja SPBE yang mendeskripsikan ukuran indikator kinerja untuk pencapaian sasaran SPBE.

Informasi sasaran SPBE dituangkan ke dalam Formulir 2.2 seperti terlihat pada Tabel 2 di bawah ini.

Tabel 2
Contoh Pengisian Formulir 2.2 Sasaran SPBE

No	Sasaran UPR SPBE	Sasaran SPBE	Indikator Kinerja SPBE	Target Kinerja SPBE
1	Terwujudnya tata kelola pemerintahan yang berbasis elektronik	Meningkatnya kualitas penyelenggaraan Sistem Pemerintahan Berbasis Elektronik	Indeks SPBE Nasional	3,5
			Jumlah Instansi Pemerintah yang mencapai predikat SPBE "Baik"	121 IP

3. Penentuan Struktur Pelaksana Manajemen Risiko SPBE

Penentuan struktur pelaksana Manajemen Risiko SPBE bertujuan untuk menentukan unit kerja yang bertanggung jawab atas pelaksanaan Manajemen Risiko SPBE. Penentuan struktur pelaksana Manajemen Risiko SPBE meliputi:

- a. Unit Pemilik Risiko SPBE;
- b. Pemilik Risiko SPBE;
- c. Koordinator Risiko SPBE; dan
- d. Pengelola Risiko SPBE.

Informasi struktur pelaksana Manajemen Risiko SPBE dituangkan ke dalam Formulir 2.3 seperti terlihat pada Tabel 3 di bawah ini.

Tabel 3
Contoh Pengisian Formulir 2.3
Struktur Pelaksana Manajemen Risiko SPBE

Struktur Pelaksana Manajemen Risiko SPBE	
Pemilik Risiko SPBE	Sekretaris Utama Badan Siber dan Sandi Negara
Koordinator Risiko SPBE	Kepala Pusat Data dan Teknologi Informasi Komunikasi
Pengelola Risiko SPBE	Koordinator Kelompok Manajemen Risiko dan Kelangsungan TIK

4. Identifikasi Pemangku Kepentingan

Identifikasi pemangku kepentingan bertujuan untuk mendapatkan informasi dan memahami pihak-pihak yang melakukan interaksi dengan UPR SPBE dalam rangka pencapaian sasaran SPBE. Pihak-pihak tersebut meliputi unit kerja internal, unit kerja eksternal, instansi pemerintah, atau non instansi pemerintah. Hubungan kerja antara UPR SPBE dan setiap pihak pemangku kepentingan yang terkait dengan penerapan SPBE perlu dideskripsikan dengan jelas. Daftar pemangku kepentingan dituangkan ke dalam Formulir 2.4 seperti terlihat pada Tabel 4 di bawah ini.

Tabel 4

Contoh Pengisian Formulir 2.4 Daftar Pemangku Kepentingan

No	Nama Unit/Instansi	Hubungan
1	Perguruan Tinggi (UI, UGM, PENS, Tel-U, UG)	Pelaksana evaluasi SPBE sebagai evaluator eksternal
2	Badan Siber dan Sandi Negara	Penyedia layanan repositori data evaluasi SPBE

5. Identifikasi Peraturan Perundang-Undangan

Identifikasi peraturan perundang-undangan bertujuan untuk memahami kewenangan, tanggung jawab, tugas dan fungsi, serta kewajiban hukum yang harus dilaksanakan oleh UPR SPBE. Informasi yang perlu dijelaskan dalam melakukan identifikasi peraturan perundang-undangan meliputi nama peraturan dan amanat dalam peraturan tersebut. Daftar peraturan dituangkan ke dalam Formulir 2.5 seperti terlihat pada Tabel 5 di bawah ini.

Tabel 5

Contoh Pengisian Formulir 2.5 Daftar Peraturan Perundang-Undangan

No	Nama Peraturan	Amanat
	Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik	Pasal 42 (1) Pemantauan dan evaluasi SPBE bertujuan untuk mengukur kemajuan dan meningkatkan kualitas SPBE di Instansi Pusat dan Pemerintah Daerah. (2) Tim Koordinasi SPBE Nasional melakukan pemantauan dan evaluasi terhadap SPBE secara nasional dan berkala.

		(3) Koordinator SPBE Instansi Pusat dan Pemerintah Daerah melakukan pemantauan dan evaluasi terhadap SPBE pada Instansi Pusat dan Pemerintah Daerah masing-masing secara berkala. (4) Pelaksanaan pemantauan dan evaluasi SPBE sebagaimana dimaksud pada ayat (3) dikoordinasikan oleh menteri yang menyelenggarakan urusan pemerintahan di bidang aparatur negara.
2	Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 5 Tahun 2020 tentang Pedoman Manajemen Risiko SPBE	Pasal 3 Evaluasi mandiri Sistem Pemerintahan Berbasis Elektronik pada Badan Siber dan Sandi Negara sebagaimana dimaksud dalam Pasal 2 huruf a dikoordinasikan oleh Sekretaris Utama pada BSSN atau pejabat yang memimpin unit sekretariat.

6. Penetapan Kategori Risiko SPBE

Penetapan Kategori Risiko SPBE bertujuan untuk menjamin agar proses identifikasi, analisis, dan evaluasi Risiko SPBE dapat dilakukan secara komprehensif. Kategori Risiko SPBE meliputi:

- a. Rencana Induk SPBE Nasional, merupakan Risiko SPBE yang berkaitan dengan penyusunan dan pelaksanaan perencanaan pembangunan SPBE Nasional;
- b. Arsitektur SPBE, merupakan Risiko SPBE yang berkaitan dengan penyusunan dan pemanfaatan arsitektur SPBE yang mendeskripsikan integrasi proses bisnis, data dan informasi, infrastruktur SPBE, dan keamanan SPBE;

- c. Peta Rencana SPBE, merupakan Risiko SPBE yang berkaitan dengan penyusunan dan pelaksanaan Peta Rencana SPBE;
- d. Proses Bisnis, merupakan Risiko SPBE yang berkaitan dengan penyusunan dan penerapan proses bisnis SPBE;
- e. Rencana dan Anggaran, merupakan Risiko SPBE yang berkaitan dengan proses perencanaan dan penganggaran SPBE;
- f. Inovasi, merupakan Risiko SPBE yang berkaitan dengan ide baru atau pemikiran kreatif yang memberikan nilai manfaat dalam penerapan SPBE;
- g. Kepatuhan terhadap Peraturan, merupakan Risiko SPBE yang berkaitan dengan kepatuhan unit kerja di lingkungan Instansi Pusat dan Pemerintah Daerah terhadap peraturan perundang-undangan, kesepakatan internasional, maupun ketentuan lain yang berlaku;
- h. Pengadaan Barang dan Jasa, merupakan Risiko SPBE yang berkaitan dengan proses pengadaan dan penyediaan barang dan jasa;
- i. Proyek Pembangunan/Pengembangan Sistem, merupakan Risiko SPBE yang berkaitan dengan proyek pembangunan ataupun pengembangan sistem pada penerapan SPBE;
- j. Data dan Informasi, merupakan Risiko SPBE yang berkaitan dengan semua data dan informasi yang dimiliki oleh Instansi Pusat dan Pemerintah Daerah;
- k. Infrastruktur SPBE, merupakan Risiko SPBE yang berkaitan dengan pusat data, jaringan intra pemerintah, dan sistem penghubung layanan pemerintah termasuk perangkat keras, perangkat lunak, dan fasilitas yang menjadi penunjang utama;
- l. Aplikasi SPBE, merupakan Risiko SPBE yang berkaitan dengan program komputer yang diterapkan untuk melakukan tugas atau fungsi layanan SPBE;
- m. Keamanan SPBE, merupakan Risiko SPBE yang berkaitan dengan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan (*non repudiation*) sumber daya yang mendukung SPBE;
- n. Layanan SPBE, merupakan Risiko SPBE yang berkaitan dengan pemberian layanan SPBE kepada Pengguna SPBE;

- o. Sumber Daya Manusia SPBE, merupakan Risiko SPBE yang berkaitan dengan SDM yang bekerja sebagai penggerak penerapan SPBE di Instansi Pusat dan Pemerintah Daerah; dan
- p. Bencana Alam, merupakan Risiko SPBE yang berkaitan dengan peristiwa yang disebabkan oleh alam.

Kategori Risiko SPBE dapat disesuaikan dengan konteks internal dan eksternal di masing-masing Instansi Pusat dan Pemerintah Daerah. Kategori Risiko SPBE dituangkan ke dalam Formulir 2.6 seperti terlihat pada Tabel 6 di bawah ini.

Tabel 6
Formulir 2.6 Kategori Risiko SPBE

No	Kategori Risiko SPBE
1	Rencana Induk SPBE Nasional
2	Arsitektur SPBE
3	Peta Rencana SPBE
4	Proses Bisnis
5	Rencana dan Anggaran
6	Inovasi
7	Kepatuhan terhadap Peraturan
8	Pengadaan Barang dan Jasa
9	Proyek Pembangunan/Pengembangan Sistem
10	Data dan Informasi
11	Infrastruktur SPBE
12	Aplikasi SPBE
13	Keamanan SPBE
14	Layanan SPBE
15	SDM SPBE
16	Bencana Alam

7. Penetapan Area Dampak Risiko SPBE

Penetapan Area Dampak Risiko SPBE bertujuan untuk mengetahui area mana saja yang terkena efek dari Risiko SPBE di BSSN. Penetapan Area

Dampak Risiko SPBE diawali dengan melakukan identifikasi dampak Risiko SPBE. Area Dampak Risiko SPBE yang menjadi fokus penerapan Manajemen Risiko SPBE meliputi:

- a. Finansial, dampak Risiko SPBE berupa aspek yang berkaitan dengan keuangan;
- b. Reputasi, dampak Risiko SPBE berupa aspek yang berkaitan dengan tingkat kepercayaan pemangku kepentingan;
- c. Kinerja, dampak Risiko SPBE berupa aspek yang berkaitan dengan pencapaian sasaran SPBE;
- d. Layanan Organisasi, dampak Risiko SPBE berupa aspek yang berkaitan dengan pemenuhan kebutuhan atau jasa kepada pemangku kepentingan;
- e. Operasional dan Aset TIK, dampak Risiko SPBE berupa aspek yang berkaitan dengan kegiatan operasional TIK dan pengelolaan aset TIK;
- f. Hukum dan Regulasi, dampak Risiko SPBE berupa aspek yang berkaitan dengan peraturan perundang-undangan dan kebijakan; dan
- g. Sumber Daya Manusia, dampak Risiko SPBE berupa aspek yang berkaitan dengan fisik dan mental pegawai.

Area Dampak Risiko SPBE terdiri atas area dampak positif dan atau negatif. Area Dampak Risiko SPBE dapat disesuaikan dengan konteks internal dan eksternal di masing-masing Unit Kerja BSSN. Area Dampak Risiko SPBE dituangkan ke dalam Formulir 2.7 seperti terlihat pada Tabel 7 di bawah ini.

Tabel 7

Formulir 2.7 Area Dampak Risiko SPBE

No	Area Dampak Risiko SPBE
1	Finansial
2	Reputasi
3	Kinerja
4	Layanan Organisasi
5	Operasional dan Aset TIK

No	Area Dampak Risiko SPBE
6	Hukum dan Regulasi
7	Sumber Daya Manusia

8. Penetapan Kriteria Risiko SPBE

Penetapan Kriteria Risiko SPBE bertujuan untuk mengukur dan menetapkan seberapa besar kemungkinan kejadian dan dampak Risiko SPBE yang dapat terjadi. Kriteria Risiko SPBE ini ditinjau secara berkala dan perlu melakukan penyesuaian dengan perubahan yang terjadi.

Penetapan Kriteria Risiko SPBE ini terdiri atas:

a. Kriteria Kemungkinan SPBE

Penetapan Kriteria Kemungkinan Risiko SPBE dilakukan berdasarkan penetapan level kemungkinan dan penetapan kriteria dari setiap level kemungkinan terhadap Risiko SPBE.

Unit Kerja BSSN dapat menggunakan level kemungkinan dengan 3 level, 4 level, 5 level, atau level lainnya yang disesuaikan dengan kompleksitas Risiko SPBE. Untuk 5 level kemungkinan, dapat diuraikan sebagai berikut:

- 1) Hampir Tidak Terjadi;
- 2) Jarang Terjadi;
- 3) Kadang-kadang Terjadi;
- 4) Sering Terjadi;
- 5) Hampir Pasti Terjadi.

Sedangkan, penetapan kriteria kemungkinan dilakukan melalui pendekatan persentase probabilitas statistik, jumlah frekuensi terjadinya suatu Risiko SPBE dalam satuan waktu, ataupun berdasarkan *expert judgement*.

Selanjutnya, kriteria kemungkinan dituliskan pada setiap level kemungkinan yang dituangkan ke dalam Formulir 2.8.A seperti terlihat pada Tabel 8 di bawah ini.

Tabel 8

Contoh Pengisian Formulir 2.8.A Kriteria Kemungkinan Risiko SPBE

Level Kemungkinan		Persentase Kemungkinan Terjadinya dalam Satu Tahun	Jumlah Frekuensi Kemungkinan Terjadinya dalam Satu Tahun
1	Hampir Tidak Terjadi	$X \leq 5\%$	$X < 2$ kali
2	Jarang Terjadi	$5\% < X \leq 10\%$	$2 \leq X \leq 5$ kali
3	Kadang-kadang Terjadi	$10\% < X \leq 20\%$	$6 \leq X \leq 9$ kali
4	Sering Terjadi	$20\% < X \leq 50\%$	$10 \leq X \leq 12$ kali
5	Hampir Pasti Terjadi	$X > 50\%$	> 12 kali

b. Kriteria Dampak SPBE

Penetapan Kriteria Dampak Risiko SPBE dilakukan dengan kombinasi antara Area Dampak Risiko SPBE (sebagaimana dijelaskan pada angka 7 di atas tentang Penetapan Area Dampak Risiko SPBE) dan level dampak. Instansi Pusat dan Pemerintah Daerah dapat menggunakan 3 level, 4 level, 5 level, atau level dampak lainnya yang disesuaikan dengan kompleksitas Risiko SPBE. Untuk 5 level dampak, dapat diuraikan sebagai berikut:

- 1) Tidak Signifikan;
- 2) Kurang Signifikan;
- 3) Cukup Signifikan;
- 4) Signifikan;
- 5) Sangat Signifikan.

Kriteria Dampak Risiko SPBE dijabarkan untuk setiap Area Dampak Risiko SPBE Positif dan Area Dampak Risiko SPBE Negatif terhadap setiap level dampak ke dalam Formulir 2.8.B seperti terlihat pada Tabel 9 di bawah ini.

Tabel 9

Contoh Pengisian Formulir 2.8.B Kriteria Dampak Risiko SPBE

Area Dampak		Level Dampak				
		1	2	3	4	5
		Tidak Signifikan	Kurang Signifikan	Cukup Signifikan	Signifikan	Sangat Signifikan
Kinerja	Positif	Peningkatan kinerja < 20%	Peningkatan kinerja 20% s.d < 40%	Peningkatan kinerja 40% s.d < 60%	Peningkatan kinerja 60% s.d < 80%	Peningkatan kinerja ☐ 80%
	Negatif	Penurunan kinerja < 20%	Penurunan kinerja 20% s.d < 40%	Penurunan kinerja 40% s.d < 60%	Penurunan kinerja 60% s.d < 80%	Penurunan kinerja ☐ 80%

9. Matriks Analisis Risiko SPBE dan Level Risiko SPBE

Matriks analisis Risiko SPBE berisi kombinasi antara level kemungkinan dan level dampak untuk dapat menetapkan Besaran Risiko SPBE yang direpresentasikan dalam bentuk angka. Besaran Risiko SPBE kemudian dimasukkan ke dalam Formulir 2.9.A seperti terlihat pada Tabel 10 di bawah ini.

Tabel 10

Contoh Pengisian Formulir 2.9.A Matriks Analisis Risiko SPBE

Matriks Analisis Risiko 5 x 5			Level Dampak				
			1	2	3	4	5
			Tidak Signifikan	Kurang Signifikan	Cukup Signifikan	Signifikan	Sangat Signifikan
Level Kemungkinan	5	Hampir Pasti Terjadi	9	15	18	23	25
	4	Sering Terjadi	6	12	16	19	24
	3	Kadang- Kadang Terjadi	4	10	14	17	22
	2	Jarang Terjadi	2	7	11	13	21
	1	Hampir Tidak Terjadi	1	3	5	8	20

Besaran Risiko SPBE ini selanjutnya dikelompokkan ke dalam Level Risiko SPBE dimana setiap Level Risiko SPBE memiliki rentang nilai Besaran Risiko SPBE. Pemilihan Level Risiko SPBE dapat menggunakan 3 level, 4 level, 5 level, atau Level Risiko SPBE lainnya yang disesuaikan dengan kompleksitas Risiko SPBE. Setiap level tersebut direpresentasikan dengan warna sesuai dengan preferensi masing-masing Instansi Pusat dan Pemerintah Daerah. Untuk 5 Level Risiko SPBE, dapat diuraikan sebagai berikut:

- b. Sangat Rendah, direpresentasikan dengan warna biru;
- c. Rendah, direpresentasikan dengan warna hijau;
- d. Sedang, direpresentasikan dengan warna kuning;
- e. Tinggi, direpresentasikan dengan warna jingga;
- f. Sangat Tinggi, direpresentasikan dengan warna merah.

Nilai rentang Besaran Risiko dituangkan ke dalam Formulir 2.9.B seperti terlihat pada Tabel 11 di bawah ini.

Tabel 11

Contoh Pengisian Formulir 2.9.B Level Risiko SPBE

Level Risiko		Rentang Besaran Risiko	Keterangan Warna
1	Sangat Rendah	1-5	Biru
2	Rendah	6-10	Hijau
3	Sedang	11-15	Kuning
4	Tinggi	16-20	Jingga
5	Sangat Tinggi	21-25	Merah

10. Selera Risiko SPBE

Selera Risiko SPBE bertujuan untuk memberikan acuan dalam penentuan ambang batas minimum terhadap Besaran Risiko SPBE yang harus ditangani untuk setiap Kategori Risiko SPBE baik Risiko SPBE Positif maupun Risiko SPBE Negatif. Penentuan Selera Risiko SPBE ini dapat disesuaikan dengan kompleksitas Risiko SPBE serta konteks internal dan eksternal masing-masing Instansi Pusat dan Pemerintah Daerah. Besaran Risiko yang ditangani pada setiap Kategori Risiko SPBE dituangkan ke dalam Formulir 2.10 seperti terlihat pada Tabel 12 di bawah ini.

Tabel 12

Contoh Pengisian Formulir 2.10 Selera Risiko SPBE

No	Kategori Risiko SPBE	Besaran Risiko Minimum yang Ditangani	
		Risiko SPBE Positif	Risiko SPBE Negatif
1	Rencana dan Anggaran	16	6
2	Pengadaan Barang dan Jasa	18	11
3	SDM SPBE	20	14

C. Penilaian Risiko SPBE

Penilaian Risiko SPBE pada penerapan SPBE dilakukan melalui proses identifikasi, analisis, dan evaluasi Risiko SPBE. Penilaian Risiko SPBE bertujuan untuk memahami penyebab, kemungkinan, dan dampak Risiko SPBE yang dapat terjadi di Instansi Pusat dan Pemerintah Daerah. Penilaian Risiko SPBE dilakukan pada setiap Sasaran SPBE. Tahapan penilaian Risiko SPBE meliputi:

1. Identifikasi Risiko SPBE

Identifikasi Risiko SPBE merupakan proses menggali informasi mengenai kejadian, penyebab, dan dampak Risiko SPBE. Informasi yang dicantumkan meliputi:

a. Jenis Risiko SPBE

Jenis Risiko SPBE terbagi menjadi Risiko SPBE positif dan Risiko SPBE negatif. Dalam melakukan identifikasi Risiko SPBE, Risiko SPBE dituliskan ke dalam masing-masing jenis Risiko SPBE.

b. Kejadian

Kejadian dapat diidentifikasi dari terjadinya suatu peristiwa yang menimbulkan Risiko SPBE yang diperoleh dari riwayat peristiwa dan/atau prediksi terjadinya peristiwa di masa yang akan datang. Kejadian selanjutnya disebut sebagai Risiko SPBE.

c. Penyebab

Penyebab dapat diidentifikasi dari akar masalah yang menjadi pemicu munculnya Risiko SPBE. Penyebab dapat berasal dari lingkungan internal maupun eksternal Instansi Pusat dan Pemerintah Daerah. Identifikasi penyebab akan membantu menemukan tindakan yang tepat untuk menangani Risiko SPBE.

d. Kategori

Penentuan Kategori Risiko SPBE didasarkan pada penyebab dari munculnya Risiko SPBE. Kategori Risiko SPBE telah dijelaskan pada bagian huruf B angka 6 tentang Penetapan Kategori Risiko SPBE.

e. Dampak

Dampak dapat diidentifikasi dari pengaruh atau akibat yang timbul dari Risiko SPBE.

f. Area Dampak

Penentuan Area Dampak Risiko SPBE didasarkan pada dampak

yang telah teridentifikasi. Area Dampak Risiko telah dijelaskan pada bagian huruf B angka 7 tentang Penetapan Area Dampak.

Proses Identifikasi Risiko SPBE dituangkan ke dalam Formulir 3.0 pada bagian Identifikasi Risiko SPBE seperti terlihat pada Tabel 13.

Tabel 13
Contoh Pengisian Formulir 3.0 Penilaian Risiko SPBE Bagian
Identifikasi Risiko SPBE

Identifikasi Risiko SPBE					
Jenis Risiko SPBE	Kejadian	Penyebab	Kategori	Dampak	Area Dampak
Positif	Respon dari K/L/D sangat antusias	Adanya mandat dari Peraturan Presiden No 95 Tahun 2018	Kepatuhan terhadap Peraturan	Peningkatan kualitas layanan SPBE	Kinerja
Negatif	Terdapat K/L/D yang tidak dievaluasi	Kurangnya jumlah evaluator eksternal	SDM SPBE	Penurunan kinerja	Kinerja

2. Analisis Risiko SPBE

Analisis Risiko SPBE merupakan proses untuk melakukan penilaian atas Risiko SPBE yang telah diidentifikasi sebelumnya. Analisis Risiko SPBE dilakukan dengan cara menentukan sistem pengendalian, level kemungkinan, dan level dampak terjadinya Risiko SPBE. Informasi yang dicantumkan pada analisis Risiko SPBE meliputi:

a. Sistem Pengendalian

- 1) Sistem pengendalian internal mencakup perangkat manajemen yang dapat menurunkan/meningkatkan level Risiko SPBE dalam rangka pencapaian sasaran SPBE.
- 2) Sistem pengendalian internal dapat berupa *Standard Operating Procedure* (SOP), pengawasan melekat, revidi berjenjang, regulasi, dan pemantauan rutin yang dilaksanakan terkait Risiko SPBE tersebut.

b. Level Kemungkinan

Penentuan level kemungkinan dilakukan dengan mengukur persentase probabilitas atau frekuensi peluang terjadinya Risiko SPBE dalam satu periode yang dicocokkan dengan Kriteria Kemungkinan

Risiko SPBE sebagaimana telah dijelaskan pada bagian huruf B angka

8 huruf a. Penentuan level kemungkinan harus didukung dengan penjelasan singkat untuk mengetahui alasan pemilihan level kemungkinan tersebut.

c. Level Dampak

Penentuan level dampak dilakukan dengan mengukur besar dampak dari terjadinya Risiko SPBE yang dicocokkan dengan Kriteria Dampak Risiko SPBE sebagaimana telah dijelaskan pada bagian huruf B angka 8 huruf b. Level dampak harus didukung dengan penjelasan singkat untuk mengetahui alasan pemilihan level dampak tersebut.

d. Besaran Risiko SPBE dan Level Risiko SPBE

Penentuan Besaran Risiko SPBE dan Level Risiko SPBE didapat dari kombinasi Level Kemungkinan dan Level Dampak dengan menggunakan rumusan dalam Matriks Analisis Risiko SPBE sebagaimana telah dijelaskan pada bagian huruf B angka 9.

