KEMENTERIAN HUKUM DAN HAK ASASI MANUSIA
REPUBLIK INDONESIA
INSPEKTORAT JENDERAL
Jl. H.R. Rasuna Said Kav. X-6 No.8, Kuningan
Jakarta Selatan 12940, P.O. Box 3489, Telepon/Faksimili 021-5252975
Laman : http://www.itjen.kemenkumham.go.id, Surel : itjen@kemenkumham.go.id

Nomor : ITJ-PW.02.04-115 20 Februari 2024
Sifat : Sangat Segera
Lampiran : -
Hal : Permohonan Narasumber Kegiatan Aktif Belajar Kolaboratif di Lingkungan Inspektorat Jenderal Kementerian Hukum dan Hak Asasi Manusia Periode Bulan Maret Tahun 2024

Yth. Deputi Bidang Operasi Keamanan Siber dan Sandi
Badan Siber dan Sandi Negara (BSSN)
di Jakarta

Sehubungan dengan pelaksanaan kegiatan Aktif Belajar Kolaboratif Periode Bulan Maret Tahun 2024 di Lingkungan Inspektorat Jenderal Kementerian Hukum dan Hak Asasi Manusia yang akan dilaksanakan secara *offline* pada:

Hari / Tanggal : Kamis, 14 Maret 2024
Pukul : 09.00 – 11.00 WIB
Tempat : Auditorium Inspektorat Jenderal Lt. 16 Kementerian Hukum dan HAM
Materi : Audit Keamanan SPBE

Berkenaan dengan hal tersebut, diharapkan agar konfirmasi kesediaan awal menjadi narasumber pada kegiatan dimaksud melalui tautan https://forms.gle/RYXX168itTAdr6sdA paling lambat hari Jumat, 1 Maret 2024. Adapun biaya yang timbul atas pelaksanaan kegiatan ini sepenuhnya menjadi beban DIPA Inspektorat Jenderal Kementerian Hukum dan HAM Tahun Anggaran 2024. Untuk keterangan lebih lanjut dapat menghubungi Sdr. Anjas (087763744968).

Demikian kami sampaikan. Atas perhatian dan kerjasama Saudara, kami ucapkan terimakasih.

Inspektur Jenderal,

RAZILU
NIP 196511281991031002

KEMENTERIAN HUKUM DAN HAK ASASI MANUSIA
REPUBLIK INDONESIA
INSPEKTORAT JENDERAL
Jl. H.R. Rasuna Said Kav. X-6 No. 8, Kuningan,
Jakarta Selatan 12940, P.O. Box 3489, Telepon/Faksimili 021-5252975
Laman: http://www.itjen.kemenkumham.go.id, Surel: itjen@kemenkumham.go.id

NOTULA

Aktif Belajar Kolaboratif Bulan Maret Tahun 2024 Hari-II

dengan tema "Audit Kemananan SPBE"

Hari/Tanggal	:	Kamis, 14 Maret 2024
Tempat	:	Ruang Auditorium Inspektur Jenderal Kementerian Hukum dan HAM
Pukul	:	09.00 s.d 11.00 WIB
Tema	:	Audit Kemananan SPBE
Narasumber	:	Firdaus Kifli, S.ST., M.AP
Peserta	:	1. Inspektur Wilayah III 2. Perwakilan Auditor Inspektorat Wilayah I 3. Perwakilan Auditor Inspektorat Wilayah II 4. Perwakilan Auditor Inspektorat Wilayah III 5. Perwakilan Auditor Inspektorat Wilayah IV 6. Perwakilan Auditor Inspektorat Wilayah V 7. Perwakilan Auditor Inspektorat Wilayah VI

Sesi Pemaparan:

Kegiatan dibuka oleh MC dan diserahkan kepada moderator yaitu Bapak Vito Adriano Wismar dan diserahkan kepada Bapak Firdaus Kifli selaku Narasumber dari Badan Siber dan Sandi Negara (BSSN). Dalam paparannya Bapak Firdaus Kifli menyampaikan materi tentang Audit Keamanan Aplikasi Khusus Sistem Pemerintahan Berbasis Elektronik (SPBE), dengan pembahasan sebagai berikut:

