# PEDOMAN KONSEPSI
# PERENCANAAN PENGAWASAN INTERN BERBASIS RISIKO BAGI APIP DAERAH


BADAN PENGAWASAN KEUANGAN DAN PEMBANGUNAN
DEPUTI BIDANG PENGAWASAN PENYELENGGARAAN KEUANGAN DAERAH
2018

Integritas - Inovasi - Independen

## KATA PENGANTAR

Rencana Jangka Panjang Menengah Nasional (RPJMN) Tahun 2015-2019 mengamanatkan agar kapabilitas Aparat Pengawasan Intern Pemerintah (APIP), termasuk APIP Daerah, berada pada Level 3. APIP Daerah yang memiliki Kapabilitas pada level 3 diharapkan dapat memberikan nilai tambah dalam aspek ekonomis, efektivitas, dan efisiensi serta dapat memberikan perbaikan kepada pemerintah dari sisi *governance, risk* dan *control*.

Untuk mencapai Level 3, *Internal Audit Capability Model* (IA-CM) mensyaratkan agar APIP Daerah mampu melakukan pengawasan pada kegiatan-kegiatan yang memiliki risiko tinggi. Hal ini dapat dilakukan apabila APIP Daerah memiliki perencanaan pengawasan yang berbasis pada risiko auditan.

Kedeputian Bidang Pengawasan Penyelenggaraan Keuangan Daerah sebagai fungsi Perencanaan dan Pengendalian (Rendal) memandang perlu untuk menyusun *Pedoman Perencanaan Pengawasan Intern Berbasis Risiko Bagi APIP Daerah* dan *Buku Saku Praktik Penyusunan Perencanaan Pengawasan Berbasis Risiko Bagi APIP Daerah*. Keduanya diharapkan dapat memberikan gambaran umum dan menyamakan persepsi APIP Daerah terkait dengan perencanaan pengawasan berbasis risiko.

Buku saku ini akan terus dipantau serta disesuaikan dengan perkembangan terkini dari teori dan praktik-praktik pengawasan intern terbaik dan dinamika kepemerintahan di Indonesia.

Jakarta, 2 Juli 2018
Deputi Kepala BPKP

Gatot Darmasto
NIP 19591121 198503 1 001

**DAFTAR ISI**

## DAFTAR ISTILAH

Aparat Pengawasan Intern Pemerintah (APIP) adalah instansi pemerintah yang dibentuk dengan tugas melaksanakan pengawasan intern di lingkungan pemerintah pusat dan/atau pemerintah daerah, yang terdiri dari Badan Pengawasan Keuangan dan Pembangunan (BPKP), Inspektorat Jenderal/Inspektorat/Unit Pengawasan Intern pada Kementerian/Kementerian Negara, Inspektorat Utama/Inspektorat Lembaga Pemerintah Non Kementerian, Inspektorat/Unit Pengawasan Intern pada Kesekretariatan Lembaga Tinggi Negara dan Lembaga Negara, Inspektorat Provinsi/Kabupaten/Kota, dan Unit Pengawasan Intern pada Badan Hukum Pemerintah lainnya sesuai dengan peraturan perundang-undangan.

APIP Daerah adalah Inspektorat Provinsi/Kabupaten/Kota

*Assurance* adalah sebuah jasa profesional dan independen yang meningkatkan kualitas informasi untuk para pengambil keputusan. Termasuk jasa *assurance* yaitu audit, reviu, evaluasi, dan pemantauan/monitoring.

Audit adalah proses identifikasi masalah, analisis, dan evaluasi yang dilakukan secara independen, objektif, dan profesional berdasarkan standar audit, untuk menilai kebenaran, kecermatan, kredibilitas, efektivitas, efisiensi, dan keandalan informasi pelaksanaan tugas dan fungsi instansi pemerintah.

Audit intern adalah kegiatan yang independen dan objektif dalam bentuk pemberian keyakinan (*assurance activities*) dan konsultansi (*consulting activities*), yang dirancang untuk memberi nilai tambah dan meningkatkan operasional sebuah organisasi (auditi). Kegiatan ini membantu organisasi (auditi) mencapai tujuannya dengan cara menggunakan pendekatan yang sistematis dan teratur untuk menilai dan meningkatkan efektivitas dari proses manajemen risiko, kontrol (pengendalian), dan tata kelola (sektor publik).

*Audit universe* adalah seluruh populasi *auditable unit*.

*Auditable unit* adalah urusan/OPD/program/kegiatan yang dapat dilakukan pengawasan.

Dampak risiko/konsekuensi (*impact*) adalah dampak jika risiko yang diidentifikasi terjadi atau diputuskan diambil, yang memberi dampak positif atau negatif.

Faktor risiko adalah istilah yang digunakan untuk menggambarkan faktor-faktor umum yang dapat mengindikasikan tingkat risiko yang lebih tinggi dan/atau mempengaruhi penentuan prioritas pada suatu bagian dari *audit universe.* Dalam panduan ini, penggunaan faktor risiko ditujukan untuk penentuan prioritas *auditable unit*.

Kemungkinan kejadian/probabilitas (*likelihood*) risiko adalah kemungkinan terjadinya risiko.

Manajemen risiko adalah sebuah proses untuk mengidentifikasi, menilai, mengelola, dan mengendalikan peristiwa atau situasi potensial untuk memberikan keyakinan memadai tentang pencapaian tujuan organisasi. Tata Kelola adalah kombinasi proses dan struktur yang dilaksanakan oleh manajemen untuk menginformasikan, mengarahkan, mengelola, dan memantau kegiatan organisasi menuju pencapaian tujuannya.