Proses Analisis Risiko SPBE dituangkan ke dalam Formulir 3.0 pada bagian Analisis Risiko SPBE seperti terlihat pada Tabel 14 di bawah ini.

Tabel 14
Contoh Pengisian Formulir 3.0 Penilaian Risiko SPBE Bagian
Analisis Risiko SPBE

Analisis Risiko SPBE						
Sistem Pengendalian	Kemungkinan		Dampak		Besaran Risiko SPBE	Level Risiko SPBE
	Level	Penjelasan	Level	Penjelasan		
Konfirmasi keikutsertaan dalam evaluasi SPBE	Hampir Pasti Terjadi	Keikutsertaan lebih dari 80%	Sangat Signifikan	Peningkatan kinerja hingga 80%	25	Sangat Tinggi
Analisis beban kerja evaluator eksternal	Kadang - Kadang Terjadi	Terjadi sekitar 15% dalam satu periode	Cukup Signifikan	Penurunan kinerja hingga 50%	14	Sedang

3. Evaluasi Risiko SPBE

Evaluasi Risiko SPBE dilakukan untuk mengambil keputusan mengenai perlu tidaknya dilakukan upaya penanganan Risiko SPBE lebih lanjut serta penentuan prioritas penanganannya. Pengambilan keputusan mengacu pada Selera Risiko SPBE yang telah ditentukan sebagaimana telah dijelaskan pada bagian huruf B angka 10. Prioritas penanganan Risiko SPBE diurutkan berdasarkan Besaran Risiko SPBE. Apabila terdapat lebih dari satu Risiko SPBE yang memiliki besaran yang sama maka cara penentuan prioritas berdasarkan *expert judgement*. Proses Evaluasi Risiko SPBE dituangkan ke dalam Formulir 3.0 pada bagian Penilaian Risiko SPBE seperti terlihat pada Tabel 15 di bawah ini.

Tabel 15
Contoh Pengisian Formulir 3.0 Penilaian Risiko SPBE Bagian
Evaluasi Risiko SPBE

Evaluasi Risiko SPBE	
Keputusan Penanganan Risiko SPBE (Ya/Tidak)	Prioritas Penanganan Risiko SPBE
Ya	1
Ya	2

D. Penanganan Risiko SPBE

Penanganan Risiko SPBE merupakan proses untuk memodifikasi penyebab Risiko SPBE. Penanganan Risiko SPBE dilakukan dengan mengidentifikasi berbagai opsi yang mungkin diterapkan dan memilih satu atau lebih opsi penanganan Risiko SPBE. Informasi yang dicantumkan pada penanganan Risiko SPBE meliputi:

1. Prioritas Risiko

Prioritas Risiko SPBE diurutkan berdasarkan Besaran Risiko SPBE. Risiko SPBE yang memiliki prioritas lebih tinggi ditunjukkan dengan nilai Besaran Risiko SPBE yang lebih tinggi.

2. Rencana Penanganan Risiko SPBE

Rencana penanganan Risiko SPBE merupakan agenda kegiatan untuk menangani Risiko SPBE agar mencapai Selera Risiko SPBE yang telah ditetapkan. Rencana penanganan Risiko SPBE dilakukan dengan mengidentifikasi hal-hal sebagai berikut:

a. Opsi Penanganan Risiko SPBE

Opsi penanganan Risiko SPBE, berisikan alternatif yang dipilih untuk menangani Risiko SPBE. Opsi penanganan Risiko SPBE dilakukan dengan mengidentifikasi berbagai opsi yang mungkin untuk diterapkan. Opsi penanganan Risiko SPBE terbagi menjadi dua, yaitu penanganan Risiko SPBE Positif dan penanganan Risiko SPBE

Negatif. Adapun opsi yang ditentukan pada pedoman ini meliputi:

1) Opsi Penanganan Risiko Positif

a) Eskalasi Risiko

Eskalasi risiko dipilih jika Risiko SPBE berada di luar atau melampaui wewenang. Opsi ini dilakukan dengan memindahkan tanggung jawab penanganan Risiko SPBE ke unit kerja yang lebih tinggi.

b) Eksploitasi Risiko

Eksploitasi risiko dipilih jika Risiko SPBE dapat dipastikan terjadi. Opsi ini dilakukan dengan cara memanfaatkan Risiko SPBE tersebut semaksimal mungkin.

c) Peningkatan Risiko

Peningkatan risiko dilakukan dengan cara meningkatkan level kemungkinan dan/atau level dampak dari Risiko SPBE.

d) Pembagian Risiko

Pembagian risiko dipilih jika Risiko SPBE tidak dapat ditangani secara langsung dan membutuhkan pihak lain untuk menangani Risiko SPBE tersebut. Pembagian risiko dilakukan dengan bekerja sama dengan dengan pihak lain.

e) Penerimaan Risiko

Penerimaan risiko dipilih jika upaya penanganan lebih tinggi dibandingkan manfaat yang didapat atau kemungkinan terjadinya kecil. Opsi ini dilakukan dengan cara membiarkan Risiko SPBE terjadi apa adanya.

2) Opsi Penanganan Risiko Negatif

a) Eskalasi Risiko

Eskalasi risiko dipilih jika Risiko SPBE berada di luar atau melampaui wewenang. Opsi ini dilakukan dengan memindahkan tanggung jawab penanganan Risiko SPBE ke unit kerja yang lebih tinggi.

- b) Mitigasi Risiko
Mitigasi risiko dilakukan dengan cara mengurangi level kemungkinan dan/atau level dampak dari Risiko SPBE.
 - c) Transfer Risiko
Transfer risiko dipilih jika terdapat kekurangan sumber daya untuk mengelola Risiko SPBE. Opsi ini dilakukan dengan cara mengalihkan kepemilikan risiko kepada pihak lain untuk melakukan pengelolaan dan pertanggung-jawaban terhadap Risiko SPBE.
 - d) Penghindaran Risiko
Penghindaran risiko dilakukan dengan mengubah perencanaan, penganggaran, program, dan kegiatan, atau aspek lainnya untuk mencapai sasaran SPBE.
 - e) Penerimaan Risiko
Penerimaan risiko dipilih jika biaya dan usaha penanganan lebih tinggi dibandingkan manfaat yang didapat, kemungkinan terjadinya sangat kecil atau dampak sangat tidak signifikan. Opsi ini dilakukan dengan cara membiarkan risiko terjadi apa adanya.
- b. Rencana Aksi Penanganan Risiko
Rencana aksi penanganan risiko merupakan rancangan kegiatan tindak lanjut untuk menangani Risiko SPBE.
- c. Keluaran
Keluaran merupakan hasil dari rencana aksi penanganan Risiko SPBE.
- d. Jadwal Implementasi
Jadwal implementasi merupakan jadwal pelaksanaan dari setiap rencana aksi penanganan Risiko SPBE.
- e. Penanggung Jawab
Penanggung jawab berisikan nama unit yang bertanggung jawab dan unit pendukung dari setiap rencana aksi penanganan Risiko SPBE.

Tabel 16

Contoh Pengisian Formulir 4.0 Rencana Penanganan Risiko SPBE
Bagian Rencana Penanganan

Rencana Penanganan				
Opsi Penanganan Risiko SPBE	Rencana Aksi Penanganan Risiko SPBE	Keluaran	Jadwal Implementasi	Penanggung Jawab
Eksplorasi Risiko	Melakukan sosialisasi dan asistensi kepada K/L/D	Kegiatan sosialisasi dan asistensi	Triwulan I	Asisten Deputi SPBE
Mitigasi Risiko	Rekrutmen evaluator eksternal baru	Penambahan jumlah evaluator eksternal	Triwulan I	Asisten Deputi SPBE

3. Risiko Residual

Risiko residual merupakan Risiko SPBE yang tersisa dari Risiko SPBE yang telah ditangani. Dalam melakukan penanganan terhadap risiko residual, dilakukan pengulangan proses penilaian risiko sampai dengan risiko residual tersebut berada di bawah Selera Risiko SPBE. Penetapan risiko residual ini dapat ditetapkan berdasarkan *expert judgement*.

E. Pemantauan dan Reviu

Pemantauan bertujuan untuk memonitor faktor-faktor atau penyebab yang mempengaruhi Risiko SPBE dan kondisi lingkungan BSSN. Selain itu, pemantauan dilakukan guna memonitor pelaksanaan rencana aksi penanganan Risiko SPBE. Hasil pelaksanaan pemantauan dapat menjadi dasar untuk melakukan penyesuaian kembali proses Manajemen Risiko SPBE. Pemantauan dilakukan berdasarkan setiap triwulan, semester, tahun, atau sewaktu-waktu (insidental) sesuai dengan kesepakatan dari masing-masing Unit Kerja BSSN.

Reviu bertujuan untuk mengontrol kesesuaian dan ketepatan seluruh pelaksanaan proses Manajemen Risiko SPBE sesuai dengan ketentuan yang berlaku. Reviu dilakukan sesuai dengan kesepakatan dari masing-masing Instansi Pusat dan Pemerintah Daerah.

F. Pencatatan dan Pelaporan

Pencatatan merupakan kegiatan atau proses pendokumentasian suatu aktivitas dalam bentuk tulisan dan dituangkan dalam dokumen. Pelaporan merupakan kegiatan yang dilakukan untuk menyampaikan hal-hal yang berhubungan dengan hasil pekerjaan yang telah dilakukan selama satu periode tertentu.

Proses Manajemen Risiko SPBE dan keluaran yang dihasilkan perlu dicatat dan dilaporkan dengan mekanisme yang tepat. Pencatatan dan pelaporan bertujuan untuk mengkomunikasikan aktivitas Manajemen Risiko SPBE serta keluaran yang dihasilkan, menyediakan informasi untuk pengambilan keputusan, meningkatkan kualitas aktivitas Manajemen Risiko SPBE, serta mengawal interaksi dengan pemangku kepentingan termasuk tanggung jawab serta akuntabilitas terhadap Manajemen Risiko SPBE.

Pencatatan dan pelaporan Manajemen Risiko SPBE terdiri dari:

1. Pencatatan dan Pelaporan Periodik

Pencatatan dan pelaporan periodik merupakan kegiatan yang dilakukan secara berulang pada waktu yang telah ditentukan.

2. Pencatatan dan Pelaporan Insidental

Pencatatan dan pelaporan insidental merupakan kegiatan yang dilakukan pada waktu tertentu sesuai dengan kebutuhan.

G. Dokumen Manajemen Risiko SPBE

1. Pakta Integritas Manajemen Risiko SPBE

Pakta Integritas Manajemen Risiko SPBE merupakan dokumen pernyataan atau janji untuk berkomitmen menjalankan Manajemen Risiko SPBE di BSSN. Dokumen Pakta Integritas dapat dilihat pada Formulir 1.0 Pakta Integritas.

2. Dokumen Proses Risiko SPBE

Dokumen Proses Risiko SPBE merupakan dokumen pendukung

pelaksanaan proses penetapan konteks, penilaian, dan penanganan Risiko SPBE. Dokumen Proses Risiko SPBE terdiri dari:

a. Formulir Konteks Risiko SPBE

Formulir Konteks Risiko SPBE merupakan dokumen dari aktivitas penetapan konteks pada proses Manajemen Risiko SPBE. Formulir ini dapat dilihat pada Formulir 2.0.

b. Formulir Penilaian Risiko SPBE

Formulir Penilaian Risiko SPBE merupakan dokumen dari aktivitas penilaian Risiko SPBE pada proses Manajemen Risiko SPBE. Formulir ini dapat dilihat pada Formulir 3.0.

c. Formulir Rencana Penanganan Risiko SPBE

Formulir Rencana Penanganan Risiko SPBE merupakan dokumen dari aktivitas penanganan Risiko SPBE pada proses Manajemen Risiko SPBE. Formulir ini dapat dilihat pada Formulir 4.0.

2. Dokumen Proses Pengendalian Risiko SPBE

Dokumen Proses Pengendalian Risiko SPBE merupakan dokumen pendukung pelaksanaan proses komunikasi dan konsultasi, serta pelaporan Risiko SPBE. Dokumen Proses Pengendalian Risiko SPBE terdiri dari:

a. Dokumen Kegiatan Komunikasi dan Konsultasi

Dokumen Kegiatan Komunikasi dan Konsultasi merupakan dokumen dari aktivitas pelaksanaan kegiatan komunikasi dan konsultasi. Dokumen dapat berbentuk notulensi dan laporan atau dokumen lainnya yang dihasilkan dari pelaksanaan kegiatan komunikasi dan konsultasi.

b. Dokumen Laporan Pemantauan

Dokumen Laporan Pemantauan merupakan dokumen dari aktivitas pelaksanaan kegiatan pemantauan Risiko. Dalam pedoman ini menggunakan 2 format laporan yaitu laporan pemantauan triwulan dan laporan pemantauan tahunan.

Laporan pemantauan triwulan menggambarkan kondisi pelaksanaan dalam waktu setiap tiga bulan terkait rencana aksi penanganan yang meliputi besaran/level Risiko SPBE saat ini dan proyeksi Risiko SPBE, penanganan yang telah dilakukan, rencana penanganan,

penanggung jawab, dan waktu pelaksanaan.

Laporan pemantauan tahunan merangkum laporan triwulan I sampai dengan triwulan IV dengan berfokus pada tendensi besaran Risiko SPBE dan memberikan rekomendasi penanganan Risiko SPBE yang dapat digunakan sebagai masukan pelaksanaan proses Manajemen Risiko SPBE pada tahun selanjutnya. Format laporan pemantauan triwulan dan tahunan dapat dilihat pada Formulir 5.0.

3. Dokumen Proses Pengendalian Risiko SPBE

Dokumen Proses Pengendalian Risiko SPBE merupakan dokumen pendukung pelaksanaan proses komunikasi dan konsultasi, serta pelaporan Risiko SPBE. Dokumen Proses Pengendalian Risiko SPBE terdiri dari:

a. Dokumen Kegiatan Komunikasi dan Konsultasi

Dokumen Kegiatan Komunikasi dan Konsultasi merupakan dokumen dari aktivitas pelaksanaan kegiatan komunikasi dan konsultasi. Dokumen dapat berbentuk notulensi dan laporan atau dokumen lainnya yang dihasilkan dari pelaksanaan kegiatan komunikasi dan konsultasi.

b. Dokumen Laporan Pemantauan

Dokumen Laporan Pemantauan merupakan dokumen dari aktivitas pelaksanaan kegiatan pemantauan Risiko. Dalam pedoman ini menggunakan 2 format laporan yaitu laporan pemantauan triwulan dan laporan pemantauan tahunan.

Laporan pemantauan triwulan menggambarkan kondisi pelaksanaan dalam waktu setiap tiga bulan terkait rencana aksi penanganan yang meliputi besaran/level Risiko SPBE saat ini dan proyeksi Risiko SPBE, penanganan yang telah dilakukan, rencana penanganan, penanggung jawab, dan waktu pelaksanaan.

Laporan pemantauan tahunan merangkum laporan triwulan I sampai dengan triwulan IV dengan berfokus pada tendensi besaran Risiko SPBE dan memberikan rekomendasi penanganan Risiko SPBE yang dapat digunakan sebagai masukan pelaksanaan proses Manajemen Risiko SPBE pada tahun selanjutnya. Format laporan pemantauan triwulan dan tahunan dapat dilihat pada Formulir 5.0

Laporan Pemantauan Risiko SPBE Triwulan I

Nama Unit : Deputi Bidang Kelembagaan dan Tata Laksana

Sasaran : Meningkatnya kualitas penyelenggaraan Sistem Pemerintahan Berbasis Elektronik

Risiko : Terdapat K/L/D yang tidak dievaluasi karena kurangnya jumlah evaluator eksternal sehingga terjadi penurunan kinerja

Besaran/Level Risiko SPBE Saat ini dan Proyeksi Risiko SPBE

Risiko SPBE pada awal tahun berada pada Level Risiko SPBE "sedang" dengan Besaran Risiko SPBE sebesar 14 di mana kemungkinan terjadinya Risiko SPBE tersebut sekitar 15% dalam satu periode (Kadang-kadang Terjadi) dan berdampak pada penurunan kinerja hingga 50% (Cukup Signifikan).

Risiko SPBE tersebut pada triwulan I telah berada pada Level Risiko SPBE "rendah" dengan Besaran Risiko SPBE sebesar 10 di mana kemungkinan terjadinya Risiko SPBE tersebut sekitar 15% dalam satu periode (Kadang-Kadang Terjadi) dan berdampak pada penurunan kinerja hingga 20% (Kurang Signifikan).

Risiko SPBE tersebut kedepannya tidak dilakukan penanganan, karena sudah berada di bawah Selera Risiko SPBE.

Penanganan yang telah dilakukan

Rekrutmen evaluator eksternal.

Rencana Penanganan	Penanggung jawab	Waktu Pelaksanaan
Melakukan pemantauan terhadap kegiatan evaluasi SPBE.	Asisten Deputi SPBE	Triwulan I

Gambar 3. Formulir 5.0 Laporan Pemantauan Risiko SPBE Triwulan I

Laporan Pemantauan Risiko SPBE Tahunan			
2	Nama Unit : Deputi Bidang Kelembagaan dan Tata Laksana Sasaran : Meningkatnya kualitas penyelenggaraan Sistem Pemerintahan Berbasis Elektronik Risiko : Terdapat K/L/D yang tidak dievaluasi karena kurangnya jumlah evaluator eksternal sehingga terjadi penurunan kinerja		
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: center; padding: 5px;">Besaran/Level Risiko SPBE Saat ini</th> </tr> </thead> <tbody> <tr> <td style="padding: 5px;"> Risiko SPBE pada awal tahun berada pada Level Risiko SPBE "sedang" dengan Besaran Risiko SPBE sebesar 14. Risiko SPBE tersebut pada triwulan I, II, III, dan IV telah berada pada Level Risiko SPBE "rendah" dengan Besaran Risiko SPBE sebesar 10. </td> </tr> </tbody> </table>		Besaran/Level Risiko SPBE Saat ini	Risiko SPBE pada awal tahun berada pada Level Risiko SPBE "sedang" dengan Besaran Risiko SPBE sebesar 14. Risiko SPBE tersebut pada triwulan I, II, III, dan IV telah berada pada Level Risiko SPBE "rendah" dengan Besaran Risiko SPBE sebesar 10.
Besaran/Level Risiko SPBE Saat ini			
Risiko SPBE pada awal tahun berada pada Level Risiko SPBE "sedang" dengan Besaran Risiko SPBE sebesar 14. Risiko SPBE tersebut pada triwulan I, II, III, dan IV telah berada pada Level Risiko SPBE "rendah" dengan Besaran Risiko SPBE sebesar 10.			
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: center; padding: 5px;">Penanganan yang telah dilakukan</th> </tr> </thead> <tbody> <tr> <td style="padding: 5px;"> 1. Rekrutmen evaluator eksternal termasuk pelatihan bagi evaluator eksternal. 2. Pemantauan terhadap kegiatan evaluasi SPBE. </td> </tr> </tbody> </table>		Penanganan yang telah dilakukan	1. Rekrutmen evaluator eksternal termasuk pelatihan bagi evaluator eksternal. 2. Pemantauan terhadap kegiatan evaluasi SPBE.
Penanganan yang telah dilakukan			
1. Rekrutmen evaluator eksternal termasuk pelatihan bagi evaluator eksternal. 2. Pemantauan terhadap kegiatan evaluasi SPBE.			
Rekomendasi	Untuk mengantisipasi terjadinya Risiko SPBE yang serupa, perlu dipastikan jumlah evaluator eksternal yang dibutuhkan untuk pelaksanaan evaluasi SPBE sesuai dengan analisis beban kerja.		

Gambar 4. Formulir 5.0 Laporan Pemantauan Risiko SPBE Tahunan

BAB IV

STRUKTUR MANAJEMEN DAN BUDAYA SADAR Risiko SPBE

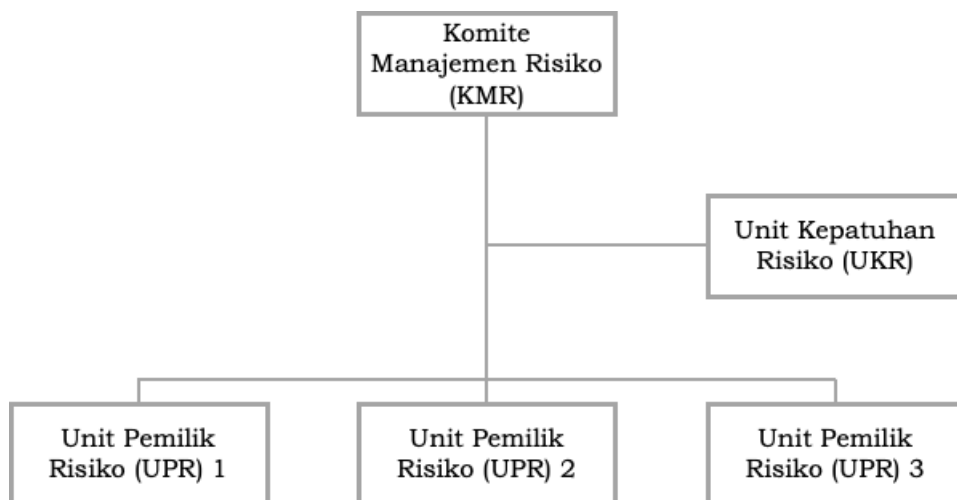
Manajemen Risiko SPBE merupakan tanggung jawab bersama pada semua unit kerja di lingkungan BSSN. Agar proses dan pengukuran dalam Manajemen Risiko SPBE dapat dilaksanakan dengan baik, maka diperlukan tata kelola Manajemen Risiko SPBE yang mengatur tugas dan tanggung jawab dari struktur Manajemen Risiko SPBE, dan budaya sadar Risiko SPBE yang dapat menggerakkan pegawai ASN menerapkan Manajemen Risiko SPBE.

A. Struktur Manajemen Risiko SPBE

Struktur Manajemen Risiko SPBE terdiri atas

1. Komite Manajemen Risiko (KMR) SPBE yang memiliki fungsi penetapan kebijakan strategis terkait Manajemen Risiko SPBE.
2. Unit Pemilik Risiko (UPR) SPBE yang memiliki fungsi pelaksanaan Manajemen Risiko SPBE.
3. Unit Kepatuhan Risiko (UKR) SPBE yang memiliki fungsi pengawasan terhadap pelaksanaan Manajemen Risiko SPBE.

Gambar 5 mengilustrasikan struktur Manajemen Risiko SPBE seperti di bawah ini



Gambar 5. Struktur Manajemen Risiko SPBE

Struktur Manajemen Risiko SPBE merupakan struktur *ex-officio* yang menjalankan tugas tambahan terkait Manajemen Risiko SPBE. Apabila Instansi Pusat dan Pemerintah Daerah telah memiliki kebijakan manajemen risiko bagi organisasi, struktur Manajemen Risiko SPBE hendaknya mengadopsi struktur manajemen risiko yang telah ada tersebut untuk keterpaduan pelaksanaan manajemen risiko secara menyeluruh.