1. Dasar Pelaksanaan Audit Keamanan SPBE

a) Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik
b) Peraturan Presiden Nomor 132 Tahun 2022 tentang Arsitektur Sistem Pemerintahan Berbasis Elektronik Nasional
c) Peraturan Menteri PANRB Nomor 59 Tahun 2020 tentang Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik
d) Peraturan Menteri Komunikasi dan Informasi Nomor 16 Tahun 2022 tentang Kebijakan Umum Penyelenggaraan Audit Teknologi Informasi dan Komunikasi

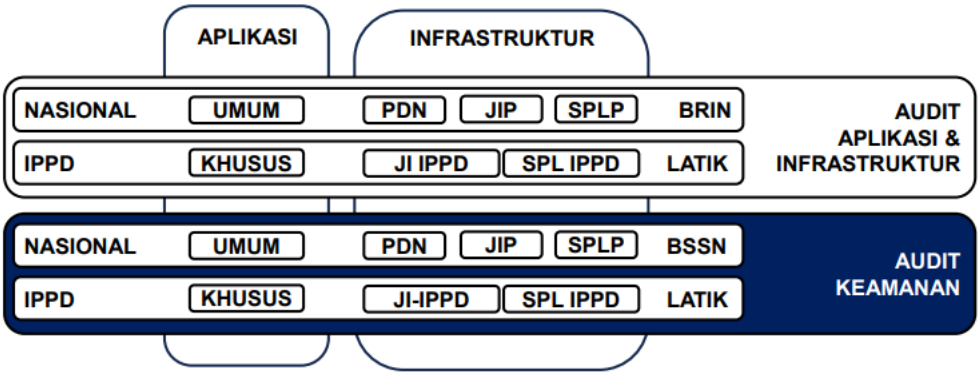
e) Peraturan BSSN Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik
f) Peraturan BSSN Nomor 4 Tahun 2023 tentang Perubahan Atas Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara
g) Rancangan Peraturan BSSN tentang Standar dan Tata Cara Audit Keamanan SPBE

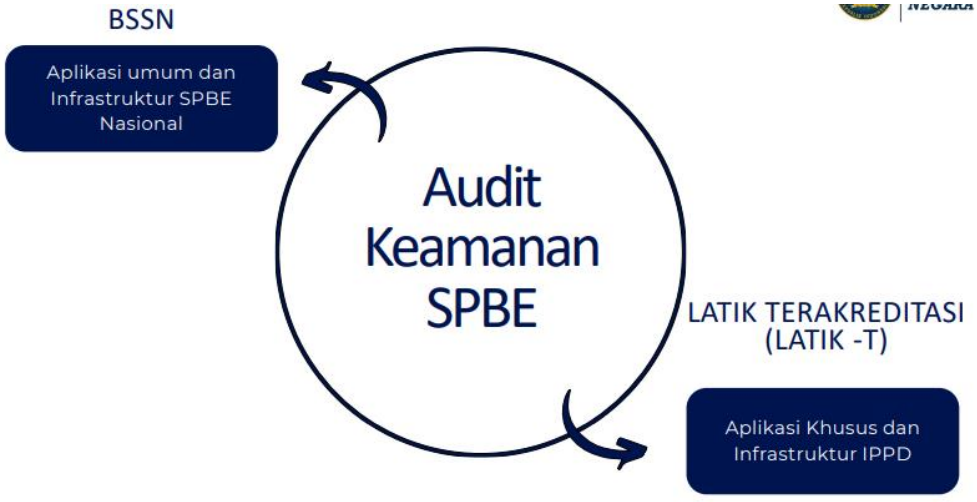
2. Audit TIK SPBE

Berdasarkan Pasa1 1 Peraturan Presiden Nomor 95 Tahun 2018:

- Audit Teknologi Informasi dan Komunikasi adalah proses yang sistematis untuk memperoleh dan mengevaluasi bukti secara objektif terhadap aset teknologi informasi dan komunikasi dengan tujuan untuk menetapkan tingkat kesesuaian antara teknologi informasi dan komunikasi dengan kriteria dan/atau standar yang telah ditetapkan.
- Aplikasi Umum adalah Aplikasi SPBE yang sama, standar, dan digunakan secara bagi pakai oleh instansi pusat dan/atau pemerintah daerah.
- Aplikasi Khusus adalah Aplikasi SPBE yang dibangun, dikembangkan, digunakan, dan dikelola oleh instansi pusat atau pemerintah daerah tertentu untuk memenuhi kebutuhan khusus yang bukan kebutuhan instansi pusat dan pemerintah daerah lain.