Di dalam penerapan Manajemen Risiko SPBE, struktur Manajemen Risiko SPBE di Instansi Pusat dan Pemerintah Daerah dapat memiliki struktur yang berbeda satu sama lain. Perbedaan struktur Manajemen Risiko SPBE dapat dipengaruhi oleh ukuran organisasi, kompleksitas tugas, dan/atau tingkat risiko di Instansi Pusat dan Pemerintah Daerah. Instansi Pusat dan Pemerintah Daerah yang memiliki ukuran organisasi yang besar, kompleksitas tugas yang tinggi, dan/atau tingkat risiko yang tinggi memerlukan pengendalian Risiko SPBE yang lebih ketat melalui struktur Manajemen Risiko SPBE yang lebih berjenjang.

1. Komite Manajemen Risiko (KMR) SPBE

Komite Manajemen Risiko SPBE yang disingkat KMR SPBE dibentuk dan ditetapkan oleh Kepala BSSN, dan memiliki anggota yang terdiri atas pejabat yang memiliki kewenangan pengambilan keputusan dan penetapan kebijakan strategis terkait Manajemen Risiko SPBE. KMR SPBE memiliki tugas menyelenggarakan perumusan dan penetapan kebijakan, pengendalian, pemantauan, dan evaluasi penerapan kebijakan Manajemen Risiko SPBE. Dalam melaksanakan tugasnya, KMR SPBE menyelenggarakan fungsi sebagai berikut:

- a. penyusunan dan penetapan kebijakan Manajemen Risiko SPBE;
- b. penyusunan dan penetapan kerangka kerja dan pedoman pelaksanaan Manajemen Risiko SPBE;
- c. penyusunan dan penetapan pakta integritas Manajemen Risiko SPBE;
- d. penyusunan dan penetapan konteks Risiko SPBE;
- e. pengendalian proses Risiko SPBE melalui komunikasi dan konsultasi, pencatatan dan pelaporan, serta pemantauan dan evaluasi terhadap penerapan Manajemen Risiko SPBE; dan

- f. pelaksanaan komitmen pimpinan dan penerapan budaya sadar Risiko SPBE.
2. Unit Pemilik Risiko (UPR) SPBE
- Unit Pemilik Risiko SPBE yang disingkat UPR SPBE merupakan unit kerja di BSSN yang bertanggung jawab langsung kepada Kepala BSSN. UPR SPBE memiliki tugas melaksanakan penerapan Manajemen Risiko SPBE pada unit kerja tertinggi sampai terendah. UPR SPBE terdiri atas unsur:
- a. Pemilik Risiko SPBE merupakan pejabat yang bertanggung jawab atas pelaksanaan penerapan Manajemen Risiko SPBE di unit organisasi tersebut;
 - b. Koordinator Risiko SPBE merupakan pejabat/pegawai yang ditunjuk oleh Pemilik Risiko SPBE untuk bertanggung jawab atas pelaksanaan koordinasi penerapan Manajemen Risiko SPBE kepada semua pemangku kepentingan baik internal maupun eksternal UPR SPBE; dan
 - c. Pengelola Risiko SPBE merupakan pejabat/pegawai yang ditunjuk oleh Pemilik Risiko SPBE untuk bertanggung jawab atas pelaksanaan operasional Manajemen Risiko SPBE pada unit-unit kerja yang berada di bawah UPR SPBE.

Dalam melaksanakan tugasnya, UPR SPBE menjalankan fungsi sebagai berikut:

- a. penyusunan dan penetapan penilaian Risiko SPBE dan rencana pelaksanaan Manajemen Risiko SPBE termasuk rencana kontinjensi penanganan Risiko SPBE;
- b. pelaksanaan koordinasi penerapan Manajemen Risiko SPBE kepada semua pemangku kepentingan;
- c. pelaksanaan operasional Manajemen Risiko SPBE yang efektif melalui komunikasi dan konsultasi, pencatatan dan pelaporan, serta pemantauan dan evaluasi; dan
- d. pelaksanaan pembinaan budaya sadar Risiko SPBE melalui sosialisasi, bimbingan, pelatihan, dan supervisi penerapan Manajemen Risiko SPBE;

3. Unit Kepatuhan Risiko (UKR) SPBE

Unit Kepatuhan Risiko SPBE yang disingkat UKR SPBE merupakan unit kerja di BSSN yang melaksanakan fungsi pengawasan intern di BSSN (Aparat Pengawasan Intern Pemerintah-APIP). UKR SPBE memiliki tugas melaksanakan pengawasan terhadap penerapan kebijakan Manajemen Risiko SPBE di semua UPR SPBE. Dalam melaksanakan tugasnya, UKR SPBE menjalankan fungsi sebagai berikut:

- a. penyusunan kebijakan pengawasan terhadap penerapan Manajemen Risiko SPBE;
- b. pelaksanaan pengawasan intern terhadap penerapan Manajemen Risiko SPBE di semua UPR SPBE melalui audit, reviu, pemantauan, evaluasi, dan kegiatan pengawasan lainnya;
- c. pelaksanaan konsultasi dan asistensi kepada UPR SPBE dalam penerapan Manajemen Risiko SPBE;
- d. penyusunan dan penyampaian rekomendasi terhadap efektivitas penerapan Manajemen Risiko SPBE kepada KMR SPBE dan UPR SPBE; dan pelaksanaan konsultasi dan asistensi kepada UPR dalam pembinaan budaya sadar Risiko SPBE

B. Budaya Sadar Risiko SPBE

Budaya sadar Risiko SPBE merupakan perilaku ASN yang mengenal, memahami, dan mengakui kemungkinan terjadinya Risiko SPBE, baik positif maupun negatif, yang ditindaklanjuti dengan upaya yang berfokus pada penerapan Manajemen Risiko SPBE di Instansi Pusat dan Pemerintah Daerah. ASN harus peka terhadap faktor-faktor dan peristiwa yang mungkin berpengaruh terhadap tujuan dan sasaran penerapan SPBE di Instansi Pusat dan Pemerintah Daerah. Dengan menyadari adanya Risiko SPBE, ASN dapat merencanakan dan mempersiapkan tindakan atau penanganan Risiko SPBE secepatnya. Keterlibatan ASN di dalam budaya sadar Risiko SPBE akan memberikan nilai tambah dan meningkatkan efektivitas penerapan Manajemen Risiko SPBE yang pada akhirnya berdampak pada peningkatan kualitas penerapan SPBE di Instansi Pusat dan Pemerintah Daerah.

1. Faktor Keberhasilan

Faktor-faktor yang dapat mendukung keberhasilan dalam menciptakan budaya sadar Risiko SPBE antara lain:

a. Kepemimpinan

KMR SPBE harus dapat menunjukkan sikap kepemimpinan, yaitu konsisten dalam perkataan dan tindakan, mampu mendorong atau menggerakkan ASN dalam penerapan budaya sadar Risiko SPBE, mampu menempatkan Manajemen Risiko SPBE sebagai agenda penting di dalam setiap pengambilan keputusan yang terkait dengan penerapan SPBE, dan memiliki komitmen yang kuat menerapkan Manajemen Risiko SPBE melalui penyediaan sumber daya yang cukup, baik anggaran, SDM, kebijakan, pedoman, maupun strategi penerapannya di Instansi Pusat dan Pemerintah Daerah.

b. Keterlibatan Semua Pihak

Budaya sadar Risiko SPBE melibatkan semua ASN yang terkait secara langsung maupun tidak langsung dengan penerapan SPBE, baik ASN yang berada pada KMR SPBE, UPR SPBE, maupun UKR SPBE, karena mereka yang paling memahami terjadinya Risiko SPBE dan cara penanganannya dalam level strategis maupun operasional.

c. Komunikasi

Komunikasi tentang pentingnya Manajemen Risiko SPBE harus dapat disampaikan kepada setiap ASN yang terlibat dalam penerapan SPBE melalui penyediaan saluran komunikasi yang variatif dan efektif. Tidak hanya KMR SPBE menyampaikan informasi terkait kebijakan Manajemen Risiko kepada ASN, tetapi juga ASN dapat menyampaikan informasi Risiko SPBE kepada pimpinan di setiap jenjang termasuk kepada KMR SPBE. Saluran komunikasi ini dapat diwujudkan melalui rapat-rapat pengambilan keputusan, berbagai pertemuan dalam proses Manajemen Risiko SPBE, dan penyampaian informasi melalui saluran komunikasi elektronik seperti surat elektronik, sistem naskah dinas elektronik, sistem aplikasi manajemen risiko, *video conference*, dan lain sebagainya.

d. Daya Responsif

Dalam budaya sadar Risiko SPBE, Risiko SPBE dieskalasi kepada pihak yang bertanggung jawab agar dapat ditangani dengan cepat. Sikap responsif ini sangat penting untuk mencegah ancaman yang dapat menghambat tercapainya tujuan penerapan SPBE ataupun meraih peluang untuk mempercepat tercapainya tujuan penerapan SPBE termasuk peningkatan kualitasnya. ASN yang responsif akan lebih siap beradaptasi terhadap perubahan dan penyelesaian masalah yang rumit dalam penerapan SPBE.

e. Sistem Penghargaan

KMR SPBE hendaknya memahami secara langsung permasalahan yang dialami oleh ASN pada pelaksanaan tugas UPR SPBE dan UKR SPBE, serta menjadikan pencapaian kinerja Risiko SPBE sebagai salah satu indikator dalam pemberian penghargaan dan sanksi.

f. Integrasi Proses

Proses Manajemen Risiko SPBE hendaknya diintegrasikan dengan proses manajemen di Instansi Pusat dan Pemerintah Daerah sehingga tidak dipandang sebagai tambahan beban pekerjaan. Integrasi proses dapat dilakukan dengan menyelaraskan proses Manajemen Risiko SPBE sebagai satu kesatuan dari setiap proses kegiatan, proses manajemen risiko, dan proses manajemen kinerja Instansi Pusat dan Pemerintah Daerah.

g. Program Kegiatan Berkelanjutan

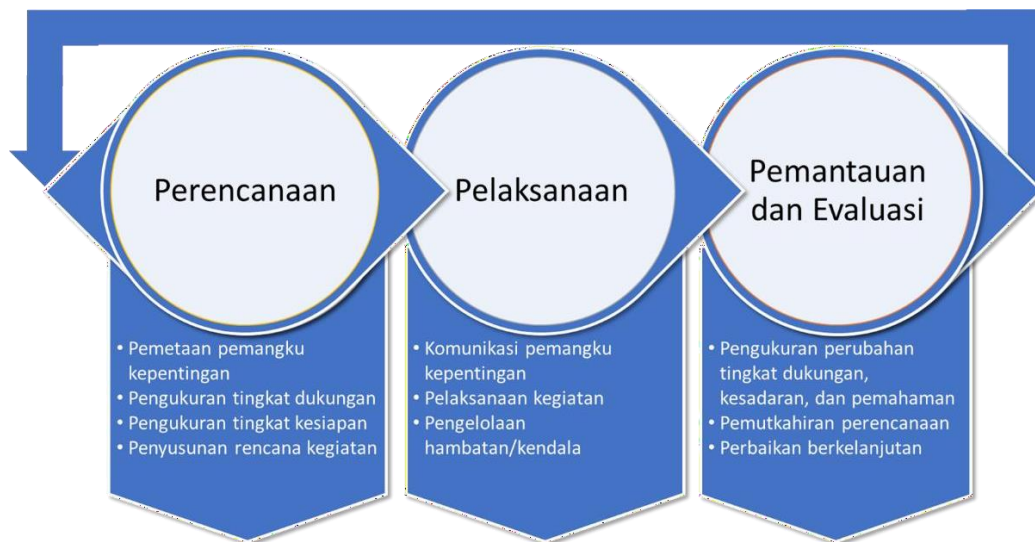
Agar budaya sadar Risiko SPBE dapat diterima oleh ASN, KMR SPBE hendaknya menyusun program kegiatan budaya sadar Risiko SPBE secara sistematis dan terencana, seperti kegiatan edukasi, berbagi pengetahuan, dan kunjungan kerja/supervisi ke UPR SPBE.

2. Langkah-Langkah Pengembangan

Pengembangan budaya sadar Risiko SPBE dapat dilakukan melalui langkah-langkah berikut ini:

- a. Menyusun perencanaan kegiatan budaya sadar Risiko SPBE;
- b. Melaksanakan kegiatan budaya sadar Risiko SPBE; dan
- c. Melakukan pemantauan dan evaluasi pelaksanaan kegiatan budaya sadar Risiko SPBE.

Langkah-langkah pengembangan budaya sadar Risiko SPBE dapat dilihat pada Gambar 6 di bawah ini.



Gambar 6. Langkah Pengembangan Budaya Sadar Risiko SPBE
Perencanaan kegiatan budaya sadar Risiko SPBE difokuskan pada:

- a. Pemetaan pemangku kepentingan terhadap pelaksanaan Manajemen Risiko SPBE.

Tujuan dari pemetaan pemangku kepentingan adalah untuk melakukan penilaian terhadap pemangku kepentingan terkait peran dan kapasitas mereka dalam mempengaruhi keberhasilan penerapan budaya sadar Risiko SPBE, serta untuk menyusun prioritas kegiatan budaya sadar Risiko SPBE berdasarkan tingkat kekuatan, posisi penting, ataupun pengaruh dari pemangku kepentingan. Dalam hal ini, pemangku kepentingan dapat diidentifikasi dengan merujuk pada struktur Manajemen Risiko SPBE yang mencakup KMR SPBE, UPR SPBE, dan UKR SPBE..

- b. Pengukuran tingkat dukungan pemangku kepentingan terhadap budaya sadar Risiko SPBE.

Hal ini menjadi penting untuk mengelola kegiatan budaya sadar Risiko SPBE secara efektif. Dukungan pemangku kepentingan dapat digolongkan ke dalam tiga kategori, yaitu: sangat mendukung secara konsisten, mendukung secara tidak konsisten, dan tidak mendukung atau resistan terhadap budaya sadar Risiko SPBE.

- c. Pengukuran tingkat kesiapan budaya sadar Risiko SPBE. Pengukuran ini biasanya menggunakan kuesioner yang disampaikan kepada pemangku kepentingan, baik secara sampel maupun semua populasi. Pengukuran dapat difokuskan antara lain pada komitmen, manfaat/dampak, pemahaman/kesadaran, tata cara/prosedur pelaksanaan, dan partisipasi dari pemangku kepentingan terhadap penerapan Manajemen Risiko SPBE.
- d. Penyusunan rencana kegiatan budaya sadar Risiko SPBE. Rencana kegiatan yang tepat disusun dengan mempertimbangkan sumber daya yang tersedia di Instansi Pusat dan Pemerintah Daerah seperti anggaran, waktu, sarana dan prasarana, SDM pelaksana, peserta, dan metode pelaksanaan. Metode pelaksanaan kegiatan budaya sadar Risiko SPBE mencakup antara lain pelatihan, seminar, sosialisasi, kelompok diskusi, berbagi pengetahuan dan pengalaman, konsultasi, pembimbingan/pendampingan, dan supervisi.

Pelaksanaan kegiatan budaya sadar Risiko SPBE difokuskan pada implementasi rencana kegiatan budaya sadar Risiko SPBE, yaitu:

- a. Melakukan komunikasi kepada pemangku kepentingan. Sebelum melaksanakan rencana kegiatan budaya sadar Risiko SPBE, rencana tersebut perlu dikomunikasikan kepada pemangku kepentingan dengan memberikan alasan-alasan yang rasional agar mendapatkan dukungan pelaksanaan oleh pemangku kepentingan.
- b. Mengelola hambatan/kendala. Dalam pelaksanaan kegiatan budaya sadar Risiko SPBE, kendala-kendala yang terjadi agar dikelola dengan baik agar tujuan dari kegiatan tersebut dapat dicapai.

Pemantauan dan evaluasi kegiatan budaya sadar Risiko SPBE ditujukan untuk meningkatkan budaya sadar Risiko SPBE melalui perbaikan berkelanjutan. Pelaksanaan pemantauan dan evaluasi difokuskan pada:

- a. Pengukuran perubahan tingkat dukungan, kesadaran, dan pemahaman dari pemangku kepentingan terhadap penerapan Manajemen Risiko SPBE. Pengukuran terkait hal ini dapat dilakukan melalui pengumpulan dan analisis umpan balik dari pemangku kepentingan dengan cara supervisi ke unit-unit para pemangku

kepentingan. Hasil analisis selanjutnya digunakan untuk memutakhirkan tingkat dukungan, kesadaran, dan pemahaman dari pemangku kepentingan, serta memberikan saran-saran perbaikan terhadap kegiatan budaya sadar Risiko SPBE.

b. Pemutakhiran rencana kegiatan budaya sadar Risiko SPBE.

Rencana kegiatan budaya sadar Risiko SPBE dilakukan pemutakhiran berdasarkan saran-saran perbaikan dengan tetap mempertimbangkan ketersediaan sumber daya yang dimiliki oleh Instansi Pusat dan Pemerintah Daerah.

c. Pelaksanaan perbaikan berkelanjutan.

Rencana kegiatan budaya sadar Risiko SPBE yang telah dimutakhirkan dilaksanakan melalui langkah ke dua di atas sehingga mencapai peningkatan budaya sadar Risiko SPBE

BAB V

PENUTUP

Penerapan Manajemen Risiko SPBE mutlak diperlukan untuk lebih menjamin pencapaian tujuan dan keberlangsungan dari SPBE. Pelaksanaan Manajemen Risiko SPBE diawali dengan penyusunan dan penetapan kerangka kerja Manajemen Risiko SPBE yang terintegrasi dengan proses kerja di BSSN. Kerangka kerja Manajemen Risiko SPBE mencakup prinsip, kepemimpinan dan komitmen, proses Manajemen Risiko SPBE, dan tata kelola Manajemen Risiko SPBE. Dalam pelaksanaannya, kerangka kerja Manajemen Risiko SPBE dapat disesuaikan dengan kondisi unit kerja masing-masing.

Agar Manajemen Risiko SPBE dapat diimplementasi dengan baik, diperlukan peran serta seluruh pihak maupun pemangku kepentingan lain. Koordinasi dan kolaborasi yang baik dengan seluruh elemen termasuk sistem yang telah berjalan di BSSN menjadi kunci keberhasilan pelaksanaan Manajemen Risiko SPBE

Pedoman ini diharapkan dapat bermanfaat dan dijadikan acuan dalam pengintegrasian layanan publik di lingkungan BSSN.

Ditetapkan di Depok

pada tanggal Nopember 2022

A.n. KEPALA BADAN SIBER DAN SANDI NEGARA

KEPALA PUSAT DATA DAN TEKNOLOGI
INFORMASI KOMUNIKASI



FERDINAND MAHULETTE, S.E.

LAMPIRAN 2

STANDAR OPERASIONAL PROSEDUR (SOP)

PENILAIAN RISIKO (RISK ASSESMENT)



STANDAR OPERASIONAL PROSEDUR PENILAIAN RISIKO KEAMANAN INFORMASI (*RISK ASSESMENT*)

2022

BADAN SIBER DAN SANDI NEGARA

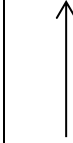
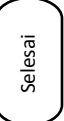
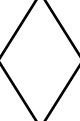
Alamat : JALAN RAYA MUCHTAR NO. 70, KEL. BOJONGSARI LAMA, KEC. BOJONGSARI, DEPOK,

 BADAN SIBER DAN SANDI NEGARA PUSAT DATA DAN TEKNOLOGI INFORMASI KOMUNIKASI		Nomor SOP	:	/P2/11/2022
		Tanggal Pembuatan	:	Nopember 2022
		Tanggal Revisi	:	-
		Tanggal Efektif	:	Nopember 2022
		Disahkan Oleh	:	
		Nama SOP	:	Penilaian Risiko Keamanan Informasi (Risk Assessment)

Dasar Hukum		Kualifikasi Pelaksana	
1	Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik	1	Memahami substansi pelaksanaan Penilaian Risiko Keamanan Informasi
2	Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik	2	Dapat mengoperasikan komputer
3	Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan Pada Penyelenggaraan Sistem Elektronik		

4	Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik	
5	Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara	
6	Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2019 tentang Pedoman Penyusunan SOP di Lingkungan Badan Siber dan Sandi Negara	
Keterkaitan SOP		Peralatan/Perlengkapan
		1 ATK 2 Komputer dan Jaringan Internet 3 Printer 4 Risk Register
Peringatan		Pencatatan & Pendataan
Apabila SOP ini tidak dibuat maka akan menyebabkan pelaporan layanan menjadi tidak memiliki standar, dan akan menghambat proses pelaporan layanan secara keseluruhan		1 Poin-poin hasil pelaksanaan penilaian risiko

Keterangan Simbol :

	Proses mulai		Alur ke proses berikutnya
	Proses		Proses berakhir
	Dokumen / Formulir		Pilihan

Keterangan Pelaksana:

- PSE adalah penyelenggara sistem elektronik (K/L/D)
- Tim Teknis adalah pegawai unit kerja bidang keamanan TIK
- Bagian Administrasi adalah bagian TU unit kerja.
- Pimpinan Unit Kerja adalah pimpinan unit kerja (Pejabat Eselon 2)

Prosedur Penilaian Risiko Keamanan Informasi (Risk Assessment)

Lampiran Nota Dinas

Nomor :

Tanggal :

NO	KEGIATAN	PELAKSANA				MUTU BAKU			KETERANGAN
		PSE	BAGIAN ADMINISTRASI	TIM TEKNIS	PIMPINAN UNIT KERJA	KELENGKAPAN	WAKTU	OUTPUT	
1	PSE mengajukan Permohonan Kegiatan Penilaian Risiko Keamanan Informasi					Data Dukung Lingkup Penilaian Risiko	5 menit	Surat Permohonan	
2	Bagian Administrasi Menerima Pengajuan Permohonan dan Penyiapan Permohonan ke Pimpinan Unit Kerja					Surat Permohonan	5 menit	Lampiran Nota Dinas	
3	Pimpinan Unit Kerja Menyetujui Permohonan dan Melakukan Disposisi Surat Permohonan Penilaian Risiko Keamanan Informasi					Surat Permohonan	10 Menit	Disposisi Surat Permohonan	
4	Bagian Administrasi Memberikan Surat Jawaban Kesiadaan atas Permohonan Kegiatan Penilaian Risiko Keamanan Informasi dan Menyiapkan Surat Penetapan Tim Teknis Pelaksana					Daftar Tim Teknis Pelaksana	10 menit	Surat Jawaban Kepada PSE dan Draf Surat Perintah Tim Teknis Pelaksana	

NO	KEGIATAN	PELAKSANA				MUTU BAKU			KETERANGAN
		PSE	BAGIAN ADMINISTRASI	TIM TEKNIS	PIMPINAN UNIT KERJA	KELENGKAPAN	WAKTU	OUTPUT	
			1						
5	Pimpinan Unit Kerja Mengesahkan Surat Penetapan Tim Teknis Pelaksana					Draf Surat Perintah Tim Teknis Pelaksana	10 menit	Surat Perintah Tim Teknis Pelaksana	
6	Tim Teknis Berkoordinasi terkait dengan perencanaan dan persiapan penilaian risiko kepada PSE					Data Dukung Lingkup Penilaian Risiko	1 hari	Dokumen Konteks Penilaian Risiko	
7	Tim Teknis melaksanakan Identifikasi Risiko					Dokumen Konteks Penilaian Risiko	2 hari	Dokumen Identifikasi Risiko	
8	Tim Teknis melaksanakan Analisis Risiko					Dokumen Identifikasi Risiko	1 hari	Dokumen Analisis Risiko	
9	Tim Teknis melaksanakan Evaluasi Risiko					Dokumen Analisis Risiko	2 hari	Dokumen Evaluasi Risiko	
10	Tim Teknis Menyusun Laporan Penilaian Risiko					Dokumen Konteks, Identifikasi, Analisis dan Evaluasi Penilaian Risiko	2 hari	Draf Laporan Penilaian Risiko	
			2		3				

NO	KEGIATAN	PELAKSANA				MUTU BAKU			KETERANGAN
		PSE	BAGIAN ADMINISTRASI	TIM TEKNIS	PIMPINAN UNIT KERJA	KELENGKAPAN	WAKTU	OUTPUT	
			2		3				
11	Bagian Administrasi menyerahkan Draf Laporan					Draf Laporan Penilaian Risiko	5 menit	Nodin Draf Laporan Penilaian Risiko	
12	Pimpinan Unit Kerja mengoreksi Draf Laporan Penilaian Risiko Ya, jika tidak ada koreksi lanjut ke poin 13 Tidak, jika ada koreksi kembali ke poin 10					Draf Laporan Penilaian Risiko	30 menit	Laporan Penilaian Risiko	
13	Pimpinan Unit Kerja mengesahkan Laporan Penilaian Risiko					Laporan Penilaian Risiko	5 menit	Laporan Penilaian Risiko	
14	Bagian Administrasi Menyerahkan Laporan Penilaian Risiko kepada PSE					Laporan Penilaian Risiko	5 menit	Laporan Penilaian Risiko	
15	PSE menerima Hasil Laporan Penilaian Risiko Keamanan Informasi	Selesai				Laporan Penilaian Risiko	5 menit	Laporan Penilaian Risiko	

LAMPIRAN 3

**PETUNJUK TEKHNIS (JUKNIS)
PENILAIAN RISIKO (RISK ASSESMENT)**



BADAN SIBER DAN SANDI NEGARA

Jalan Raya Muchtar Nomor 70, Kel. Bojongsari Lama, Kec. Bojongsari, Depok 16518

Telepon (021) 7805814, Faksimile (021) 78844104,

Website: <http://www.bssn.go.id>, E-mail: humas@bssn.go.id

PETUNJUK TEKNIS

PENILAIAN RISIKO KEAMANAN INFORMASI (RISK ASSESSMENT)

BAB I PENDAHULUAN

A. Umum

Hal mendasar yang menjadi perhatian Pusat Data dan Teknologi Informasi Komunikasi (Pusdatik) dalam memberikan layanan ke Penyelenggara Sistem Elektronik (PSE) adalah pelaksanaan kegiatan penilaian risiko keamanan informasi (*Risk Assessment*). Penilaian risiko Keamanan Informasi dilaksanakan untuk mengidentifikasi dan menilai risiko-risiko yang dihadapi oleh Badan Siber dan Sandi Negara dan menentukan langkah-langkah mitigasi risiko yang tepat, serta sebagai bagian dari pengelolaan keamanan siber.

Seiring dengan meningkatnya permohonan kebutuhan layanan penilaian risiko keamanan informasi oleh PSE sektor Pemerintah perlu di rumuskan landasan proses kerja dalam pelaksanaan kegiatan tersebut. Untuk mendukung pelaksanaan tersebut, Pusdatik telah menyiapkan proses bisnis dan langkah kerja dalam melaksanakan kegiatan penilaian risiko keamanan informasi.

B. Maksud dan Tujuan

Maksud disusunnya petunjuk teknis ini adalah untuk memberikan panduan kepada tim pelaksana teknis dalam melaksanakan kegiatan penilaian risiko keamanan informasi.

Adapun tujuannya adalah:

1. Menjelaskan langkah-langkah Perencanaan dan Persiapan
2. Menjelaskan langkah-langkah Penetapan konteks
3. Menjelaskan langkah-langkah Penilaian Risiko

C. Ruang Lingkup

Ruang lingkup petunjuk teknis ini terbatas pada pelaksanaan penilaian risiko yaitu Identifikasi Risiko, Analisis Risiko dan Evaluasi Risiko.

D. Referensi

- Pedoman Pengelolaan Risiko - Kerangka Kerja Keamanan Siber Sektor Pemerintah
- ISO 31000 - Risk Management

E. Pengertian

1. Risiko adalah segala sesuatu yang berdampak negatif terhadap pencapaian tujuan yang diukur berdasarkan kemungkinan dan dampaknya.
2. Penilaian Risiko (*Risk Assessment*) adalah kegiatan untuk:
 - Menentukan prioritas risiko berdasarkan peluang terjadinya gangguan kegiatan dan Layanan TIK Utama;
 - Mengidentifikasi ancaman-ancaman terhadap kegiatan dan Layanan TIK Utama;
 - Mengidentifikasi kelemahan yang dapat meningkatkan risiko berdasarkan ancaman yang ada
3. Ancaman (*threat*) adalah potensi/kemungkinan suatu sumber ancaman untuk mengeksploitasi suatu kelemahan (*vulnerability*).
4. Kerawanan/Kerentanan (*vulnerability*) adalah kekurangan atau kerentanan dalam prosedur, rancangan, dan implementasi keamanan sistem, atau kontrol internal yang dapat dieksploitasi sehingga menyebabkan pelanggaran terhadap kebijakan keamanan sistem.

BAB II

PELAKSANAAN

Penilaian risiko merupakan satu rangkaian dalam proses Risiko Manajemen. Risiko dapat diartikan suatu peluang terjadinya sesuatu rangkaian peristiwa yang bisa berdampak negatif/mengancam pencapaian tujuan dan atau sasaran organisasi. Manajemen Risiko sendiri merupakan pendekatan sistematis yang meliputi budaya, proses, dan struktur untuk menentukan tindakan terbaik terkait risiko yang dihadapi dalam pencapaian tujuan/sasaran organisasi.

Untuk melakukan Manajemen Risiko dilingkungan BSSN ditetapkan proses sebagai berikut:

A. Perencanaan Risiko 1. Ruang Lingkup Penilaian Risiko

Ruang lingkup penilaian risiko ini hanya terkait dengan risiko-risiko berdasarkan pada aset/proses bisnis/layanan yang berhubungan dengan keamanan siber dan diidentifikasi berdasarkan kerentanan dan ancaman siber yang ada pada aset/proses bisnis/layanan tersebut. Dan nilai risiko yang dihasilkan adalah kombinasi dari besarnya kemungkinan dan dampak yang ditimbulkan dari risiko siber yang telah diidentifikasi.

2. Jadwal dan Detil Aktivitas

Pelaksanaan Penilaian Risiko keamanan siber disyaratkan untuk dilaksanakan oleh setiap instansi/organisasi dengan mengikuti penjadwalan kegiatan yang dimiliki PSE maupun Tim Pelaksana yang telah ditetapkan oleh instansi/organisasi masing-masing. Pelaksanaan Penilaian Risiko ini perlu dilakukan berdasarkan kesepakatan dan dilakukan proses monitoring pelaksanaan.

3. Pelaksana Penilaian Risiko

Peran dan tanggungjawab dalam pelaksanaan penilaian risiko sebagaimana tercantum dalam Tabel 1 atau disesuaikan dengan organisasi/instansi masingmasing

Table 1 Peran dan Tanggungjawab Penilaian Risiko

Peran	Tanggungjawab
<i>Top Level Management</i>	- Bertanggungjawab terhadap rencana beserta risiko yang melekat pada proses bisnis/aset suatu organisasi. - Pengambil keputusan terhadap hasil penilaian risiko dan rencana penanganan risiko pada instansi/organisasi. - Memiliki komitmen dalam perbaikan yang berkelanjutan untuk instansi/organisasi. - Monitoring dan review hasil penilaian risiko. - Menetapkan kebijakan, prosedur, atau peraturan yang berkaitan dengan penilaian risiko keamanan siber.
<i>Middle Level Management</i>	- Memastikan bahwa penilaian risiko dilaksanakan sesuai dengan kebijakan, prosedur atau peraturan yang telah ditetapkan. - Monitoring dan review terkait proses pelaksanaan penilaian risiko. - Memantau pelaksanaan rencana penanganan risiko.
Tim Pelaksana Penilaian Risiko	- Melaksanakan penilaian risiko sesuai dengan kebijakan, prosedur atau peraturan yang telah ditetapkan. - Memberikan masukan kepada <i>middle level</i> dan <i>top level management</i> berkaitan dengan hasil evaluasi risiko dan rekomendasi penanganan risiko. - Melaporkan pelaksanaan penilaian risiko

4. Penetapan Konteks

Dalam penilaian risiko diperlukan ditetapkan tujuan, ruang lingkup (eksternal maupun internal) serta kriteria-kriteria (kemungkinan, dampak, nilai risiko, penerimaan dan penanganan risiko) sebagaimana yang telah dijelaskan pada Bagian Kriteria Penilaian Risiko. Penetapan konteks perlu disesuaikan dengan karakteristik dan kondisi masing-masing instansi/organisasi.

B. Identifikasi Risiko

Pengambilan identifikasi risiko dapat dilakukan sebagai berikut:

- Melakukan identifikasi aktifitas/kegiatan dari elemen risiko;
- Melihat faktor risiko yang timbul;

- Proses terjadinya risiko yang mengakibatkan dampak pada organisasi;
- Melakukan dokumentasi terhadap identifikasi risiko.

Beberapa hal yang harus diperhatikan detail dalam identifikasi risiko sebagai berikut:

1. Menetapkan Element Risiko

Penetapan identifikasi risiko memerlukan dokumentasi dan analisis elemen – elemen yang terdiri dari risiko

- Koneskuensi yang terkait dengan asset tertentu.
- Ancaman terhadap asset tersebut, yang membutuhkan dorongan dan kemampuan.
- Kerentanan yang spesifik terhadap ancaman keamanan.

Table 2 elemen risiko

Ketentuan	Pengertian
Asset	sesuatu yang bernilai tangible atau intangible dilindungi, termasuk manusia, informasi, infrastruktur, keuangan dan reputasi
Asset value	nilai aset yang dapat diukur dengan nilai mata uang. Hal ini baik yang akan dibayar atau diterima oleh organisasi.
Impact	Besarnya kerugian akibat ancaman yang mengeksploitasi kerentanan
Impact analysis	Sebuah studi untuk memprioritaskan kekritisian sumber daya informasi untuk perusahaan berdasarkan biaya (atau konsekuensi) dari efek samping. Dalam analisis dampak, ancaman terhadap aset diidentifikasi dan potensi kerugian bisnis ditentukan untuk periode waktu yang berbeda. Penilaian ini digunakan untuk membenarkan sejauh mana perlindungan yang diperlukan dan kerangka waktu pemulihan. Analisis ini merupakan dasar untuk menetapkan strategi pemulihan.
Impact assessment	Tinjauan tentang kemungkinan konsekuensi dari suatu risiko
Likelihood	Kemungkinan sesuatu terjadi, atau yang akan mungkin sering terjadi.
Threat	Apa pun (misalnya, objek, zat, manusia) yang mampu bertindak melawan aset dengan cara yang dapat mengakibatkan kerugian
Threat agent	Metode dan hal-hal yang digunakan untuk mengeksploitasi kerentanan, seperti tekad, kemampuan, motif, dan sumber daya
Ketentuan	Pengertian
Threat analysis	Evaluasi jenis, ruang lingkup dan sifat peristiwa atau tindakan yang dapat mengakibatkan konsekuensi yang merugikan; identifikasi ancaman yang ada terhadap aset perusahaan

Threat vector	Jalur atau rute yang digunakan oleh musuh untuk mendapatkan akses ke target
Vulnerability	Kelemahan dalam desain, implementasi, operasi, atau pengendalian internal dari suatu proses yang dapat mengekspos sistem terhadap ancaman yang merugikan dari peristiwa ancaman
Vulnerability analysis	Sebuah proses mengidentifikasi dan mengklasifikasikan kerentanan aset.
Vulnerability scanning	Proses otomatis untuk secara proaktif mengidentifikasi kelemahan keamanan dalam jaringan atau sistem individu .

2. Faktor Risk Analisis

Proses pembuatan factor risiko menentukan apakah risiko tersebut menjadi acuan utaman dalam penananganan risiko atau tidak.

Beberapa proses untuk menetapkan risiko dari risk factor sebagai berikut: a.

- Menetakan agen pembawa ancaman (threat agent);
- b. Menetapkan ancaman;
- c. Munculnya ancaman sebagai celah keamanan;
- d. Risiko dihitung dari celah keamanan yang muncul;
- e. Dampak terhadap asset yang telah ditentukan.

3. Pengaruh Risiko terhadap Aset

Aset adalah sesuatu yang bernilai baik berwujud atau tidak berwujud yang layak dilindungi. Contoh aset yang biasa ditemukan dalam organisasi meliputi:

- Informasi
- Reputasi
- Merek
- Hak milik intelektual
- Fasilitas
- Peralatan
- Uang tunai dan investasi
- Daftar pelanggan
- Riset
- Orang/Pegawai/Pengelola
- Layanan/proses bisnis

4. Ancaman

Ancaman dapat didefinisikan sebagai/bersifat internal atau eksternal, disengaja atau tidak disengaja, disebabkan keterbatasan infrastuktur system. Sebab lain yang dapat menjadi ancaman adalah peristiwa alam, faktor politik, ekonomi, atau persaingan. Ancaman dapat terjadi atau mungkin terjadi diluar kendali penanganan risiko atau kendali pemilik asset.

C. Analisis Risiko

Proses analisis risiko mempertimbangkan 3 (tiga) komponen yaitu ancaman, kerentanan, dan dampak. Pada tahapan ini dilakukan penentuan nilai kemungkinan, nilai dampak, dan penghitungan nilai risiko dengan penjelasan sebagai berikut:

1. Penentuan Nilai Kemungkinan

Nilai kemungkinan yang dimaksud dalam tahapan ini adalah frekuensi kejadian dimana kerentanan dan ancaman itu muncul pada suatu aset/layanan/proses bisnis yang ada pada instansi/organisasi. Penentuan nilai kemungkinan dalam panduan ini menggunakan kriteria kemungkinan atau disesuaikan dengan kriteria kemungkinan yang telah ditetapkan oleh masing-masing instansi/organisasi.

Table 3 *Tingkat Kriteria Kemungkinan Risiko*

No	Tingkat Peluang Kejadian	Kriteria Kemungkinan/Frekuensi
1	Jarang	Misal: Kejadian tidak lebih dari 2 kali per tahun; atau Kejadian rata-rata tidak lebih dari 1 kali setiap enam bulan
2	Kemungkinan Kecil	Misal: Kejadian lebih dari 2 kali / tahun, namun tidak lebih dari 5 kali / tahun; atau Kejadian rata-rata tidak lebih dari 2 kali setiap enam bulan
3	Mungkin	Misal: Kejadian lebih dari 5 kali / tahun, namun tidak lebih dari 8 kali / tahun; atau Kejadian rata-rata tidak lebih dari 1 kali setiap bulan
4	Kemungkinan Besar	Misal: Kejadian lebih dari 8 kali / tahun, namun tidak lebih dari 10 kali / tahun; atau Kejadian rata-rata tidak lebih dari 1 kali setiap bulan
5	Hampir Pasti	Misal: Kejadian lebih dari 10 kali / tahun; atau Kejadian rata-rata lebih dari 1 kali setiap bulan

2. Penentuan Nilai Dampak

Nilai dampak yang dimaksud dalam tahapan ini adalah besarnya dampak yang diakibatkan oleh eksploitasi kerentanan berdasarkan hasil identifikasi yang telah dilakukan. Dampak yang ditimbulnya dapat berupa dampak terhadap finansial, operasional, hukum, reputasi, dan sebagainya. Penentuan nilai dampak menggunakan kriteria dampak yang telah ditetapkan oleh masing-masing instansi/organisasi.

Table 4 Tingkat kriteria dampak risiko

Nilai	Tingkat	Reputasi	Operasional	Finansial	Hukum
1	Sangat Kecil	Tidak ada pemberitaan negatif	Penundaan proses bisnis antara 0 sampai dengan 30 menit	Kerugian dan/atau adanya pengeluaran biaya sampai dengan maksimal sebanding dengan 0 – 5% revenue/pendapatan	Terdapat teguran
2	Kecil	Terdapat pemberitaan negatif namun tidak mengakibatkan penurunan kepercayaan pemangku kepentingan (stakeholder)	Penundaan proses bisnis antara 30 menit sampai dengan maksimal 1 jam.	pengeluaran biaya sampai dengan maksimal sebanding dengan 6 – 10% revenue/pendapatan	Terdapat permasalahan hukum (misal: pelanggaran) namun belum menjadi tuntutan hukum
Nilai	Tingkat	Reputasi	Operasional	Finansial	Hukum
3	Menengah	Terdapat pemberitaan negatif yang dapat mempengaruhi kepercayaan sebagian kecil dari stakeholder	Penundaan proses bisnis antara 1 jam sampai dengan maksimal 3 jam	pengeluaran biaya sampai dengan maksimal sebanding dengan 11 – 20% revenue/pendapatan	Tuntutan hukum dengan dampak relatif kecil
4	Besar	Terdapat pemberitaan negatif yang dapat mengakibatkan penurunan kepercayaan sebagian besar dari stakeholder	Penundaan proses bisnis antara 3 jam sampai dengan maksimal 5 jam	pengeluaran biaya sampai dengan maksimal sebanding dengan 20 – 30% revenue/pendapatan	Tuntutan hukum yang berdampak pada kinerja/performa organisasi
5	Sangat Besar	Terdapat pemberitaan negatif yang dapat menghilangkan kepercayaan dari stakeholder	Penundaan proses bisnis lebih dari 5 jam	pengeluaran biaya sampai dengan maksimal lebih dari 30% revenue/pendapatan	Tuntutan hukum yang mengancam eksistensi dan manajemen puncak organisasi

3. Penghitungan Nilai Risiko

Penghitungan nilai risiko dihasilkan dari kombinasi nilai kemungkinan dan nilai dampak yang telah ditentukan dengan formula penghitungan sebagai berikut:

$\text{Nilai risiko} = \text{Nilai kemungkinan berbanding Nilai Dampak}$
--

Dalam penetapan nilai risiko diperlukan matriks risiko untuk mempermudah dalam memberikan gambaran kondisi risiko hasil penilaian yang telah dilakukan.

Table 5 Matriks Nilai Risiko

Tingkat Risiko			Tingkat Dampak				
			1	2	3	4	5
			Sangat Kecil	Kecil	Menengah	Besar	Sangat Besar
Tingkat kemungkinan	5	Hampir Pasti	9	15	18	23	25
	4	Kemungkinan besar	6	12	16	19	24
	3	Mungkin	4	10	14	17	22
	2	Kemungkinan Kecil	2	7	11	13	21
	1	Jarang	1	3	5	8	20

Catatan:

Angka dalam kolom:

- Bukan merupakan hasil perkalian secara matematis** antara tingkat kemungkinan dengan tingkat dampak.
- Merupakan nilai baku dan berlaku untuk seluruh satuan kerja/unit kerja.
- Menunjukkan nilai besaran risiko (1 sd 25), misalnya:
 - Jika tingkat kemungkinan risiko = 1 (sangat jarang) dan tingkat dampak risiko = 5 (sangat besar) maka nilai besaran risikonya = 20 (sangat tinggi).
 - Jika tingkat kemungkinan risiko = 5 (sangat sering) dan tingkat dampak risiko = 1 (sangat kecil) maka nilai besaran risikonya = 9 (Rendah).

Besaran Risiko	Tingkat Risiko	Warna
1 – 5	Sangat Rendah	Hijau Muda
6 – 11	Rendah	Hijau
12 – 15	Sedang	Kuning
16 - 19	Tinggi	Orange
20 – 25	Sangat Tinggi	Merah

D. Evaluasi Risiko

Pada proses evaluasi risiko dilakukan penetapan prioritas risiko untuk menentukan risiko yang diterima dan risiko yang perlu dilakukan penanganan atau rencana perbaikan. Instansi/organisasi disyaratkan memiliki toleransi risiko yang menjadi batas maksimal suatu risiko dapat diterima. Untuk mempermudah dalam melakukan evaluasi risiko diperlukan suatu matrik penerimaan risiko beserta toleransi risiko yang ditetapkan.

Table 6 Kriteria Penerimaan Risiko

Penerimaan Risiko	Definisi
Risiko diterima	Keputusan untuk menerima risiko, manajemen harus membuat keputusan untuk mengizinkan atau mengambil risiko tanpa berusaha mengurangi kemungkinan atau dampaknya.
Perlu dilakukan penanganan	Tindakan harus diambil untuk mengurangi kemungkinan risiko atau dampak risiko. Mengurangi risiko untuk mencapai kondisi yang dapat diterima sesuai dengan selera risiko. Beberapa kontrol mungkin dilakukan untuk memitigasi risiko.
Perlu dihindari	Organisasi berhenti dari aktivitas atau kondisi yang menimbulkan risiko. Penghindaran harus sering dilaksanakan ketika tidak ada respons efektif ataupun tidak ada biaya dan sumber daya yang tersedia untuk risiko yang dianggap tidak dapat diterima oleh manajemen.
Berbagi Risiko	Berbagi risiko yang berarti mentransfer sebagian atau semua dampak risiko tersebut ke pihak lain

Table 7 Kriteria Prioritas

Level Risiko	Rasio Manfaat/Sumber Daya			
	Manfaat Rendah, Sumber daya tidak tersedia	Manfaat Tinggi, Sumber daya tidak tersedia	Manfaat sedang, sumber daya tersedia	Manfaat Tinggi, sumber daya tersedia
Sangat Tinggi	Segera	Segera	Sangat Segera	Sangat Segera
Tinggi	Segera	Segera	Sangat Segera	Sangat Segera
Sedang	Segera	Segera	Segera	Segera
Rendah	Biasa	Biasa	Segera	Segera
Sangat Rendah	Biasa	Biasa	Segera	Segera

E. Monitor dan Review Risiko

Menentukan Monitor dan Review setelah melakukan Penilaian dan Evaluasi. Pada proses Monitor dan Review risiko ditetapkan sebagai berikut:

1. Menentukan Key Risk Indikator;
2. Membuat KPI berdasarkan KRI;
3. Melakukan maturity terhadap risiko;
4. Melakukan monitor terhadap asset dengan menerapkan sentralisasi log dan monitoring aktifitas dalam log asset TI.

F. Komunikasi dan Konsultasi Risiko

Proses komunikasi ditetapkan dalam organisasi kepada stakeholder organisasi dalam proses pemantauan risiko. Proses dalam melakukan komunikasi dan konsultasi didapatkan sebagai berikut:

1. Stakeholder menerima laporan yang telah dibuat dalam proses analisis risiko, monitoring dan review risiko;
2. Stakeholder membuat meeting komite dalam hitungan masa: bulanan, triwulan, semester, tahunan;
3. Stakeholder menetapkan penanganan risiko terhadap risiko yang tidak dapat dikendalikan;
4. Stakeholder menetapkan kriteria *Risk Acceptance* untuk risiko yang tidak dapat dikendalikan;
5. Stakeholder menetapkan control terhadap risiko yang tidak dapat ditutup atau dikontrol.

BAB III PENUTUP

Demikian Petunjuk Teknis Penilaian Risiko Pemerintah (*Risk Assessment*) ini dibuat. Dengan adanya petunjuk teknis ini diharapkan pelaksanaan kegiatan Identifikasi Kerentanan dan Penilaian Risiko dapat berjalan dengan baik dan lancar.

KEPALA PUSAT DATA DAN TEKNOLOGI
INFORMASI KOMUNIKASI



FERDINAND MAHULETTE, S.E.