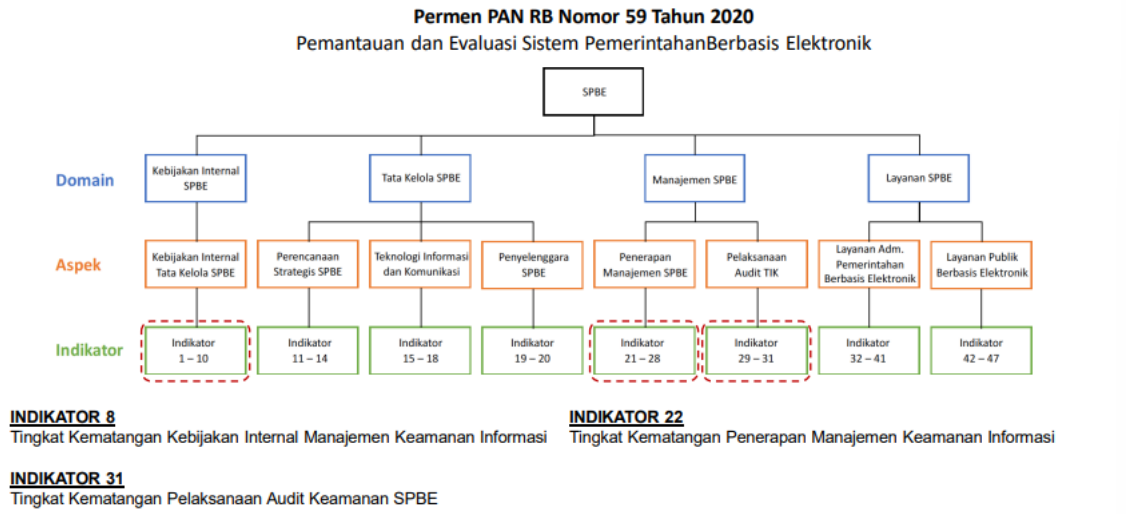
Semesta Audit TIK SPBE





Audit TIK (Cakupan Keamanan)

Proses yang sistematis untuk memperoleh dan mengevaluasi bukti secara objektif terhadap keamanan aset TIK dengan tujuan untuk menetapkan tingkat kesesuaian antara keamanan TIK dengan kriteria dan/atau standar keamanan yang telah ditetapkan.



Indikator 31: Tingkat kematangan Pelaksanaan Audit Keamanan SPBE

Tingkat 1 : Kegiatan Audit Keamanan SPBE belum atau telah dilaksanakan. Kondisi: Kegiatan Audit Keamanan dilaksanakan tanpa perencanaan yang berkesinambungan

Tingkat 2 : Kriteria tingkat 1 telah terpenuhi dan kegiatan Audit Keamanan dilaksanakan sesuai dengan perencanaan berkesinambungan. Kondisi: Kegiatan Audit Keamanan dilaksanakan tanpa pedoman Audit Keamanan

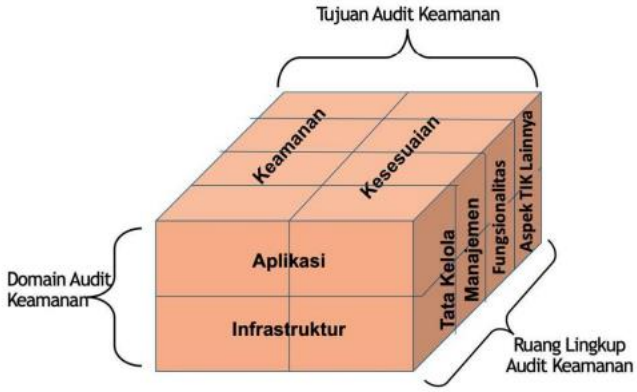
Tingkat 3 : Kriteria tingkat 2 telah terpenuhi dan kegiatan Audit Keamanan dilaksanakan sesuai dengan pedoman Audit Keamanan. Kondisi : kegiatan Audit Keamanan dilaksanakan oleh auditor TIK/Sistem Keamanan Informasi internal Instansi Pusat/Pemerintah Daerah

Tingkat 4 : Kriteria tingkat 3 telah terpenuhi dan kegiatan Audit Keamanan dilaksanakan oleh auditor TIK/Sistem Keamanan Informasi eksternal yang memiliki sertifikasi auditor TIK/Sistem Keamanan Informasi.