Lampiran

Table 8 Form Penilaian Risiko

1. Tahun	:	diisi dengan tahun proses manajemen risiko						
2. Pemilik Risiko	:	diisi dengan nama satuan/unit kerja level jabatan administrator/unit pelaksana teknis						
3. Pengelola Risiko	:	diisi dengan nama satuan/unit kerja level jabatan pengawas						
4. Proses Bisnis	:	diisi dengan nama kegiatan dimana manajemen risiko diterapkan						
5. Tujuan	:	diisi dengan uraian tujuan kegiatan						
6. <i>Output</i>	:	diisi dengan uraian <i>output</i> kegiatan						
7. <i>Outcome</i>	:	diisi dengan uraian <i>outcome</i> yang berkaitan dengan kegiatan						
8. Kriteria Risiko								
a. Kriteria Tingkat Kemungkinan								
	Tingkat Kemungkinan	Uraian						
	1 Sangat Jarang	Diisi dengan rumusan kriteria kemungkinan risiko. <i>Misalnya:</i> 1. Jarang – Jika Kejadian tidak lebih dari 2 kali per tahun; atau Kejadian rata-rata tidak lebih dari 1 kali setiap enam bulan 2. Jarang -						
	2 Jarang							
	3 Kadang							
	4 Sering							
	5 Sering Sekali							
b. Kriteria Tingkat Dampak								
	Tingkat Dampak	Uraian						
	1 Sangat Kecil	Diisi dengan rumusan kriteria dampak risiko. <i>Misalnya:</i> 1. Menengah - Pengeluaran biaya sampai dengan maksimal sebanding dengan 11 – 20% revenue/pendapatan,-. 2. Besar -						
	2 Kecil							
	3 Menengah							
	4 Besar							
	5 Besar Sekali							
9. Tabel Analisis Risiko dan Tingkat Risiko								
Tingkat Risiko			Tingkat Dampak					
			1	2	3	4	5	
			Sangat Kecil	Kecil	Menengah	Besar	Sangat Besar	
Tingkat Kemungkinan	5	Hampir Pasti	9	15	18	23	25	
	4	Kemungkinan besar	6	12	16	19	24	
	3	Mungkin	4	10	14	17	22	
	2	Kemungkinan Kecil	2	7	11	13	21	
	1	Jarang	1	3	5	8	20	

Table 9 List Risk Register

NO	ASET/ PROSES/ LAYANAN	DESKRIPSI RISIKO DAMPAK TANPA KONTROL (INHERENT <i>RISK IMPACT DESCRIPTION</i>)			PENGENDALIAN YANG ADA (EXISTING CONTROL)	RISIKO SAAT IN (CURRENT RISK)			KEPUTUSAN	PRIORITAS
		Kerawanan/ker entanan(<i>Vulner ability</i>)	Ancaman CIA (<i>Threat</i>)	Uraian Dampak (<i>Impact Description</i>)		Nilai Kemungkinan (Likelihood Scale)	Nilai Dampak (Impact Scale)	Nilai Risiko (Risk Score)		
Aset (Perangkat keras, Perangkat Lunak, informasi), Proses Bisnis, Layanan										

Table 10 Risk Register

Ref:		Nama: Manajemen Risiko IT			
Dampak terhadap Aset:					
Tingkat Kemungkinan	Tingkat Dampak	Dampak Level CIA			Level Risiko
		Confidentiality	Integrity	Availability	
Rekomendasi:				Status	Tingkat Risiko Sisa
1. Pengelolaan risiko disetujui					

Contoh Surat perintah

		Kop surat
SURAT PERINTAH NOMOR .../.../.../...		Penomoran yang berurutan dalam satu tahun kalender
Menimbang :	a. bahwa; b. bahwa;	Memuat peraturan / dasar ditetapkan-nya Surat Perintah
Dasar :	1.; 2.;	
Memberi Perintah		
Kepada :	1.; 2.; 3.; 4. dan seterusnya.	Daftar pejabat yang menerima perintah
Untuk :	1.; 2.; 3.; 4. dan seterusnya.	Memuat substansi arahan yang diperintahkan
Nama Tempat, Tanggal		Kota sesuai alamat instansi dan tanggal
Nama Jabatan,		
Tanda Tangan dan Cap Instansi		Nama jabatan dan nama lengkap ditulis dengan huruf awal kapital
Nama Lengkap		
Tembusan:		
1.;		
2.;		
3.;		
dan seterusnya.		

Contoh nota dinas

XXXXXX	}	Nama Instansi
NOTA DINAS NOMOR .../.../.../BULAN/TAHUN		
Yth. :	}	Penomoran yang berurutan dalam satu tahun kalender
Dari :		
Hal :	}	Memuat laporan, pemberitahuan, pernyataan, atau permintaan yang sifatnya rutin, berupa catatan ringkas.
Tanggal:		
.....		
.....		
.....		
.....	}	Nama lengkap ditulis dengan huruf awal kapital, tidak dibubuhi cap dinas
Tanda Tangan		
Nama Lengkap		
Tembusan:		
1.		
2.		
3.		

LAMPIRAN 4

RAPAT PEMBENTUKAN TIM EFEKTIF



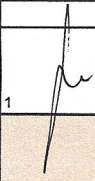
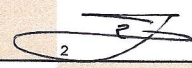
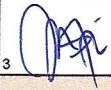
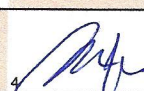
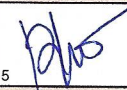
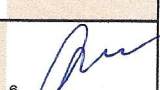
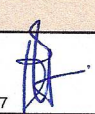
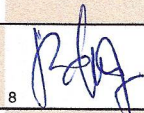
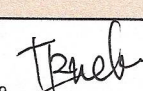
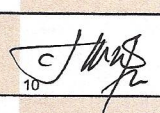
MENGHADAP WAKA BSSN DAN MEMINTA ARAHAN



MENGHADAP KAPUSDATIK BSSN DAN MEMINTA ARAHAN



**RAPAT PEMBENTUKAN TIM EFEKTIF PROPER MANAJEMEN RISIKO SPBE DI
LINGKUNGAN BSSN**

NO	NAMA	UNIT KERJA	TTD / PARAF
1	2	3	4
1	Ferdinand Mahulette, S.E.	Kapusdatik	1 
2	Rakham Dandani	P21	2 
3	Jama Leonardo	P22	3 
4	ADI WOROLO	P24	4 
5	Zeno Pandano	P24	5 
6	Aqung Nursico	P22	6 
7	BASHIR ATIREMAN	P22	7 
8	Rudi Darmasah	P23	8 
9	Theria Rahmat	P24	9 
10	Cut Agung	P21	10 
11			11
12			12
13			13
14			14
15			15
16			16
17			17
18			18
19			19
20			20



BADAN SIBER DAN SANDI NEGARA

Jalan Raya Muchtar No.70, Kel. Duren Mekar, Kec. Bojongsari, Depok 16518

Telepon (021) 77973360, Faksimile (021) 78844104, (021) 77973579

Website : <https://bssn.go.id>, E-mail : humas@bssn.go.id

SURAT PERINTAH NOMOR : 23/P2/KP.07.01/09/2022

Menimbang : bahwa dalam rangka mendukung pelaksanaan kegiatan Pelatihan Kepemimpinan Nasional (PKN) Tingkat II angkatan XVIII tahun 2022, dipandang perlu mengeluarkan surat perintah bagi Pegawai Badan Siber dan Sandi Negara;

Dasar : 1. Surat Perintah Kapolri Nomor : Sprin/1718/VII/DIK.2.5/2022 tanggal 15 Juli 2022 perihal Perintah mengikuti Pelatihan Kepemimpinan Nasional Tingkat II Angkatan XVIII tahun 2022 di Pusdikmin Lemdiklat Polri;

2. Surat Kapolri Nomor : B/5806/VII/DIK.2.5/2022/SSDM tanggal 15 Juli 2022 perihal Penghadapan Peserta Pelatihan Kepemimpinan Nasional Tingkat II Angkatan XVIII tahun 2022;

3. Program Kerja Kepala Pusat Data dan Teknologi Komunikasi Informasi Tahun Anggaran 2022.

Memberi Perintah

Kepada : Pegawai Negeri Sipil Badan Siber dan Sandi Negara yang nama namanya tersebut dalam lajur dua lampiran Surat Perintah ini.

Untuk : 1. Di samping melaksanakan tugas dan jabatan sehari-hari, ditunjuk sebagai tim efektif untuk mendukung pembuatan Proyek Perubahan PKN Tingkat II angkatan XVIII tahun 2022 a.n. AKBP Rakhmat Damdami S.A.P, M.Si., NRP 74050727 selaku Kepala Bagian Umum, Pusat Data dan TIK BSSN terkait pelaksanaan proyek perubahan dengan judul "Optimalisasi Pusdatik Dalam Melakukan Manajemen Risiko Sistem Pemerintah Berbasis Elektronik di Lingkungan Badan Siber dan Sandi Negara;

2. Melaksanakan perintah ini dengan sebaik-baiknya dan penuh tanggung jawab;

3. Membuat laporan setelah melaksanakan kegiatan dimaksud.

Depok, 14 September 2022

Kepala Pusat Data dan Teknologi Informasi Komunikasi



Tembusan :

1. Kepala Badan Siber dan Sandi Negara;
2. Wakil Kepala BSSN;
3. Plt. Sekretaris Utama;
4. Inspektur;
5. Kepala Biro Perencanaan dan Keuangan;
6. Plt. Kepala Biro Organisasi dan Sumber Daya Manusia.

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE), Badan Siber dan Sandi Negara

DAFTAR NAMA TIM EFEKTIF DALAM MENDUKUNG PEMBUATAN PROYEK PERUBAHAN
PKN TINGKAT II ANGKATAN XVIII TAHUN 2022

NO	NAMA	NIP/NRP	PANGKAT/GOL. RUANG	JABATAN	JABATAN DALAM TIM PROYEK PERUBAHAN
1	2	3	4	5	6
1	Rakhmat Damdami, M.Si.	74050727	Ajun Komisaris Besar Polisi	Kepala Bagian Umum, Pusat Data dan TIK	Project Leader
2	Adi Nugroho, S.ST., S.Kom	19841229 200312 1 007	Pembina (IV/a)	Koordinator Fungsi Manajemen Risiko Dan Kelangsungan TIK	Wakil Project Leader
3	James Leonardo, S.ST	19840114 200312 1 005	Penata Tk. I (III/d)	Koordinator Fungsi Pengembangan Sistem Dan Pengolahan Data	Tim Teknis
5	Noor Hafidz, S.ST.	19840709 200501 1 001	Penata Tk. I (III/d)	Koordinator Fungsi Operasi Dan Layanan TIK	
6	Agung Widodo, S.E.	19820904 200212 1 003	Penata (III/c)	Subkoordinator Operasional dan Pengamanan Persandian	
7	Muhammad Dwison Alizah, S.Tr.TP	19950115 201611 1 001	Penata Muda (III/a)	Subkoordinator Tatakelola dan Kepatuhan Keamanan Sistem Informasi dan TIK	
8	Agung Nursilo, S.S.T., M.T.	19870705 200701 1 002	Penata (III/c)	Subkoordinator Manajemen Sistem Informasi dan Teknologi	
9	Thoriq Rahmat Hidayat, S.Tr.TP	19940913 201712 1 001	Penata Muda (III/a)	Manggala Informatika Ahli Pertama,	
10	Fitri Ariani, S.Sos.	19760924 200212 2 002	Penata Muda (III/a)	Pengelola BMN	Tim Administrasi
11	Anis Nurul Hanifah, A.Md.	19980226 201902 2 001	Pengatur (II/c)	Pranata Komputer Pelaksana.	
12	Muhammad	19780512 199812 1 001	Penata Muda Tk. I (III/b)	Sandiman Pelaksana Lanjutan	
13	Cut Ageng Sulistyowati.S.Kom.	19871126 2021 2405	PPNPN	Asisten Pengelelola Data Perkantoran	
14	Suri Suryani	19910426 2019 2267	PPNPN	Asisten Pengelelola Data Perkantoran	

Kepala Pusat Data dan Teknologi Informasi Komunikasi



LAMPIRAN 5

RAPAT PENYUSUNAN

**DRAFT PERATURAN KEPALA BADAN SIBER DAN SANDI
NEGARA TENTANG MANAJEMEN RISIKO SISTEM
PEMERINTAHAN BERBASIS ELEKTRONIK**

BADAN SIBER DAN SANDI NEGARA

Nomor : 506/P2/KH.01.02/09/2022
Sifat : Biasa
Lampiran : Satu Berkas
Hal : Undangan Penyusunan Peraturan tentang Pedoman
Manajemen Risiko

Depok, 19 September 2022

Yth. Daftar Undangan Terlampir
di –

Tempat

1. Dasar :

- a. Peraturan Badan Siber dan Sandi negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara;
- b. Surat Perintah Kapolri Nomor Sprin/1718/VII/DIK.2.5/2022 tanggal 15 Juli 2022 perihal Perintah mengikuti Pelatihan Kepemimpinan Nasional Tingkat II Angkatan XVIII tahun 2022 di Pusdikmin Lemdiklat Polri;
- c. Surat Kapolri Nomor B/5806/VII/DIK.2.5/2022/SSDM tanggal 15 Juli 2022 perihal Penghadapan Peserta Pelatihan Kepemimpinan Nasional Tingkat II Angkatan XVIII tahun 2022;
- d. Surat Perintah Nomor 23/P2/KP.07.01/09/2022 tanggal 14 September 2022 tentang Tim efektif untuk mendukung pembuatan Proyek Perubahan PKN Tingkat II angkatan XVIII tahun 2022 a.n. AKBP Rakhmat Damdami S.A.P, M.Si., NRP 74050727 selaku Kepala Bagian Umum, Pusat Data dan TIK BSSN terkait pelaksanaan proyek perubahan dengan judul “Optimalisasi Pusdatik Dalam Melakukan Manajemen Risiko Sistem Pemerintah Berbasis Elektronik di Lingkungan Badan Siber dan Sandi Negara.

2. Merujuk dasar tersebut diatas, bersama ini kami mengundang Bapak/Ibu untuk hadir dalam Penyusunan Peraturan tentang Pedoman Manajemen Risiko yang dilaksanakan pada:

Hari/Tanggal : Rabu, 21 September 2022
Waktu : 09.30 s.d. selesai
Tempat : Ruang Rapat Pusdatik Lt. 6, Gedung D4, Kantor Sawangan

3. Demikian disampaikan, atas perhatiannya dan kerja samanya diucapkan terima kasih.



Tembusan :

1. Kepala Badan Siber dan Sandi Negara;
2. Wakil Kepala Badan Siber dan Sandi Negara;
3. Plt. Sekretaris Utama;
4. Inspektorat.

Lampiran I Surat Undangan
Nomor : 506/P2/KH.01.02/09/2022
Tanggal : 19 September 2022

DAFTAR UNDANGAN

1. Rakhmat Damdami S.A.P, M.Si., selaku Kepala Bagian Umum Pusdatik;
2. James Leonardo, S.ST, selaku Koordinator Fungsi Pengembangan Sistem Dan Pengolahan Data, Pusdatik;
3. Noor Hafidz, S.ST., selaku Koordinator Fungsi Operasi Dan Layanan TIK;
4. Adi Nugroho, S.ST., S.Kom selaku Koordinator Fungsi Manajemen Risiko Dan Kelangsungan TIK;
5. Agung Nursilo, S.S.T., M.T., selaku Subkoordinator Manajemen Sistem Informasi dan Teknologi, Kelompok/Fungsi Pengembangan Sistem dan Pengolahan Data, Pusdatik;
6. Muhammad Dwison Alizah, S.Tr.TP, selaku Subkoordinator Tatakelola dan Kepatuhan Keamanan Sistem Informasi dan TIK, Kelompok/Fungsi Manajemen Risiko dan Kelangsungan TIK;
7. Agung Widodo, S.E., selaku Subkoordinator Operasional dan Pengamanan Persandian, Kelompok/Fungsi Manajemen Risiko dan Kelangsungan TIK;
8. Thoriq Rahmat Hidayat, S.Tr.TP, selaku Manggala Informatika Ahli Pertama, Kelompok/Fungsi Manajemen Risiko dan Kelangsungan TIK;
9. Anis Nurul Hanifah, A.Md., selaku Pranata Komputer Pelaksana, Kelompok/Fungsi Operasi dan Layanan TIK;
10. Muhammad, Sandiman Pelaksana Lanjutan, Kelompok/Fungsi Bagian Umum Pusdatik;
11. Fitri Ariani, S.Sos., Pengelola BMN, Kelompok/Fungsi Bagian Umum Pusdatik;
12. Cut Ageng Sulistyowati.S.Kom., Asisten Pengelelola Data Perkantoran, Kelompok/Fungsi Bagian Umum Pusdatik;
13. Suri Suryani, Asisten Pengelelola Data Perkantoran, Kelompok/Fungsi Bagian Umum Pusdatik.



BADAN SIBER DAN SANDI NEGARA

Nomor : 575/P2/KH.01.02/10/2022
Sifat : Biasa
Lampiran : Satu Berkas
Hal : Undangan Finalisasi Penyusunan Draft Peraturan
Kepada Badan Siber dan Sandi Negara

Depok, 3 Oktober 2022

Yth. Daftar Undangan Terlampir
di –

Tempat

1. Dasar :

- a. Peraturan Badan Siber dan Sandi negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara;
- b. Surat Perintah Kapolri Nomor Sprin/1718/VII/DIK.2.5/2022 tanggal 15 Juli 2022 perihal Perintah mengikuti Pelatihan Kepemimpinan Nasional Tingkat II Angkatan XVIII tahun 2022 di Pusdikmin Lemdiklat Polri;
- c. Surat Kapolri Nomor B/5806/VII/DIK.2.5/2022/SSDM tanggal 15 Juli 2022 perihal Penghadapan Peserta Pelatihan Kepemimpinan Nasional Tingkat II Angkatan XVIII tahun 2022;
- d. Surat Perintah Nomor 23/P2/KP.07.01/09/2022 tanggal 14 September 2022 tentang Tim efektif untuk mendukung pembuatan Proyek Perubahan PKN Tingkat II angkatan XVIII tahun 2022 a.n. AKBP Rakhmat Damdami S.A.P, M.Si., NRP 74050727 selaku Kepala Bagian Umum, Pusat Data dan TIK BSSN terkait pelaksanaan proyek perubahan dengan judul “Optimalisasi Pusdatik Dalam Melakukan Manajemen Risiko Sistem Pemerintah Berbasis Elektronik di Lingkungan Badan Siber dan Sandi Negara.

2. Merujuk dasar tersebut diatas, bersama ini kami mengundang Bapak/Ibu untuk hadir dalam Undangan Melakukan Finalisasi Penyusunan Draft Peraturan Kepada Badan Siber dan Sandi Negara tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik di Lingkungan Badan Siber dan Sandi Negara, yang dilaksanakan pada:

Hari/Tanggal : Kamis, 6 Oktober 2022
Waktu : 09.00 s.d. selesai
Tempat : Ruang Rapat Pusdatik Lt. 6, Gedung D4, Kantor BSSN Sawangan

3. Demikian disampaikan, atas perhatiannya dan kerja samanya diucapkan terima kasih.



Tembusan :

1. Kepala Badan Siber dan Sandi Negara;
2. Wakil Kepala Badan Siber dan Sandi Negara;
3. Plt. Sekretaris Utama;
4. Inspektorat.

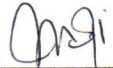
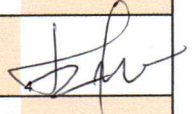
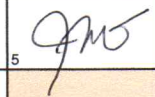
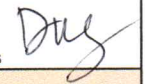
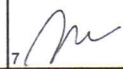
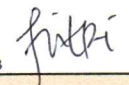
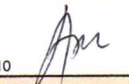
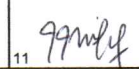
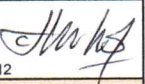
Lampiran I Surat Undangan
Nomor : 575/P2/KH.01.02/10/2022
Tanggal : 3 Oktober 2022

DAFTAR UNDANGAN

1. Rakhmat Damdami S.A.P, M.Si., selaku Kepala Bagian Umum Pusdatik;
2. James Leonardo, S.ST, selaku Koordinator Fungsi Pengembangan Sistem Dan Pengolahan Data, Pusdatik;
3. Noor Hafidz, S.ST., selaku Koordinator Fungsi Operasi Dan Layanan TIK;
4. Adi Nugroho, S.ST., S.Kom selaku Koordinator Fungsi Manajemen Risiko Dan Kelangsungan TIK;
5. Agung Nursilo, S.S.T., M.T., selaku Subkoordinator Manajemen Sistem Informasi dan Teknologi, Kelompok/Fungsi Pengembangan Sistem dan Pengolahan Data, Pusdatik;
6. Muhammad Dwison Alizah, S.Tr.TP, selaku Subkoordinator Tatakelola dan Kepatuhan Keamanan Sistem Informasi dan TIK, Kelompok/Fungsi Manajemen Risiko dan Kelangsungan TIK;
7. Agung Widodo, S.E., selaku Subkoordinator Operasional dan Pengamanan Persandian, Kelompok/Fungsi Manajemen Risiko dan Kelangsungan TIK;
8. Thoriq Rahmat Hidayat, S.Tr.TP, selaku Manggala Informatika Ahli Pertama, Kelompok/Fungsi Manajemen Risiko dan Kelangsungan TIK;
9. Anis Nurul Hanifah, A.Md., selaku Pranata Komputer Pelaksana, Kelompok/Fungsi Operasi dan Layanan TIK;
10. Muhammad, Sandiman Pelaksana Lanjutan, Kelompok/Fungsi Bagian Umum Pusdatik;
11. Fitri Ariani, S.Sos., Pengelola BMN, Kelompok/Fungsi Bagian Umum Pusdatik;
12. Cut Ageng Sulistyowati.S.Kom., Asisten Pengelelola Data Perkantoran, Kelompok/Fungsi Bagian Umum Pusdatik;
13. Suri Suryani, Asisten Pengelelola Data Perkantoran, Kelompok/Fungsi Bagian Umum Pusdatik.



**RAPAT FINALISASI PENYUSUNAN DRAF PERATURAN
KEPALA BADAN SIBER DAN SANDI NEGARA**

NO	NAMA	UNIT KERJA	TTD / PARAF
1	2	3	4
1	Bakimat Damsdani	P21	1 
2	James. leonardo	P22	2 
3	ADI NUKROTOD	P24	3 
4	Noor Hafidz	P23	4 
5	Muha mmad	P21	5 
6	M. DWISON ALIZAH	P24	6 
7	AQUNG NURSILLO	P22	7 
8	FITRI ARIANI	P21	8 
9	Thario Rahmat	P24	9 
10	ABUNG WIDODO	P24	10 
11	Anis Nurul Hanifah	P23	11 
12	CUT Agang	P21	12 
13	SURI SURRANI	P24	13 
14			14
15			15
16			16
17			17
18			18
19			19
20			20
21			21

LAMPIRAN 6

RAPAT PENYUSUNAN

STANDAR OPERASIONAL PROSEDUR (SOP)

PENILAIAN RISIKO (RISK ASSESMENT)

BADAN SIBER DAN SANDI NEGARA

Nomor : 576/P2/KH.01.02/10/2022
Sifat : Biasa
Lampiran : Satu Berkas
Hal : Undangan Pembahasan Penyusunan *Standar Operasional Prosedur* (SOP) tentang Penilaian Risiko (*Risk Assesment*) SPBE di Lingkunga BSSN

Depok, 10 Oktober 2022

Yth. Daftar Undangan Terlampir
di –

Tempat

1. Dasar :
 - a. Peraturan Badan Siber dan Sandi negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara;
 - b. Surat Perintah Kapolri Nomor Sprin/1718/VII/DIK.2.5/2022 tanggal 15 Juli 2022 perihal Perintah mengikuti Pelatihan Kepemimpinan Nasional Tingkat II Angkatan XVIII tahun 2022 di Pusdikmin Lemdiklat Polri;
 - c. Surat Kapolri Nomor B/5806/VII/DIK.2.5/2022/SSDM tanggal 15 Juli 2022 perihal Penghadapan Peserta Pelatihan Kepemimpinan Nasional Tingkat II Angkatan XVIII tahun 2022;
 - d. Surat Perintah Nomor 23/P2/KP.07.01/09/2022 tanggal 14 September 2022 tentang Tim efektif untuk mendukung pembuatan Proyek Perubahan PKN Tingkat II angkatan XVIII tahun 2022 a.n. AKBP Rakhmat Damdami S.A.P, M.Si., NRP 74050727 selaku Kepala Bagian Umum, Pusat Data dan TIK BSSN terkait pelaksanaan proyek perubahan dengan judul “Optimalisasi Pusdatik Dalam Melakukan Manajemen Risiko Sistem Pemerintah Berbasis Elektronik di Lingkungan Badan Siber dan Sandi Negara.
2. Merujuk dasar tersebut diatas, bersama ini kami mengundang Bapak/Ibu untuk hadir dalam Undangan Pembahasan Penyusunan *Standar Operasional Prosedur* (SOP) tentang Penilaian Risiko (*Risk Assesment*) Sistem Pemerintahan Berbasis Elektronik di Lingkungan Badan Siber dan Sandi Negara yang dilaksanakan pada:
Hari/Tanggal : Rabu, 12 Oktober 2022
Waktu : 09.30 s.d. selesai
Tempat : Ruang Rapat Pusdatik Lt. 6, Gedung D4, Kantor BSSN Sawangan
3. Demikian disampaikan, atas perhatiannya dan kerja samanya diucapkan terima kasih.



Tembusan :

1. Kepala Badan Siber dan Sandi Negara;
2. Wakil Kepala Badan Siber dan Sandi Negara;
3. Plt. Sekretaris Utama;
4. Inspektorat.

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE) Badan Siber dan Sandi Negara

Lampiran I Surat Undangan
Nomor : 576/P2/KH.01.02/10/2022
Tanggal : 10 Oktober 2022

DAFTAR UNDANGAN

1. Rakhmat Damdami S.A.P, M.Si., selaku Kepala Bagian Umum Pusdatik;
2. James Leonardo, S.ST, selaku Koordinator Fungsi Pengembangan Sistem Dan Pengolahan Data, Pusdatik;
3. Noor Hafidz, S.ST., selaku Koordinator Fungsi Operasi Dan Layanan TIK;
4. Adi Nugroho, S.ST., S.Kom selaku Koordinator Fungsi Manajemen Risiko Dan Kelangsungan TIK;
5. Agung Nursilo, S.S.T., M.T., selaku Subkoordinator Manajemen Sistem Informasi dan Teknologi, Kelompok/Fungsi Pengembangan Sistem dan Pengolahan Data, Pusdatik;
6. Muhammad Dwison Alizah, S.Tr.TP, selaku Subkoordinator Tatakelola dan Kepatuhan Keamanan Sistem Informasi dan TIK, Kelompok/Fungsi Manajemen Risiko dan Kelangsungan TIK;
7. Agung Widodo, S.E., selaku Subkoordinator Operasional dan Pengamanan Persandian, Kelompok/Fungsi Manajemen Risiko dan Kelangsungan TIK;
8. Thoriq Rahmat Hidayat, S.Tr.TP, selaku Manggala Informatika Ahli Pertama, Kelompok/Fungsi Manajemen Risiko dan Kelangsungan TIK;
9. Anis Nurul Hanifah, A.Md., selaku Pranata Komputer Pelaksana, Kelompok/Fungsi Operasi dan Layanan TIK;
10. Muhammad, Sandiman Pelaksana Lanjutan, Kelompok/Fungsi Bagian Umum Pusdatik;
11. Fitri Ariani, S.Sos., Pengelola BMN, Kelompok/Fungsi Bagian Umum Pusdatik;
12. Cut Ageng Sulistyowati.S.Kom., Asisten Pengelelola Data Perkantoran, Kelompok/Fungsi Bagian Umum Pusdatik;
13. Suri Suryani, Asisten Pengelelola Data Perkantoran, Kelompok/Fungsi Bagian Umum Pusdatik.

**RAPAT PEMBAHASAN PENYUSUNAN SOP TENTANG PENILAIANN RISIKO
SPBE DI LINGKUNGAN BSSN**

NO	NAMA	UNIT KERJA	TTD / PARAF
1	2	3	4
1	Rahmas Dandami	P21	1
2	ADI NUGROHO	P24	2
3	James Leonardo	P22	3
4	Nur Hayida	P23	4
5	Muhammad	P21	5
6	Agung Nursilo	P22	6
7	Thoria Rahmat	P24	7
8	AGUNG WIDODO	P24	8
9	m. Wilson Alizah	P24	9
10	Anis Nurul Harifah	P23	10
11	SURI SRANI	PM	11
12	CET AGENG	P21	12
13	FURI ARIANI	P21	13
14			14
15			15
16			16
17			17
18			18
19			19
20			20
21			21



LAMPIRAN 7

**RAPAT PENYUSUNAN
PETUNJUK TEKHNIS (JUKNIS)
PENILAIAN RISIKO (RISK ASSESMENT)**

BADAN SIBER DAN SANDI NEGARA

Nomor : 577/P2/KH.01.02/10/2022 Depok, 17 Oktober 2022
Sifat : Biasa
Lampiran : Satu Berkas
Hal : Undangan Pembahasan Penyusunan Petunjuk Teknis tentang Penilaian Risiko (*Risk Assesment*) SPBE di Lingkungan BSSN

Yth. Daftar Undangan Terlampir
di –

Tempat

1. Dasar :

- a. Peraturan Badan Siber dan Sandi negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara;
- b. Surat Perintah Kapolri Nomor Sprin/1718/VII/DIK.2.5/2022 tanggal 15 Juli 2022 perihal Perintah mengikuti Pelatihan Kepemimpinan Nasional Tingkat II Angkatan XVIII tahun 2022 di Pusdikmin Lemdiklat Polri;
- c. Surat Kapolri Nomor B/5806/VII/DIK.2.5/2022/SSDM tanggal 15 Juli 2022 perihal Penghadapan Peserta Pelatihan Kepemimpinan Nasional Tingkat II Angkatan XVIII tahun 2022;
- d. Surat Perintah Nomor 23/P2/KP.07.01/09/2022 tanggal 14 September 2022 tentang Tim efektif untuk mendukung pembuatan Proyek Perubahan PKN Tingkat II angkatan XVIII tahun 2022 a.n. AKBP Rakhmat Damdami S.A.P, M.Si., NRP 74050727 selaku Kepala Bagian Umum, Pusat Data dan TIK BSSN terkait pelaksanaan proyek perubahan dengan judul “Optimalisasi Pusdatik Dalam Melakukan Manajemen Risiko Sistem Pemerintah Berbasis Elektronik di Lingkungan Badan Siber dan Sandi Negara.

2. Merujuk dasar tersebut diatas, bersama ini kami mengundang Bapak/Ibu untuk hadir dalam Undangan Pembahasan Penyusunan Petunjuk Teknis tentang Penilaian Risiko (*Risk Assesment*) Sistem Pemerintahan Berbasis Elektronik di Lingkungan Badan Siber dan Sandi Negara yang dilaksanakan pada:

Hari/Tanggal : Kamis, 20 Oktober 2022
Waktu : 09.00 s.d. selesai
Tempat : Ruang Rapat Pusdatik Lt. 6, Gedung D4, Kantor BSSN Sawangan

3. Demikian disampaikan, atas perhatiannya dan kerja samanya diucapkan terima kasih.



Tembusan :

1. Kepala Badan Siber dan Sandi Negara;
2. Wakil Kepala Badan Siber dan Sandi Negara;
3. Plt. Sekretaris Utama;
4. Inspektorat.

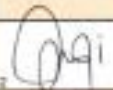
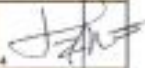
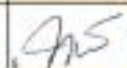
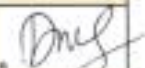
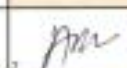
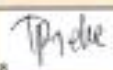
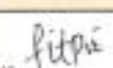
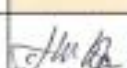
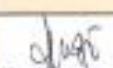
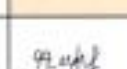
Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE) Badan Siber dan Sandi Negara

Lampiran I Surat Undangan
Nomor : 577/P2/KH.01.02/10/2022
Tanggal : 20 Oktober 2022

DAFTAR UNDANGAN

1. Rakhmat Damdami S.A.P, M.Si., selaku Kepala Bagian Umum Pusdatik;
2. James Leonardo, S.ST, selaku Koordinator Fungsi Pengembangan Sistem Dan Pengolahan Data, Pusdatik;
3. Noor Hafidz, S.ST., selaku Koordinator Fungsi Operasi Dan Layanan TIK;
4. Adi Nugroho, S.ST., S.Kom selaku Koordinator Fungsi Manajemen Risiko Dan Kelangsungan TIK;
5. Agung Nursilo, S.S.T., M.T., selaku Subkoordinator Manajemen Sistem Informasi dan Teknologi, Kelompok/Fungsi Pengembangan Sistem dan Pengolahan Data, Pusdatik;
6. Muhammad Dwison Alizah, S.Tr.TP, selaku Subkoordinator Tatakelola dan Kepatuhan Keamanan Sistem Informasi dan TIK, Kelompok/Fungsi Manajemen Risiko dan Kelangsungan TIK;
7. Agung Widodo, S.E., selaku Subkoordinator Operasional dan Pengamanan Persandian, Kelompok/Fungsi Manajemen Risiko dan Kelangsungan TIK;
8. Thoriq Rahmat Hidayat, S.Tr.TP, selaku Manggala Informatika Ahli Pertama, Kelompok/Fungsi Manajemen Risiko dan Kelangsungan TIK;
9. Anis Nurul Hanifah, A.Md., selaku Pranata Komputer Pelaksana, Kelompok/Fungsi Operasi dan Layanan TIK;
10. Muhammad, Sandiman Pelaksana Lanjutan, Kelompok/Fungsi Bagian Umum Pusdatik;
11. Fitri Ariani, S.Sos., Pengelola BMN, Kelompok/Fungsi Bagian Umum Pusdatik;
12. Cut Ageng Sulistyowati.S.Kom., Asisten Pengelelola Data Perkantoran, Kelompok/Fungsi Bagian Umum Pusdatik;
13. Suri Suryani, Asisten Pengelelola Data Perkantoran, Kelompok/Fungsi Bagian Umum Pusdatik.

**RAPAT PEMBAHASAN PENYUSUNAN PETUNJUK TEKNIS
TENTANG PENILAIAN RISIKO SPBE DI LINGKUNGAN BSSN**

NO	NAMA	UNIT KERJA	TTD / PARAF
1	Rahmat Darmawan	P2,	
2	James Leonardo		
3	Ang Nibetto		
4	Noor Hafidz		
5	Muhammad		
6	M. Anwar Muzot		
7	ADUNG WIDODO		
8	Thoris Pahant		
9	Agung Nussila		
10	Fari Arian		
11	Ced Agung		
12	Supi Subhani		
13	Anis Nurul Hanifah		
14			
15			
16			
17			
18			
19			
20			
21			



LAMPIRAN 8

**PELATIHAN PENINGKATAN KEMAMPUAN DASAR
PEGAWAI DALAM MELAKUKAN PENILAIAN RISIKO**



BADAN SIBER DAN SANDI NEGARA

Jalan Raya Muchtar No.70, Kel. Duren Mekar, Kec. Bojongsari, Depok 16518

Telepon (021) 77973360, Faksimile (021) 78844104, (021) 77973579

Website : <https://bssn.go.id>, E-mail : humas@bssn.go.id

SURAT PERINTAH

NOMOR : 26/P2/DL.01.02/10/2022

Menimbang : bahwa sehubungan pelaksanaan kegiatan Pelatihan Dasar Dalam Rangka Peningkatan Pemahaman dan Kemampuan Penilaian Risiko (*Risk Assesment*) Sistem Pemerintahan Berbasis Elektronik di Lingkungan Badan Siber dan Sandi Negara, perlu dikeluarkan Surat Perintah bagi Pegawai Negeri Sipil Badan Siber dan Sandi Negara;

Dasar : 1. Surat Kepolisian Negara Republik Indonesia Nomor B/5805/VII/DIK.2.5./2022/SSDM tanggal 15 Juli 2022 perihal Pemanggilan Peserta PKN Tingkat II Angkatan XVIII Tahun Anggaran 2022;
2. Program Kerja Kepala Pusat Data dan Teknologi Informasi Komunikasi;
3. Pertimbangan Pimpinan;

Memberi Perintah

Kepada : Pegawai Negeri Sipil Badan Siber dan Sandi Negara yang namanya tersebut dalam lajur dua Lampiran Surat Perintah ini.

Untuk : 1. Melaksanakan Pelatihan Dasar Dalam Rangka Peningkatan Pemahaman dan Kemampuan Penilaian Risiko (*Risk Assesment*) Sistem Pemerintahan Berbasis Elektronik di Lingkungan Badan Siber dan Sandi Negara pada tanggal 27 Oktober 2022 di Kantor BSSN, Sawangan;
2. Melaksanakan perintah ini dengan sebaik-baiknya dan penuh tanggung jawab;
3. Membuat laporan setelah melaksanakan kegiatan dimaksud.

Depok, 24 Oktober 2022

a.n. Kepala Badan Siber dan Sandi Negara

Kepala Pusat Data dan Teknologi Informasi Komunikasi



Tembusan :

1. Kepala Badan Siber dan Sandi Negara;
2. Wakil Kepala BSSN;
3. Deputi Bidang Operasi Keamanan Siber dan Sandi;
4. Inspektur;
5. Kepala Biro Organisasi dan Sumber Daya Manusia.

BADAN SIBER DAN SANDI NEGARA

LAMPIRAN SURAT PERINTAH
 NOMOR : 26/P2/DL.01.02/10/2022
 TANGGAL : 24 Oktober 2022

DAFTAR NAMA PERSONIL PELAKSANA KEGIATAN
 PELATIHAN DASAR DALAM RANGKA PENINGKATAN PEMAHAMAN DAN KEMAMPUAN PENILAIAN RISIKO (RISK ASSESMENT)
 SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN BSSN

NO.	NAMA	NIP.	PANGKAT/GOL. RUANG	JABATAN
1	2	3	4	5
1.	Reno Ramdano, S.S.T.TP	19910410 201012 1 001	Penata (III/c)	Analisis Sistem Informasi dan Jaringan, Kelompok/Fungsi Manajemen Risiko dan Kelangsungan TIK pada Pusat Data dan Teknologi Informasi Komunikasi
2.	Muhammad	19780512 199812 1 001	Penata Muda Tk. I (III/b)	Sandiman Pelaksana Lanjutan, Kelompok/Fungsi Layanan Tata Usaha Bagian Umum pada Pusat Data dan Teknologi Informasi Komunikasi
3.	Alfonso Brolin Sihite, S.Tr.TP	19940717 201611 1 001	Penata Muda Tk. I (III/b)	Analisis Sistem Informasi dan Jaringan, Kelompok/Fungsi Manajemen Risiko dan Kelangsungan TIK pada Pusat Data dan Teknologi Informasi Komunikasi
4.	Ahmad Faridi, S.Tr.TP	19930207 201412 1 002	Penata Muda Tk. I (III/b)	Sandiman Pertama, Kelompok/Fungsi Manajemen Risiko dan Kelangsungan TIK pada Pusat Data dan Teknologi Informasi Komunikasi
5.	Muhammad Dwison Alizah, S.Tr.TP	19950115 201611 1 001	Penata Muda (III/a)	Pranata Komputer Pertama, Kelompok/Fungsi Manajemen Risiko dan Kelangsungan TIK pada Pusat Data dan Teknologi Informasi Komunikasi
6.	Gagas Paras Mulati, S.Tr.Kom	19970321 201912 1 001	Penata Muda (III/a)	Analisis Sistem Informasi dan Jaringan, Kelompok/Fungsi Manajemen Risiko dan Kelangsungan TIK pada Pusat Data dan Teknologi Informasi Komunikasi
7.	Rico Budiyanto, A.Md.	19860129 201902 1 001	Pengatur (II/c)	Pranata Komputer Pelaksana, Kelompok/Fungsi Operasi dan Layanan TIK pada Pusat Data dan Teknologi Informasi Komunikasi

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE) Badan Siber dan Sandi Negara

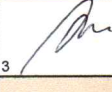
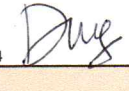
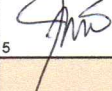
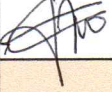
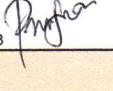
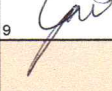
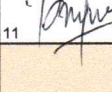
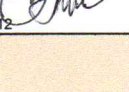
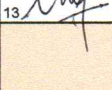
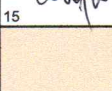
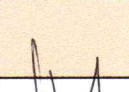
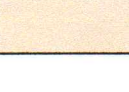
NO.	NAMA	NIP.	PANGKAT/GOL. RUANG	JABATAN
1	2	3	4	5
8.	Gilang Topani, A.Md.	19890613 201902 1 005	Pengatur (II/c)	Pranata Komputer Pelaksana, Kelompok/Fungsi Manajemen Risiko dan Kelangsungan TIK pada Pusat Data dan Teknologi Informasi Komunikasi
9.	Muhammad Luthfi, A.Md.Ml.	19961026 201902 1 002	Pengatur (II/c)	Pranata Komputer Pelaksana, Kelompok/Fungsi Manajemen Risiko dan Kelangsungan TIK pada Pusat Data dan Teknologi Informasi Komunikasi
10.	Habibi Nararyya Kirana, A.Md.	19940512 201902 1 006	Pengatur (II/c)	Pranata Komputer Pelaksana, Kelompok/Fungsi Operasi dan Layanan TIK pada Pusat Data dan Teknologi Informasi
11.	Muhamad Khairil Muttaqin, A.Md.	19861004 201902 1 002	Pengatur (II/c)	Pranata Komputer Pelaksana, Kelompok/Fungsi Manajemen Risiko dan Kelangsungan TIK pada Pusat Data dan Teknologi Informasi Komunikasi
12.	Eko Sandi Puspita, S.Kom.	19890610 202203 1 002	CPNS (III/a)	Analisis Sistem Informasi dan Jaringan (Calon Pranata Komputer Ahli Pertama), Kelompok/Fungsi Manajemen Risiko dan Kelangsungan TIK pada Pusat Data dan Teknologi Informasi Komunikasi
13.	Lingga Maulana Kurniawan, S.Kom.	19900420 202203 1 002	CPNS (III/a)	Analisis Deteksi Kerentanan Siber, Kelompok/Fungsi Manajemen Risiko dan Kelangsungan TIK pada Pusat Data dan Teknologi Informasi Komunikasi
14.	Bayu Ade Candra, S.Kom.	19901018 202203 1 001	CPNS (III/a)	Analisis Identifikasi Kerentanan Siber, Kelompok/Fungsi Manajemen Risiko dan Kelangsungan TIK pada Pusat Data dan Teknologi Informasi Komunikasi
15.	Tri Ragil Mujiyanto, A.Md.	19910502 202203 1 001	CPNS (III/a)	PengelolaKeamanan Sistem Informasi, Kelompok/Fungsi Manajemen Risiko dan Kelangsungan TIK pada Pusat Data dan Teknologi Informasi Komunikasi
16.	Dukhaan Awakhir, A.Md.Kom.	19980811 202203 1 001	CPNS (III/a)	Pengolah Data Keamanan Siber dan Sandi, Kelompok/Fungsi Manajemen Risiko dan Kelangsungan TIK pada Pusat Data dan Teknologi Informasi Komunikasi

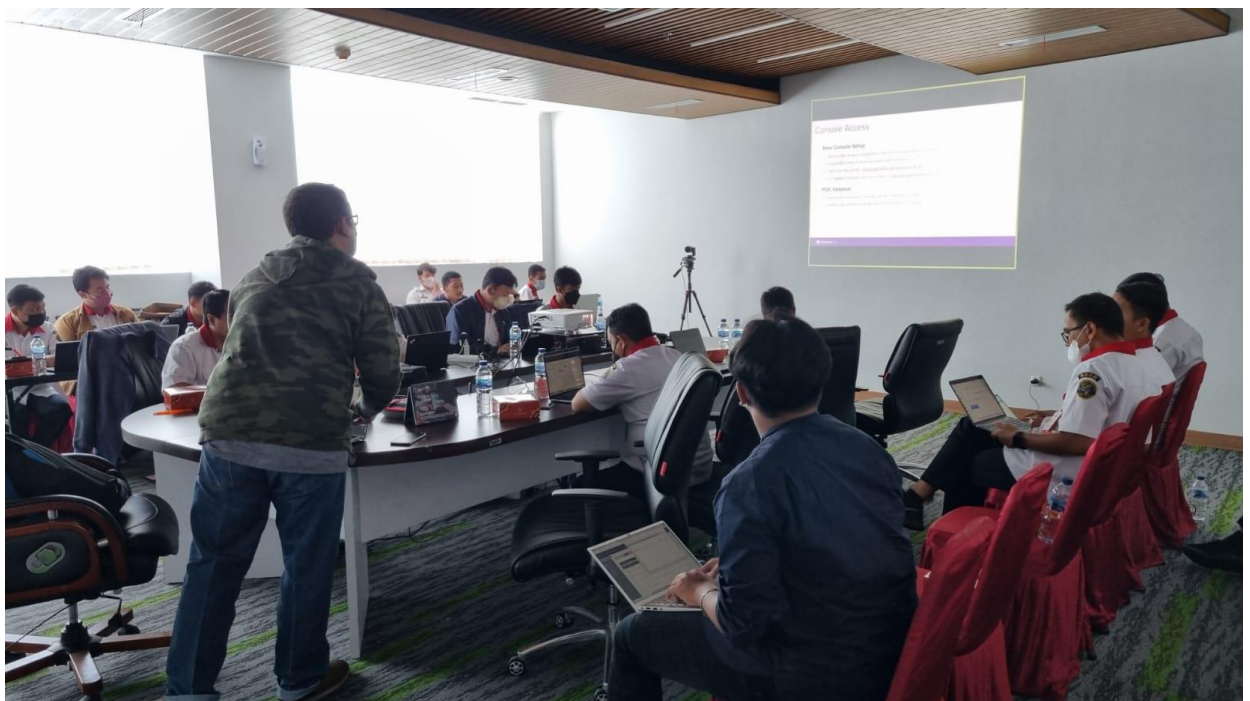
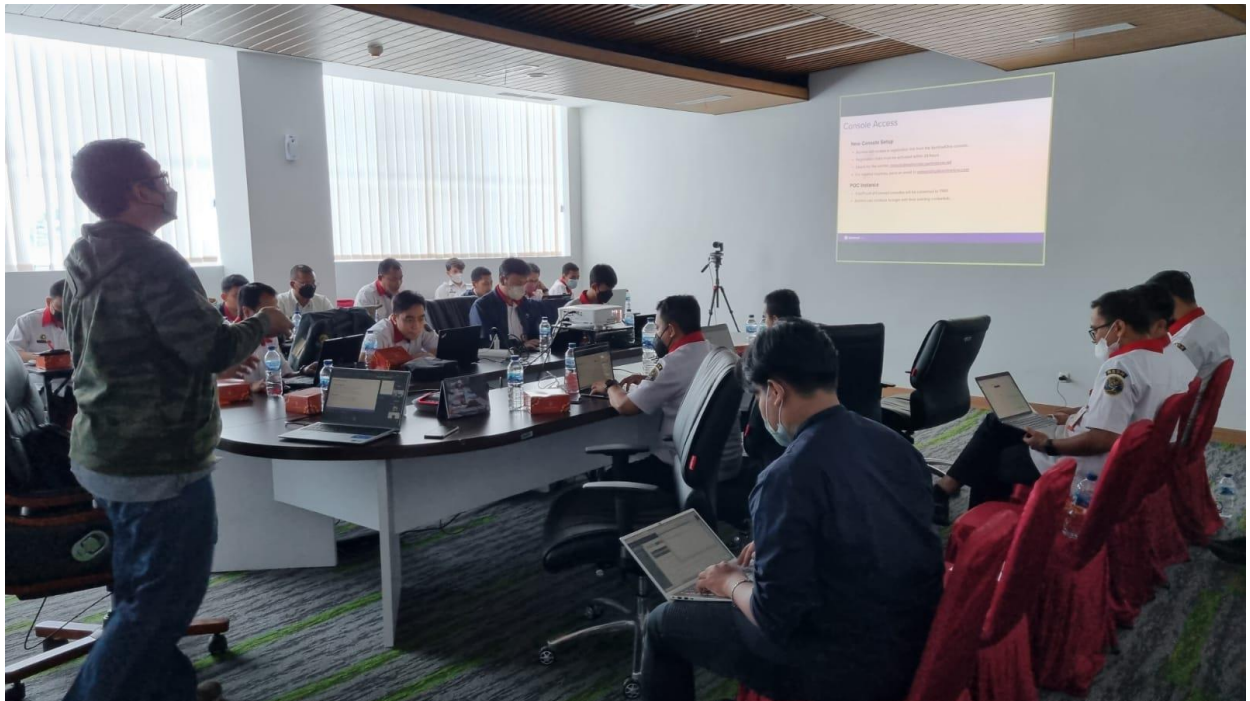
Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE) Badan Siber dan Sandi Negara