Tingkat 5 : Kriteria tingkat 4 telah terpenuhi dan hasil audit Keamanan SPBE telah ditindaklanjuti melalui perbaikan penerapan Keamanan SPBE.

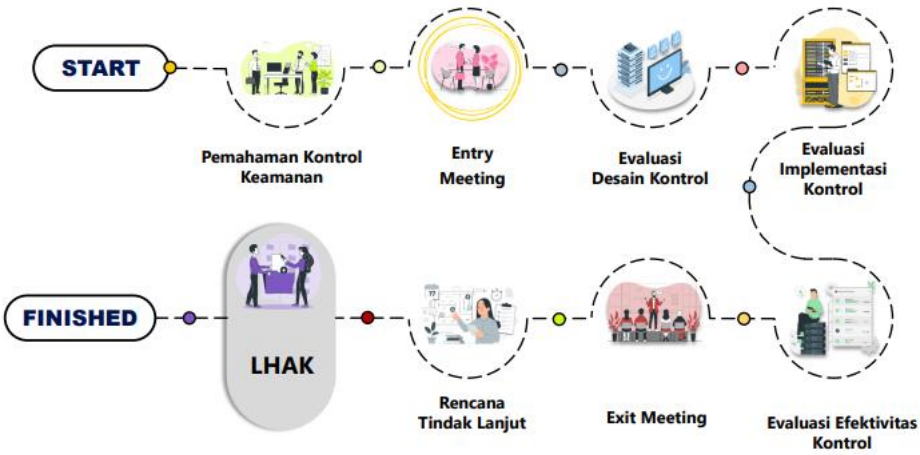
3. Proses Audit Keamanan Aplikasi Khusus dan Infrastruktur IPPD

Pemeriksaan Hal Pokok Teknis

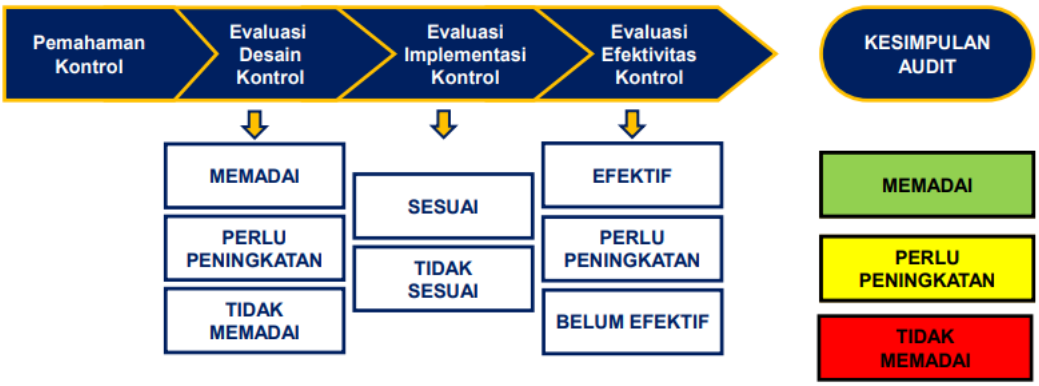


Sumber: Peraturan Presiden No 95 Tahun 2018 tentang SPBE

Tahapan Pelaksanaan Audit Keamanan SPBE



Kesimpulan Audit Keamanan SPBE



Metode Penarikan Kesimpulan

Kondisi	Evaluasi Desain Kontrol	Evaluasi Implementasi Kontrol	Evaluasi Efektivitas Kontrol	Kesimpulan Audit
1	Memadai	Sesuai Dengan Desain Kontrol	Efektif	Memadai
			Perlu Peningkatan	Memadai
			Belum Efektif	Perlu Peningkatan
		Tidak Sesuai Dengan Desain Kontrol	Efektif	Perlu Peningkatan
			Perlu Peningkatan	Tidak Memadai
			Belum Efektif	Tidak Memadai
2	Perlu Peningkatan	Sesuai Dengan Desain Kontrol	Efektif	Memadai
			Perlu Peningkatan	Perlu Peningkatan
			Belum Efektif	Tidak Memadai
		Tidak Sesuai Dengan Desain Kontrol	Efektif	Tidak Memadai
			Perlu Peningkatan	Tidak Memadai
			Belum Efektif	Tidak Memadai
3	Tidak Memadai	--	Efektif	Tidak Memadai
			Perlu Peningkatan	Tidak Memadai
			Belum Efektif	Tidak Memadai

Tanya Jawab:

1. Pertanyaan dari Anton Kurniawan:
   Terdapat 3 evaluasi kontrol. Apa saja yang kita evaluasi? Apakah ada toolsnya karena terkait dengan waktu evaluasi yang 1-2 hari?

   Jawaban Narasumber:

   Akan dijelaskan di materi selanjutnya, ada tools untuk penilaian audit sesuai pedoman. Untuk waktu sesuai pedoman yang telah kita lakukan selama ini berjalan dengan baik, dengan tim yang muda dan basic IT. Untuk audit keamanan sebaiknya ada yang memiliki basic IT, di tim kami pada aspek teknis ada spesialisasinya.

2. Pertanyaan dari Raymond Tinating Pangihutan Siagian:
   Apa saja Layanan SPBE? Secara umum dan khusus? Apakah ada kaitannya dengan Survei Kepuasan Pelanggan?

   Jawaban Narasumber:

   Setelah selesai audit terdapat kewajiban untuk mengisi survey kepuasan.

Materi selanjutnya tentang Teknis Pelaksanaan Audit Keamanan Sistem Pemerintahan Berbasis Elektronik disampaikan oleh Ibu Siti Marfuah, dengan pembahasan sebagai berikut:

1. Kriteria dan Kontrol Keamanan

Kriteria yaitu berbagai peraturan perundangperundangan dan/atau kebijakan, prosedur, dan instruksi kerja, serta standar dan praktik-praktik terbaik, yang digunakan oleh Auditor TIK untuk melakukan evaluasi dan pengujian atas pengendalian intern TIK, manajemen risiko TIK dan tata kelola TIK (Peraturan Menteri Kominfo 16/2022).

Kontrol Kemananan yaitu sekumpulan aktivitas keamanan yang harus didefinisikan dan dilaksanakan. Kontrol keamanan diturunkan dari kriteria audit keamanan.

2. Prosedur pada Tahapan Pelaksanaan Audit Keamanan SPBE

1) Pemahaman Desain Kontrol

Prosedur yang dilakukan Auditor Keamanan Informasi dalam mengidentifikasi informasi terdokumentasi untuk memperoleh pemahaman yang memadai tentang kontrol keamanan SPBE.

Hal-hal yang dilakukan Auditor:

a. Mengumpulkan data dukung awal seperti peraturan, kebijakan, prosedur, dan data/informasi pendukung lainnya dan berkaitan dengan Objel yang diaudit.
b. Mempelajari dan memahami data dukung awal yang telah diberikan Auditan.

2) Evaluasi Desain Kontrol

Prosedur yang dilakukan Auditor Keamanan Informasi untuk melakukan evaluasi atas kelaikan desain kontrol keamanan aplikasi/objek yang audit, dibandingkan dengan kontrol keamanan yang ada pada kriteria audit keamanan. Hal tersebut dilakukan untuk memperoleh keyakinan yang memadai bahwa desain kontrol keamanan yang ada telah sesuai dengan kontrol keamanan pada kriteria audit keamanan.

Hal-hal yang dilakukan Auditor:

a. Auditor melakukan identifikasi desain control keamanan yang akan diuji terhadap kriteria;
b. Auditor melakukan wawancara dengan auditan terkait desain control keamanan yang dimiliki, dalam pengembangan dan pengelolaan Aplikasi;
c. Auditor melakukan evaluasi kesesuaian terhadap bukti atau data dukung desain kontrol keamanan yang dimiliki Auditan.

3) Evaluasi Implementasi Kontrol

Prosedur yang dilakukan Auditor Keamanan Informasi untuk memperoleh keyakinan yang memadai bahwa implementasi kontrol telah sesuai dengan desain kontrol yang ada.