NO.	NAMA	NIP.	PANGKAT/GOL. RUANG	JABATAN
1	2	3	4	5
17.	Imam Muhammad Nurul Huda, A.Md	19890707 202203 1 001	CPNS (III/a)	Pengolah Data Keamanan Siber dan Sandi, Kelompok/Fungsi Manajemen Risiko dan Kelangsungan TIK pada Pusat Data dan Teknologi Informasi Komunikasi
18.	Irfan Jafar, A.Md.	19961029 202203 1 001	CPNS (III/a)	Pengolah Data Keamanan Siber dan Sandi, Kelompok/Fungsi Manajemen Risiko dan Kelangsungan TIK pada Pusat Data dan Teknologi Informasi Komunikasi
19.	Agung Wibisono, A.Md.	19950906 202203 1 002	CPNS (III/a)	Pengolah Data Keamanan Siber dan Sandi, Kelompok/Fungsi Manajemen Risiko dan Kelangsungan TIK pada Pusat Data dan Teknologi Informasi Komunikasi
20.	Boma Indra Gunawan, S.T.	19961011 202203 1 001	CPNS (III/a)	Analisis Pertahanan Siber, Kelompok/Fungsi Pengembangan Sistem dan Pengolahan Data pada Pusat Data dan Teknologi Informasi Komunikasi

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE) Badan Siber dan Sandi Negara

**PELATIHAN DASAR DALAM RANGKA PENINGKATAN PEMAHAMAN DAN KEMAMPUAN
PENILAIAN RISIKO SPBE DI LINGKUNGAN BSSN**

NO	NAMA	UNIT KERJA	TTD / PARAF
1	2	3	4
1	Alfonso Brodin Sibbe	P24	1 
2	A. FARIDI	P24	2 
3	Pico Baidianto	P23	3 
4	m. anison. Aritah	P24	4 
5	Muhamma d	P24	5 
6	Pano Ramdano	P24	6 
7	GILANG TOPANSI	P24	7 
8	BAYU ADE CANDRA	P24	8 
9	Gagas Mulati	P24	9 
10	MUKHAMMAD AWAKHIR	P24	10 
11	Tri Ragil Mulyanto	P24	11 
12	Lingga Maulani Kurniawan	P24	12 
13	MUHAMMAD LUTHFI	P24	13 
14	Habibi	P23	14 
15	Muhamad Khairil M	P24	15 
16	Eko Sandi Rospita	P24	16 
17	Irfan Jafar	P24	17 
18	Boma Indra Gunawan	P22	18 
19	Agung Wibisono	P24	19 
20	IMAM MUHAMMAD KIRUL HUDA	P24	20 
21			21





BADAN SIBER DAN SANDI NEGARA

Jalan Raya Muchtar No.70, Kel. Duren Mekar, Kec. Bojongsari, Depok 16518

Telepon (021) 77973360, Faksimile (021) 78844104, (021) 77973579

Website : <https://bssn.go.id>, E-mail : humas@bssn.go.id

LAPORAN HASIL PELATIHAN DASAR

PEMAHAMAN DAN KEMAMPUAN PENILAIAN RISIKO

“Menurunkan Risiko Insiden Keamanan Informasi

Yang Disebabkan Oleh E-Mail Phishing”

A. DASAR

1. Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara;
2. Program Kerja Bagian Pusat Data dan Teknologi Informasi Komunikasi Badan Siber dan Sandi Negara Tahun Anggaran 2022.
3. Surat Perintah Kapusdatik Nomor : 26/P2/DL.01.02/10/2022 tanggal 24 Oktober 2022 tentang Pelatihan Dasar Dalam Rangka Peningkatan Pemahaman dan Kemampuan Penilaian Risiko (*Risk Assesment*) Sistem Pemerintahan Berbasis Elektronik di Lingkungan Badan Siber dan Sandi Negara

B. PELAKSANAAN

Kegiatan Pelatihan dilaksanakan pada :

Hari, tanggal : Kamis, 27 Oktober 2022

Waktu : 08.00 sd 16.00 WIB

Tempat : Ruang Rapat Gedung Deputi IV BSSN

C. PESERTA

11. Reno Ramdano, S.S.T.TP	11. Muhamad Khairil Muttaqin, A.Md.
12. Muhammad	12. Eko Sandi Puspita, S.Kom.
13. Alfonso Brolin Sihite, S.Tr.TP	13. Lingga Maulana Kurniawan, S.Kom.
14. Ahmad Faridi, S.Tr.TP	14. Bayu Ade Candra, S.Kom.
15. Muhammad Dwison Alizah, S.Tr.TP	15. Tri Ragil Mujiyanto, A.Md.
16. Gagas Paras Mulati, S.Tr.Kom	16. Dukhaan Awakhir, A.Md.Kom.
17. Rico Budiyanto, A.Md.	17. Imam Muhammad Nurul Huda, A.Md.
18. Gilang Topani, A.Md.	18. Irfan Jafar, A.Md.
19. Muhammad Luthfi, A.Md.MI.	19. Agung Wibisono, A.Md.
20. Habibi Nararyya Kirana, A.Md.	20. Boma Indra Gunawan, S.T.

D. ISI BAHASAN

1. Kegiatan yang diselenggarakan merupakan serangkaian kegiatan sebagai bagian dari Manajemen Risiko Sistem Elektronik. Adapun sampel dari kegiatan ini berasal dari masing-masing unit kerja dengan persentase 10% dari total sampel seperti pada tabel berikut:

Total Sample : 145 Orang

- Inspektur Badan Siber dan Sandi Negara : 4
- Sekretaris Utama Badan Siber dan Sandi Negara : 38
- Deputi Bidang Strategi dan Kebijakan Keamanan Siber dan Sandi : 11
- Deputi Bidang Operasi Keamanan Siber dan Sandi : 38
- Deputi Bidang Keamanan Siber dan Sandi Pemerintahan dan Pembangunan Manusia : 9
- Deputi Bidang Keamanan Siber dan Sandi Perekonomian : 9

- Pusat Pengkajian dan Pengembangan Teknologi Keamanan Siber dan Sandi:4
 - Pusat Data dan Teknologi Informasi Komunikasi : 8
 - Pusat Pengembangan Sumber Daya Manusia : 9
 - Politeknik Siber dan Sandi Negara : 15
2. Selama pelaksanaan kegiatan terdapat beberapa hal yang perlu menjadi perhatian, yaitu:
- a. Terdapat dua periode pelaksanaan Simulasi Phishing E-mail
- 1) Periode Pre Assessment
 - Simulasi 1: Pengumuman Pegawai Teladan
 - Simulasi 2: Pinjaman Bank Mandiri
 - 2) Periode Post Assessment
 - Simulasi 3: Tawaran Beasiswa Kedutaan Inggris
 - Simulasi 4: Sextortion
- b. Pada dua periode waktu yang ditetapkan untuk proses simulasi, didapatkan persentase keberhasilan phishing sebagai berikut:
- 1) Periode Pre Assessment
 - Simulasi 1: 45% (70 Pegawai)
 - Simulasi 2: 8% (19 Pegawai)
 - 2) Periode Post Assessment
 - Simulasi 3: 15% (35 Pegawai)
 - Simulasi 4: 2% (18 Pegawai)

- c. Persentase tingkat kesuksesan simulasi phishing sebagai berikut:
 - Pegawai BSSN atau Target phishing lebih tertarik dengan email yang terkait pemberian hadiah atau penawaran yang mengatasnamakan internal BSSN. Sehingga perlu menjadi catatan tersendiri dalam memformulasikan pengumuman internal agar tidak digunakan sebagai phishing campaign oleh pihak yang tidak bertanggung jawab.
 - Waktu pelaksanaan simulasi phishing yang tepat pada awal jam kerja yaitu sekitar pukul 08:00 WIB – 10:00 WIB
 - d. Simulator phishing telah dikonfigurasi untuk tidak menyimpan informasi password sebagai upaya pengamanan terhadap kerahasiaan data target.
3. Pada kegiatan juga didapatkan beberapa hasil analisa sebagai berikut::
- a. Penurunan persentase keberhasilan pada simulasi phishing menunjukkan bahwa target mengalami peningkatan kesadaran atas indikasi-indikasi phishing yang dilakukan. Namun ada kemungkinan target tidak tertarik dengan tema phishing yang dilakukan atau informasi mengenai kegiatan simulasi ini telah diketahui oleh Pegawai BSSN.
 - b. Pada saat kegiatan simulasi phishing berlangsung, Pegawai yang menerima e-mail phishing sangat minim sekali melakukan pelaporan indikasi phishing ini melalui kanal aduan Pusdatik ataupun melalui e-mail BSSN CSIRT. Sehingga ini perlu menjadi perbaikan dalam hal sosialisasi mengenai mekanisme pelaporan insiden keamanan informasi yang terjadi agar Pegawai bisa memanfaatkan kanal aduan yang ada.

- c. Berdasarkan hasil simulasi phishing yang dilakukan, pada skenario simulasi ke empat masih didapatkan pegawai yang tidak menyadari adanya indikasi serangan phishing. Oleh sebab itu, perlu dilaksanakan kegiatan lanjutan untuk lebih mengoptimalkan upaya peningkatan kesadaran pegawai dengan cara mengadakan kegiatan seperti seminar atau sosialisasi terkait indikasi phishing atau serangan siber lainnya.

E. PENUTUP

Demikian Laporan Hasil Pelatihan ini dibuat sebagai bahan masukan dan pertimbangan bagi pimpinan untuk menentukan kebijakn selanjutnya

Depok, Oktober 2022



Rakhmat Damdami, SAP, MSi

LAMPIRAN 9

SOSIALISASI

**DRAFT PERATURAN KEPALA BADAN SIBER DAN SANDI
NEGARA TENTANG MANAJEMEN RISIKO SISTEM
PEMERINTAHAN BERBASIS ELEKTRONIK**

BADAN SIBER DAN SANDI NEGARA

Nomor : 578/P2/KH.01.02/10/2022 Depok, 28 Oktober 2022
Sifat : Biasa
Lampiran : Satu Berkas
Hal : Undangan Sosialisasi terhadap Draft Peraturan Kepada Badan Siber dan Sandi Negara tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik di lingkungan Badan Siber dan Sandi Negara

Yth. Daftar Undangan Terlampir

di –

Tempat

1. Dasar :

- a. Peraturan Badan Siber dan Sandi negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara;
- b. Surat Perintah Kapolri Nomor Sprin/1718/VII/DIK.2.5/2022 tanggal 15 Juli 2022 perihal Perintah mengikuti Pelatihan Kepemimpinan Nasional Tingkat II Angkatan XVIII tahun 2022 di Pusdikmin Lemdiklat Polri;
- c. Surat Kapolri Nomor B/5806/VII/DIK.2.5/2022/SSDM tanggal 15 Juli 2022 perihal Penghadapan Peserta Pelatihan Kepemimpinan Nasional Tingkat II Angkatan XVIII tahun 2022;
- d. Surat Perintah Nomor 23/P2/KP.07.01/09/2022 tanggal 14 September 2022 tentang Tim efektif untuk mendukung pembuatan Proyek Perubahan PKN Tingkat II angkatan XVIII tahun 2022 a.n. AKBP Rakhmat Damdami S.A.P, M.Si., NRP 74050727 selaku Kepala Bagian Umum, Pusat Data dan TIK BSSN terkait pelaksanaan proyek perubahan dengan judul “Optimalisasi Pusdatik Dalam Melakukan Manajemen Risiko Sistem Pemerintah Berbasis Elektronik di Lingkungan Badan Siber dan Sandi Negara.

2. Merujuk dasar tersebut diatas, bersama ini kami mengundang Bapak/Ibu untuk hadir dalam Sosialisasi terhadap Draft Peraturan Kepada Badan Siber dan Sandi Negara tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik di lingkungan Badan Siber dan Sandi Negara yang dilaksanakan pada:

Hari/Tanggal : Selasa, 1 November 2022
Waktu : 09.00 s.d. selesai
Tempat : Ruang Rapat Lt. 2, Gedung D4, Kantor BSSN Sawangan

3. Demikian disampaikan, atas perhatiannya dan kerja samanya diucapkan terima kasih.



Tembusan :

1. Kepala Badan Siber dan Sandi Negara;
2. Wakil Kepala Badan Siber dan Sandi Negara;
3. Plt. Sekretaris Utama;
4. Inspektorat.

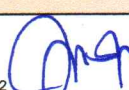
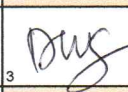
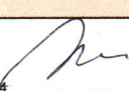
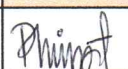
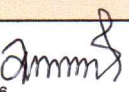
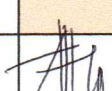
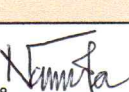
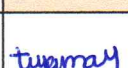
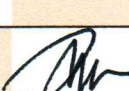
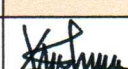
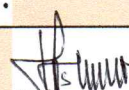
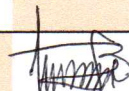
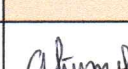
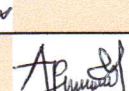
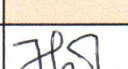
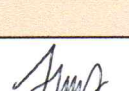
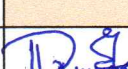
Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE) Badan Siber dan Sandi Negara

Lampiran I Surat Undangan
Nomor : 578/P2/KH.01.02/10/2022
Tanggal : 28 Oktober 2022

DAFTAR SURAT UNDANGAN

1. 3 orang staf Sekretaris Utama;
2. 3 orang staf Deputi Bidang Strategi dan Kebijakan Keamanan Siber dan Sandi;
3. 3 orang staf Deputi Bidang Operasi Keamanan Siber dan Sandi;
4. 3 orang staf Deputi Bidang Keamanan Siber Dan Sandi Pemerintahan dan Pembangunan Manusia;
5. 3 orang staf Deputi Bidang Keamanan Siber dan Sandi Perekonomian.

**SOSIALISASI TERHADAP DRAF PERATURAN KEPALA BSSN TENTANG
PEDOMAN MENAJEMEN RISIKO SPBE DI LINGKUNGAN BSSN**

NO	NAMA	UNIT KERJA	TTD / PARAF
1	2	3	4
1	Rahmat Dandami	P21	
2	James. leonardo	P22	
3	M. Dwison. Alizah	P24	
4	Agung Nursito	P22	
5	Reska Riskiyani	D42	
6	ANTON SUTOPO	dib	
7	ARIADI BAKU	D41	
8	Kanda Baku PRATAMA	S1	
9	Tiya mariana	dii	
10	IRWAN SYAH	D12	
11	asti mesyita	d13	
12	Adi Sulaiman	S2	
13	Darung Jaya	D31	
14	DET Kardono	P32	
15	ADI Humaun	B33	
16	Anji Prasasti	S1	
17	Istuningtyas	D22	
18	Tommi wibaya	D21	
19	Rachmayudi	D22	
20			
21			







LAMPIRAN 10

SERTIFIKAT PELATIHAN

MATA PELAJARAN PILIHAN



REVOLUTION MIND INDONESIA™

Number : 1299/RMI/CPRM/VIII/2022

Certificate Of Recognition Presented To

Rakhat Damdami

Has successfully completed studies satisfactorily demonstrated competence
and henceforth recognized as a

Certified Professional Risk Management (CPRM™)

Sukabumi, August 28th 2022

A handwritten signature in black ink, appearing to read "Aswin".

Aswin Sumarto, S.S., M.M.

Trainer



Muhammad Hadi Nur Yahya Tasman

Director



REVOLUTION MIND INDONESIA™

Transkrip Materi & Jam Pembelajaran

Nama Peserta : Rakhmat Damdami, CPRM™

NO	MATERI	JAM PEMBELAJARAN
1	Konsep Risiko based on ISO 31000:2018	6 JP
2	Manajemen Strategis	
3	Prinsip Manajemen Risiko based on ISO 31000:2018	
4	Kerangka Manajemen Risiko (Part 1)	
5	Kerangka Manajemen Risiko (Part 2)	
6	Proses Manajemen Risiko based on ISO 31000:2018	
7	Tes Kompetensi CPRM	14 JP
	Jumlah JP	20 JP

Keterangan :

Jumlah Jam Pembelajaran Certified Professional Risk Management (CPRM™) adalah Dua Puluh Jam Pembelajaran

Diterbitkan pada 28 Agustus 2022 oleh Revolution Mind Indonesia™.

Muhammad Hadi Nur Yahya Tasman
Direktur





REVOLUTION MIND INDONESIA™

Number : 0071/RMI/CPGRC/IX/2022

Certificate Of Recognition Presented To

Rakhmat Damdami

Has successfully completed studies satisfactorily demonstrated competence
and henceforth recognized as a

**Certified Professional Governance, Risk Management
& Compliance (CPGRC)**

Sukabumi, September 11th 2022

A handwritten signature in black ink, appearing to read "Aswin".

Aswin Sumarto, S.S., M.M.

Trainer



A handwritten signature in black ink, appearing to read "Hadi".

Muhammad Hadi Nur Yahya Tasman

Director



REVOLUTION MIND INDONESIA™

Transkrip Materi & Jam Pembelajaran

Nama Peserta : Rakhmat Damdami, CPGRC

NO	MATERI	JAM PEMBELAJARAN
1	ISO 37000:2020 (Pedoman Tata Kelola)	8 JP
2	ISO 31000:2018 (Pedoman Manajemen Risiko)	
3	ISO 37301:2021 (Compliance Management System)	
4	Definisi GRC	
5	Prinsip Tata Kelola Perusahaan	
6	Lingkup GRC	
7	Prinsip Kinerja Berprinsip	
8	GRC Capability Model – Komponen dan Elemen	
	(Learn, Align, Perform & Review)	
9	Strategi GRC	
10	Tes Kompetensi CPGRC	14 JP
	Jumlah JP	22 JP

Keterangan :

Jumlah Jam Pembelajaran Certified Professional Governance, Risk Management & Compliance (CPGRC) adalah Dua Puluh Dua Jam Pembelajaran

Diterbitkan pada 11 September 2022 oleh Revolution Mind Indonesia™.

Muhammad Hadi Nur Yahya Tasman
Direktur





REVOLUTION MIND INDONESIA™

Nomor: 14950/RMI-SEM.ON/IX/2022

Diberikan Kepada :

Rakhmat Damdami, S.A.P., M.Si

Sebagai : Peserta

Dalam acara Seminar Online Zoom dengan Tema
“Risk Management Based On Iso 31000:2018”
Pembicara : Aswin Sumarto, S.S., M.M., CBIA, CHCM,
QRM, CRA, CRPM, CGRC, CTRMI.

Sukabumi, 14 September 2022

Muhammad Hadi Nur Yahya Tasman
Direktur

CERTIFICATE

OF PARTICIPATION

No:
35/DC/W-DC/IX/2022

THIS CERTIFICATE AWARDED TO:

Rakhmat Damdami, SAP, MSi

As Participant On
National Webinar “Webinar Safety Management System”
Through Zoom Meeting which was held on
14 September 2022

Bandung

14 September 2022



Joe Lian Min

CERTIFICATE

OF PARTICIPATION

No:
10/DC/W-DC/IX/2022

THIS CERTIFICATE AWARDED TO:

Rakhmat Damdami, SAP, MSi

As Participant On
National Webinar “Webinar Enterprise Architecture”
Through Zoom Meeting which was held on
22 September 2022

Bandung

22 September 2022



Joe Lian Min

CERTIFICATE

OF PARTICIPATION

No:
11/DC/W-DC/X/2022

THIS CERTIFICATE IS AWARDED TO:

Rakhmat Damdami, SAP, MSi

As Participant On

National Webinar “Webinar Cyber Threat Management”

Through Zoom Meeting which was held on
6 Oktober 2022

Bandung

6 Oktober 2022


MOTEKAR
EDUKASI INDONESIA

Joe Lian Min



Certificate

IS HERE WITH GIVEN TO :

AKBP RAKHMAT DAMDAMI, S.A.P., M.S.I.

PAMEN BARESKRIM / BSSN

FOR HIS/HER EXCELLENT ATTENDANCE IN THE TRAINING COURSE OF

MEMBANGUN KERJA SAMA YANG STRATEGIS DENGAN INSTANSI LAIN UNTUK MENUJU POLRI YANG PRESISI

WHICH WAS HELD ON :

August 28th 2022

Given in Yogyakarta, August 28th 2022

DIRECTOR

JOGJA SMART
IN DOTAMA
TRAINING & CONSULTANT

Lisa Fitri, S.S

INSTRUCTOR

Dr. Nurus Sa'adah, S.Psi., M.Si., Psikolog.



SERTIFIKAT



WORKSHOP

“KONSEPTUALISASI DAN PENYUSUNAN INDEKS PROFESIONALITAS ANGGOTA POLRI”

Diberikan Kepada:

RAKHMAAT DAMDAMI, S.A.P., M.Si.

Bareskrim Polri

Atas Partisipasi Sebagai Peserta *Workshop*
Pada Tanggal 31 Agustus s.d. 2 September 2022 di Jakarta

Jakarta, 2 September 2022
ASISTEN KAPOLRI BIDANG SUMBER DAYA MANUSIA

Drs. WAHYU WIDADA, M.Phil.
INSPEKTUR JENDERAL POLISI



LAMPIRAN 11

**DUKUNGAN PIMPINAN TERHADAP
PROYEK PERUBAHAN YANG DILAKUKAN**

PERNYATAAN DUKUNGAN

Yang bertanda tangan di bawah ini :

Nama : Komisaris Jenderal Drs. Luki Hermawan, MSi

Jabatan : Wakil Kepala BSSN

Menyatakan **DUKUNGAN** atas proyek perubahan yang berjudul

“Optimalisasi Pusdatik Dalam Melakukan Manajemen Risiko Sistem Pemerintah
Berbasis Elektronik di Lingkungan Badan Siber dan Sandi Negara”

Yang akan dilakukan oleh : Rakhmat Damdami, SAP, MSi

Peserta PKN II Lembaga Administrasi Negara Angkatan XVIII Tahun 2022 di
Pusdikmin Polri Bandung.

Alasan Dukungan :

Seperti kita ketahui bahwa akhir akhir ini banyak terjadi kasus kasus serangan siber ataupun kebocoran data. Hal ini sangat berbahaya bagi keamanan negara maupun data pribadi setiap warga negara yang dapat disalahgunakan oleh oknum oknum yang tidak bertanggung jawab, baik untuk kepentingan pribadi dengan tujuan mendapatkan sejumlah imbalan materi ataupun dengan tujuan untuk mengacaukan stabilitas negara yang dapat dilakukan oleh state actor baik dari dalam maupun luar negeri.

Oleh karena itu perlindungan terhadap sistem elektronik suatu institusi termasuk BSSN adalah sangat penting, dengan cara melakukan manajemen risiko sistem pemerintahan berbasis elektronik. Dengan demikian dapat diketahui dengan segera kerentanan atau kerawanan pada sistem elektronik tersebut, dan dapat segera dilakukan perbaikan ataupun penguatan.

Bentuk Dukungan :

Memberikan akses seluas luasnya semua sumber daya yang ada ke setiap unit kerja dalam rangka pengumpulan data



Drs. Luki Hermawan, MSi
Komisaris Jenderal Polisi

PERNYATAAN DUKUNGAN

Yang bertanda tangan di bawah ini :

Nama : Brigadir Jenderal TNI Ferdinand Mahulette, SE

Jabatan : Wakil Kepala BSSN

Menyatakan **DUKUNGAN** atas proyek perubahan yang berjudul

“Optimalisasi Pusdatik Dalam Melakukan Manajemen Risiko Sistem Pemerintah
Berbasis Elektronik di Lingkungan Badan Siber dan Sandi Negara”

Yang akan dilakukan oleh : Rakhmat Damdami, SAP, MSi

Peserta PKN II Lembaga Administrasi Negara Angkatan XVIII Tahun 2022 di
Pusdikmin Polri Bandung.

Alasan Dukungan :

Karena Sejak terbentuknya BSSN tahun 2017, efektif beroperasi pertengahan 2018 dan pernah mengalami reorganisasi tahun 2021, masih banyak kekurangan alat kelengkapan organisasi termasuk di dalamnya adalah peraturan peraturan. Ini sangat mempengaruhi tugas pokok di BSSN, khususnya kami di Pusdatik, tidak dapat melaksanakan salah satu fungsi yang ada di kami yaitu manajemen risiko sebagai suatu upaya untuk mencegah terjadinya upaya serangan siber ataupun kebocoran data.

Tidak adanya peraturan ini juga menyebabkan kami kesulitan untuk mencapai nilai indeks nilai SPBE BSSN yang telah menjadi target yang telah ditentukan. Oleh karena itu dengan langkah optimalisasi Pusdatik melalui pembuatan peraturan ini diharapkan juga dapat mengangkat indeks SPBE BSSN yang setiap tahun dilakukan evaluasi oleh Kemenpan RB.

Dalam proyek perubahan ini kami selaku mentor menyarankan tidak hanya terbatas pada pembuatan Peraturan Kepala saja namun juga SOP dan petunjuk Teknis untuk pelaksanaannya, sehingga Ketika Peraturan tersebut disahkan, pegawai yang masuk dalam Tim Penilai dapat segera melaksanakan tugasnya karena sudah dilengkapi dengan peraturan, SOP dan Petunjuk Teknis. Tentu sebelumnya mereka juga dibekali terlebih dahulu dengan pelatihan untuk peningkatan kemampuan dan juga dukungan sarana prasana terkait.

Terakhir, saya berharap proyek perubahan ini dapat segera diterapkan dan saya dukung untuk keberlanjutannya ke depan dalam mensukseskan visi dan misi BSSN

Bentuk Dukungan :

Memberikan kesempatan untuk menggunakan seluruh sumber daya yang ada di Pusdatik termasuk pegawai, untuk turut serta membantu mensukseskan pelaksanaan implementasi proyek perubahan ini.



The image shows an official circular stamp of the Badan Siber dan Sandi Negara (BSSN) of the Republic of Indonesia. The stamp features the national emblem (Garuda Pancasila) in the center, with the text "BADAN SIBER DAN SANDI NEGARA" around the top and "REPUBLIK INDONESIA" around the bottom. To the right of the stamp is a handwritten signature in blue ink, which appears to read "Mahulette".

Ferdinand Mahulette, SE
Brigadir Jenderal TNI

SURAT PERNYATAAN KOMITMEN
PKN TK. II ANGKATAN VII TAHUN 2020

Berkenaan dengan Pelaksanaan Pelatihan kepemimpinan Nasional Tingkat II Angkatan XVIII Tahun 2022 yang diselenggarakan oleh Lembaga Administrasi Negara Republik Indonesia di Pusdikmin Polri, atas nama:

Nama Peserta : RAKHMAT DAMDAMI, S.A.P., M.Si
Nomor Siswa : 20220707012326
Instansi : Badan Siber dan Sandi Negara

Dengan ini Kami memberikan komitmen terhadap implementasi Proyek Perubahan baik pada tahap Jangka menengah dan Jangka Panjang pada proyek perubahan yang berjudul **“Optimalisasi Pusdatik Dalam Melakukan Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik Di Lingkungan Badan Siber dan Sandi Negara”**.

Demikian pernyataan ini kami buat dengan sebenarnya. Semoga Proyek Perubahan yang dibuat dapat diterapkan untuk kepentingan Badan Siber dan Sandi Negara.

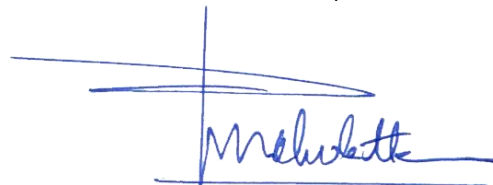
Peserta Diklat,



RAKHMAT DAMDAMI, SAP, MSI

Disetujui oleh:

Mentor,



FERDINAND MAHULETTE, S.E.
BRIGJEN TNI NRP 1900026591265



LAMPIRAN 12

LEMBAR BIMBINGAN

COACH DAN MENTOR

KARTU KENDALI PROSES COACHING

PELATIHAN KEPEMIMPINAN TINGKAT II ANGKATAN XVIII TAHUN 2022

Nama Peserta : Rakhmat Damdami, S.A.P., M.Si

Nosis : 20220707012326

Nama Coach : Burdan Ali Junjuran, S.H., M.Si.

No	Tanggal	Isu/Permasalahan	Media Komunikasi	Hasil Coaching	Tanda tangan Coach
1.	24-08-2022	Pemaparan rencana proper	zoom	Agar ditambahkan pelatihan dan usulan peralatan	
2.	30-08-2022	Penyampaian koreksi hasil paparan	WA Chat	Dipelajari	
3.	31-08-2022	Penyamaan pemahaman deskripsi proyek terkait lingkup tugas	WA Chat	Agar judul disesuaikan kembali berdasarkan lingkup tugas	
4.	01-08-2022	Pemaparan draft rencana proper hasil koreksi	Zoom	Sudah bagus, tinggal paparan diperindah lagi tampilannya	
5.	05-08-2022	Arahan persiapan seminar rancangan proper	On class	Perhatikan waktu dan teknis penyampaian mengikuti panduan yang diberikan	

No	Tanggal	Isu/Permasalahan	Media Komunikasi	Hasil Coaching	Tanda tangan Coach
6.	05-10-2022	Petunjuk penulisan outline implementasi proyek perubahan	Zoom	Penempatan foto kegiatan dan surat surat kegiatan implementasi agar ditempatkan pada lembar lampiran Pemberdayaan organisasi pembelajar Manfaat mata pelatihan pilihan	
7.	31-10-2022	Arahan penyusunan akhir Proper	Tatap Muka	Sudah cukup bagus dan lengkap Dalam paparan tambahkan Keberlanjutan jangka menengah dan panjang	
8.	08-10-2022	Pemaparan slide untuk persiapan akhir	zoom	Sudah bagus dapat segera dijilid	

Mengetahui dan disetujui oleh

Coach,

BURDAN ALI JUNJUNAN, S.H., M.Si.
NIP 196012011986031016

KARTU KENDALI PROSES MENTORING

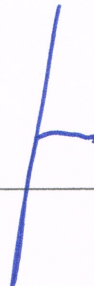
PELATIHAN KEPEMIMPINAN TINGKAT II ANGKATAN XVIII TAHUN 2022

Nama Peserta : Rakhmat Damdami, S.A.P., M.Si

Nosis : 20220707012326

Nama Mentor : Ferdinand Mahulette, S.E.

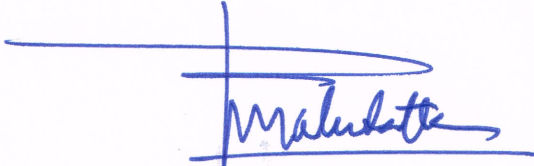
No	Tanggal	Isu/Permasalahan	Media Komunikasi	Hasil Coaching	Tanda tangan Mentor
1.	01-08-2022	Penyampaian rencana pembuatan Rancangan Proper	Tatap Muka	Agar membuat proper yang dapat meningkatkan atau mengoptimalkan fungsi Pusdatik	
2.	03-08-2022	Penyampaian tema dan judul rancangan proper	Tatap Muka	Untuk output dibuat Draft Perka, SOP dan Juknis	
3.	25-08-2022	Penyampaian arahan Coach terkait pelatihan dan usulan peralatan	WA Call	Agar dilaksanakan sesuai arahan	
4.	29-08-2022	Pemaparan bab pendahuluan latar belakang penyusunan RPP	Tatap Muka	Masukkan tentang hasil penilaian nilai indeks SPBE	
5.	31-08-2022	Pemaparan draft dalam rangka persiapan seminar rancangan proper	Tatap Muka	Dipelajari dengan seksama agar tidak terlewat saat seminar rancangan	

No	Tanggal	Isu/Permasalahan	Media Komunikasi	Hasil Coaching	Tanda tangan Mentor
6.	12-09-2022	Permohonan arahan terkait persiapan untuk implementasi proyek perubahan dengan pembentukan tim efektif	Tatap Muka	Agar diatur waktu untuk dilaksanakan rapat pembentukan tim efektif	
7.	13-09-2022	Rapat pembentukan Tim Efektif	Rapat Bersama	Segera dibuat Surat perintah Tim Efektif berdasarkan penjelasan hasil rapat	
8	02-11-2022	Analisa dan Evaluasi Akhir	Rapat Bersama	Agar dicek kembali dan disusun yang berurutan berdasarkan evidence kegiatan yang telah dilaksanakan	

No	Tanggal	Isu/Permasalahan	Media Komunikasi	Hasil Coaching	Tanda tangan Mentor
6.	12-09-2022	Permohonan arahan terkait persiapan untuk implementasi proyek perubahan dengan pembentukan tim efektif	Tatap Muka	Agar diatur waktu untuk dilaksanakan rapat pembentukan tim efektif	
7.	13-09-2022	Rapat pembentukan Tim Efektif	Rapat Bersama	Segara dibuat Surat perintah Tim Efektif berdasarkan penjelasan hasil rapat	
8	02-11-2022	Analisa dan Evaluasi Akhir	Rapat Bersama	Agar dicek kembali dan disusun yang berurutan berdasarkan evidence kegiatan yang telah dilaksanakan	

Mengetahui dan disetujui oleh

Atasan Langsung/Mentor,


 FERDINAND MAHULETTE, S.E.
 BRIGJEN TNI NRP 1900026591265

LAMPIRAN 13

PROMOSI

MEDIA ELEKTRONIK

BROSUR DAN LEAFLET

DATA PRIBADI TANGGUNG JAWAB SIAPA?

Apa sih yang dimaksud dengan data pribadi?

Data pribadi didefinisikan sebagai setiap data tentang **seseorang**, baik yang teridentifikasi dan/atau dapat diidentifikasi secara **tersendiri** atau **dikombinasi** dengan informasi lainnya baik secara **langsung** maupun **tidak langsung** melalui sistem elektronik dan/atau nonelektronik



#1

www.bsm.go.id

#JagaRuangSiber



Jenis data pribadi **ada dua**. Pertama, data pribadi yang bersifat **umum**, seperti nama lengkap, jenis kelamin, kewarganegaraan, agama, dan/atau data pribadi yang dikombinasikan untuk mengidentifikasi seseorang

Kedua, data pribadi yang bersifat **spesifik**, meliputi data dan informasi kesehatan, data biometrik (sidik jari, iris mata, bentuk wajah, tinggi badan), data genetika, kehidupan/orientasi seksual, pandangan politik, catatan kejahatan, data anak, data keuangan pribadi, dan/atau data lainnya sesuai dengan ketentuan **peraturan perundang-undangan**

#2

www.bsm.go.id

#JagaRuangSiber

Siapa yang harus melindungi data pribadi?

Semua pihak mulai dari pemilik data pribadi hingga penyelenggara sistem elektronik yang mengelola data pribadi memiliki tanggung jawab untuk melindungi data pribadi sesuai dengan kapasitas masing-masing



Sebagai pribadi, seseorang melindungi data pribadi yang dimiliki dengan tidak sembarangan membagikannya serta menjaga keamanan data pribadi yang berada dalam media penyimpanan maupun dalam gawai serta akun elektroniknya.

#3

www.bsm.go.id

#JagaRuangSiber



Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik Pasal 3 Ayat 1

"Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik **secara andal dan aman** serta **bertanggung jawab** terhadap beroperasinya Sistem elektronik sebagaimana mestinya."

#4

www.bsm.go.id

#JagaRuangSiber



Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik Pasal 3 Ayat 1

"Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem elektronik sebagaimana mestinya."

#4

www.bssn.go.id

#JagaRuangSiber



Menurut Pasal 14 Ayat 1 Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Penyelenggara Sistem Elektronik wajib melaksanakan prinsip perlindungan data pribadi dari kehilangan, penyalahgunaan, akses dan pengungkapan yang tidak sah.

Sedangkan dalam Ayat 5 dikatakan jika terjadi kegagalan dalam perlindungan terhadap Data Pribadi yang dikelolanya, Penyelenggara Sistem Elektronik wajib memberitahukan secara tertulis kepada pemilik data pribadi tersebut. Peraturan BSSN Nomor 8 Tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik menyatakan Penyelenggara Sistem Elektronik adalah setiap orang, penyelenggara negara, badan usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan Sistem Elektronik secara sendiri-sendiri maupun bersama-sama kepada pengguna Sistem Elektronik untuk keperluan dirinya dan/atau keperluan pihak lain.

#5

www.bssn.go.id

#JagaRuangSiber

BERSAMA KITA BISA LINDUNGI
DATA PRIBADI KITA



Transformasi digital merupakan suatu keniscayaan yang tidak terelakkan. Berbagai informasi data pribadi semakin banyak dipertukarkan secara elektronik melalui ruang siber. Yuk bersama kita jaga keamanan data pribadi kita.

Keamanan siber pada dasarnya merupakan tanggung jawab bersama seluruh pemangku kepentingan keamanan siber, baik penyelenggara negara, pelaku usaha, akademisi, maupun komunitas/masyarakat.

BSSN selaku lembaga yang berwenang untuk merumuskan dan menetapkan kebijakan teknis di bidang keamanan siber telah menyusun pedoman pengamanan dan penyelenggaraan Sistem Elektronik.

#6

www.bssn.go.id

#JagaRuangSiber

#Kamis
#KeamananSiber

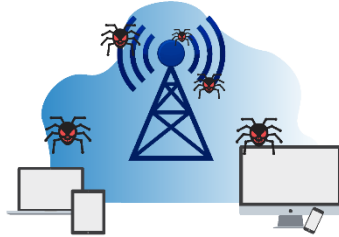


Berikut beberapa langkah yang dapat mengurangi beberapa risiko:

- Perbarui sistem operasi perangkat dan aplikasi seluler secara berkala.
- Waspada! konten dari pengirim yang tidak dikenal, terutama yang berisi tautan atau lampiran.
- Periksa URL sebelum mengklik tautan, atau kunjungi situs web secara langsung.
- Enkripsi dan gunakan kata sandi untuk melindungi perangkat Anda.
- Gunakan Jaringan Pribadi.
- Nonaktifkan opsi geo-lokasi dan tutup kamera pada perangkat.

www.bssn.go.id

Lindungi diri anda dari Alat Pengawasan Komersial



Hal ini memungkinkan kriminal untuk menginfeksi perangkat seluler dan perangkat yang terhubung ke internet dengan malware melalui WiFi dan data seluler. kriminal dapat menginfeksi perangkat yang ditargetkan tanpa tindakan dari perangkat pemilik.

#Kamais
#KeamananSiber

www.bssn.go.id

 **BADAN SIBER
DAN SANDI
NEGARA** 

WASPADA MODUS SOCENG

1. Tawaran Nasabah Prioritas
2. Layanan Konsumen Bodong
3. Biaya Administrasi



www.bssn.go.id



Sebagai salah satu bentuk kolaborasi upaya pencegahan serangan siber, sepanjang tahun 2022, BSSN mengirimkan 1.261 notifikasi kepada berbagai organisasi/kementerian/instansi pemangku kepentingan keamanan siber nasional

www.bssn.go.id

#JagaRuangSiber

www.bssn.go.id



Yuk, bersama kita #JagaRuangSiber Indonesia.
Terus update informasi mengenai risiko dan cara menghadapi phishing.

#JagaRuangSiber



**BADAN SIBER
DAN SANDI
NEGARA**

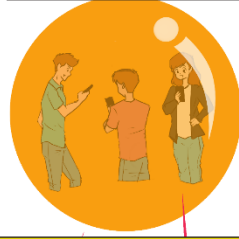
FILTER BUBBLE

filter bubble adalah istilah yang menggambarkan bagaimana algoritma menentukan informasi apa saja yang akan kita temukan di internet.



Echo Chamber

Ruang tempat kita hanya mendengar apa yang kita inginkan tanpa ingin tahu kondisi yang sebenarnya

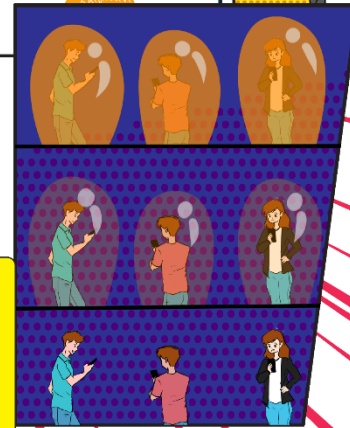
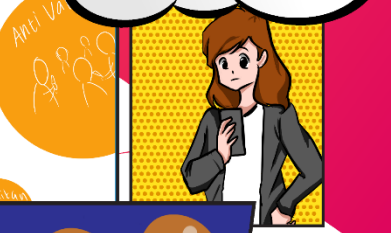


Cara Menghindari Filter Bubble:

1. Cari Literasi sebanyak-banyaknya jangan hanya dari satu sumber
2. Netral dalam menerima informasi dan telaah lebih dalam sebelum berpendapat.

Dampak dari Filter Bubble

1. Sudut Pandang terkurung
2. Mempersempit Wawasan
3. Kurang Mengerti Realita yang Sebenarnya



Biro Hukum dan Komunikasi Publik BSSN



**BADAN SIBER
DAN SANDI
NEGARA**

**G20 INDONESIA
2022**

SIAP
MELAYANI
BSSN



ANTISIPASI TERHADAP PENINGKATAN AKTIFITAS PHISHING EMAIL DI LINGKUNGAN BSSN

Bagaimana mengidentifikasinya?

- Meminta Pasward dan akses pribadi lainnya.
- Berisi ancaman dan meminta respon cepat.

IMBAUAN

- Abaikan pesan yang meminta data pribadi.
- Teliti pesan tersebut lebih lanjut dengan melihat isi pesan asli.
- Menggunakan Antivirus
- Hanya Gunakan email dinas untuk keperluan Dinas



Hubungi HALO PUSDATIK

Jika ada pertanyaan tentang email yang anda terima, silahkan menghubungi Halo Pusdatik di nomor 08119705056 (Whatsapp) dengan menggunakan form insiden yang ada pada tautan berikut <https://drive.bssn.go.id/s/DHn4NrtowCH4aNB>

#JagaRuangSiber

Biro Hukum dan Komunikasi Publik BSSN

www.bssn.go.id

[@bssn_ri](https://www.instagram.com/bssn_ri)

[Badan Siber dan Sandi Negara](https://www.facebook.com/bssn.ri)

[Badan Siber dan Sandi Negara](https://www.facebook.com/bssn.ri)

[@bssn_ri](https://www.facebook.com/bssn.ri)



Edukasi Masyarakat

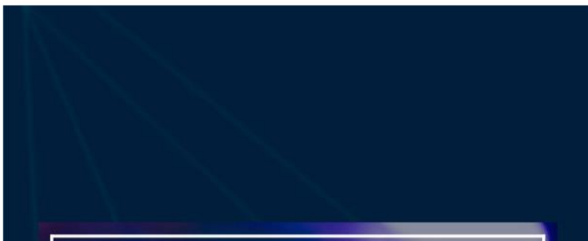
Budaya Keamanan Informasi

Pemanfaatan internet telah mengubah pola hidup dan budaya manusia dalam belajar, bekerja, berkomunikasi, berbelanja dan aspek lainnya. Saat ini masyarakat lebih banyak menggunakan internet dalam berkomunikasi seperti surat elektronik (*e-mail*) serta jejaring sosial (*social networking*) yang dianggap lebih efektif dan efisien. Kini kita berkomunikasi di dunia maya sama seperti halnya ketika berkomunikasi di dunia nyata. Informasi yang didapatkan semakin terbuka baik konten positif maupun negatif.

Pengaruh konten negatif sudah sering diberitakan di berbagai media berupa pemuatan gambar porno, perjudian, penipuan, pelecehan, pencemaran nama baik dan berita bohong. Selain itu penggunaan jejaring sosial juga memiliki dampak negatif, salah satunya adalah cyberbullying yang biasanya menimpa anak-anak dan sesama remaja. Bahkan kejahatan dunia maya yang dikenal



IMBAUAN KEAMANAN



INFO TERKINI

Bertepatan dengan Momentum Hari Santri Nasional Tahun 2022, BSSN, Kominfo, dan Lembaga Persahabatan Ormas Islam Berkolaborasi Bekali Kalangan Santri Indonesia Jadi Garda Depan Keamanan dan Kedaulatan Siber Nasional



Waspada Malware



Badan Siber dan ...
12.5K subscribers

Subscribe

30



Share



#ruangsiber #shareyangbaik

jejak digital



Badan Siber dan ...
12.5K subscribers

Subscribe

44



Share





Waspada pengambilalihan kode rahasia (OTP FRAUD)



Badan Siber dan ...
12.5K subscribers

Subscribe

31



Share



Selalu Cek Kebenaran Informasi dan Jadilah Pahlawan Kebenaran Informasi



Badan Siber dan ...
12.5K subscribers

Subscribe

11



Share