Hal-hal yang dilakukan Auditor:

a. Auditor melakukan wawancara dengan auditan terkait implementasi dari control keamanan pada aplikasi;
b. Auditor melakukan reviu/observasi bukti atau data dukung yang diberikan Auditan;

c. Auditor melakukan pengujian langsung terhadpa aplikasi pada tahap implementasi control keamanan jika diperlukan.

4) Evaluasi Efektivitas Kontrol

Prosedur yang dilakukan Auditor Keamanan Informasi untuk:

a. Memperoleh keyakinan yang memadai bahwa kontrol keamanan SPBE yang berjalan telah dapat mencapai tujuannya dengan efektif; ATAU

b. Mengidentifikasi risiko yang terjadi karena adanya kelemahan desain dan/atau implementasi kontrol keamanan SPBE.

Hal-hal yang dilakukan Auditor:

a. Auditor melakukan pemeriksaan lanjutan untuk memastikan pencapaian tujuan keamanan, yang dapat dilakukan melalui: 1. Metode survei (sampling); dan/atau 2. Pengujian Teknis Aplikasi.

b. Auditor melakukan wawancara dengan auditan guna memperkuat keyakinan auditor terkait efektivitas kontrol keamanan.

Tanya Jawab:

1. Pertanyaan dari Iqbal Albert Husein:

   Bagaiman susunan tim dalam Audit Keamanan SPBE? Berikut dengan output kerjanya seperti apa? Pertanyaan kedua, apakah kebutuhan dokumen audit semua harus terpenuhi? Dokumen-dokumen yang dibutuhkan apakah disusun dari Itjen atau Ditjen Imigrasi?

   Jawaban dari Narasumber:

   Surat permintaan dari sudut pandang selaku auditor eksternal, inisiatornya inspektorat. Dari kami harus mendapatkan surat permintaan dari Inspektorat, Inspektorat yang menentukan level berapa yang mau diaudit dan bersurat kepada BSSN.
   Sedangkan untuk Aplikasi umum inisiatornya dari BSSN.

   Tanggapan dari Iqbal Albert Husain:
   Kami (Kemenkumham) sudah mendapatkan level 3, apakah kami bisa bersurat untuk meningkatkan level menjadi 4?

   Jawaban dari Narasumber:
   Silahkan Inspektorat bersurat pada BSSN, nanti akan kami diskusikan lebih lanjut untuk timnya. Surat Jawaban dari kami nantinya berisi pelaksanaan tugas mulai dari susunan tim (Deputi, Direktur, Supervisi Manajemen dan Supervisi Teknis, Ketua Tim, Anggota Tim) Kompleksitas susunan tim tergantung dari kompleksitas aplikasi yang akan diaudit.
   Output isinya temuan sesuai indikator, aspek teknis dan aspek manajemen. Outputnya adalah Laporan Hasil Akhir yang berisi rekomendasi tindak lanjut.

2. Pertanyaan dari Eem Nurmanah:
   Dari segi SDM, apa saja yang sudah dilakukan SDM terkait dengan pengembangan kompetensi?

   Jawaban dari Narasumber:
   Pahami basic pengantar dari siber security, dari google class room yang free, pengantar-pengantar siber minimal memahami istilah-istilah dalam dokumen audit. Setelah itu kompetensi memahami secara spesifik, aspek teknis dan aspek manajemen, karena di BSSN sendiri terdapat peminatan terkait 2 aspek tersebut yaitu Spesialisasi audit SPBE. Untuk hal tersebut, dalam proses audit bisa menggunakan pihak lain sebagai anggota tim audit.

3. Pertanyaan dari Iqbal Albert Husain:
   Dari sisi alokasi anggaran, apakah dari instansi atau dari BSSN?

   Jawaban dari Narasumber:
   Anggaran di BSSN hanya terkait aplikasi umum, untuk aplikasi khusus biasanya alokasi anggaran dari instansi terkait.

Kegiatan Aktif Belajar Kolaboratif hari kedua ditutup pada pukul 16.00.

Mengetahui,

#KUMHAMPASTI

Ditandatangani secara elektronik oleh :

Iwan Santoso
NIP 197004301991031001

Notulis

Dian Lati Utami
NIP 199305172020122001