Pengendalian adalah tindakan apapun yang diambil oleh manajemen dan/atau pihak lain untuk mengelola risiko dan memberikan masukan yang dapat meningkatkan

kemungkinan bahwa tujuan dan sasaran akan dicapai. Manajemen merencanakan, mengatur, dan mengarahkan pelaksanaan tindakan yang memadai untuk memberikan keyakinan memadai bahwa tujuan dan sasaran akan dicapai.

Register risiko adalah suatu daftar yang menunjukkan seluruh risiko yang dihadapi termasuk informasi tambahan atas masing-masing risiko tersebut seperti probabilitas risiko, dampak risiko, penanggung jawab risiko, dan mitigasi/pengendalian risiko..

Risiko adalah kemungkinan terjadinya suatu peristiwa atau kejadian yang berdampak negatif pada pencapaian tujuan.

Risiko inheren adalah risiko yang melekat di organisasi sebelum adanya upaya tindakan pengendalian untuk mengubah kemungkinan dan dampak risiko.

*Risk Appetite* adalah tingkat risiko yang dapat diterima oleh manajemen.

# I. PENDAHULUAN

## A. LATAR BELAKANG

Standar Audit Intern Pemerintah Indonesia (SAIPI) paragraf 3010, mensyaratkan Pimpinan APIP untuk menyusun rencana strategis dan rencana kegiatan audit intern tahunan dengan prioritas pada kegiatan yang mempunyai risiko terbesar dan selaras dengan tujuan APIP. Hal tersebut dimaksudkan agar APIP mengelola dan mengalokasikan sumber daya yang dimiliki secara efektif untuk area yang memiliki risiko tertinggi yang akan berdampak pada tujuan organisasi (Asosisasi Auditor Intern Pemerintah Indonesia/AAIPI, 2013).

Berdasarkan Peraturan Pemerintah Nomor 60 Tahun 2008 tentang Sistem Pengendalian Intern Pemerintah (SPIP), peran Aparat Pengawasan Intern (APIP) yang efektif diwujudkan dalam pelaksanaan kegiatan pengawasan intern dalam bentuk kegiatan penjaminan, kegiatan anti-korupsi, dan kegiatan layanan konsultansi (AAIPI, 2013). Pada kegiatan penjaminan, APIP menyelenggarakan kegiatan pengawasan intern dengan memberikan keyakinan yang memadai atas ketaatan, kehematan, efisiensi, dan efektivitas pencapaian tujuan penyelenggaraan tugas dan fungsi Instansi Pemerintah. Selanjutnya, dalam pelaksanaan kegiatan anti-korupsi APIP memberikan peringatan dini dan meningkatkan efektivitas manajemen risiko dalam penyelenggaraan tugas dan fungsi Instansi Pemerintah. Sedangkan dalam kegiatan layanan konsultansi, APIP memberikan masukan yang dapat memelihara dan meningkatkan kualitas tata kelola penyelenggaraan tugas dan fungsi Instansi Pemerintah.

Kegiatan pengawasan intern yang selaras dengan harapan pemangku kepentingan serta tujuan Pemerintah Daerah sangat diperlukan agar kegiatan pengawasan yang diselenggarakan APIP Daerah dapat memberikan nilai tambah dan perbaikan pada area tata kelola, manajemen risiko, dan pengendalian intern. Terkait dengan keselarasan kegiatan pengawasan intern dengan harapan pemangku kepentingan dan tujuan Pemerintah Daerah, penyusunan rencana strategis dan rencana pengawasan tahunan APIP Daerah merupakan salah satu tahapan penting karena kedua perencanaan tersebut menjadi rujukan pelaksanaan kegiatan pengawasan intern oleh APIP Daerah dalam suatu periode tertentu.

Untuk memenuhi persyaratan dalam SAIPI paragraf 3010, APIP Daerah memerlukan sebuah pendekatan sistematis dan terstruktur untuk memprioritaskan kegiatan berdasarkan risiko terbesar dan selaras dengan tujuan APIP Daerah. Pendekatan tersebut dikenal dengan istilah perencanaan pengawasan intern berbasis risiko.

Pedoman ini membahas konsepsi perencanaan pengawasan intern yang dilaksanakan oleh APIP Daerah.

## B. TUJUAN PEDOMAN

Terkait perencanaan pengawasan intern berbasis risiko, Deputi Bidang Pengawasan Penyelenggaraan Keuangan Daerah BPKP menerbitkan satu Pedoman dan satu Buku Saku yang ditujukan bagi APIP Daerah. Pedoman Konsepsi Perencanaan Pengawasan Intern Berbasis Risiko Bagi APIP Daerah ini bertujuan untuk membahas konsepsi yang bersifat umum mengenai perencanaan pengawasan intern berbasis risiko. Sedangkan Buku Saku – yang terdapat pada dokumen terpisah – membahas langkah-langkah secara lebih detil dalam penyusunan perencanaan pengawasan intern berbasis risiko. Pedoman dan buku saku tersebut dapat dijadikan rujukan, diadopsi dan/atau dimodifikasi oleh APIP Daerah dalam menyusun kebijakan perencanaan pengawasan tahunan di lingkungan kerjanya masing-masing.

## C. SISTEMATIKA PENYAJIAN

Pedoman ini disajikan dengan sistematika sebagai berikut:

I. Pendahuluan
   Bagian ini menguraikan latar belakang, tujuan dan sistematika penyajian pedoman.
II. Konsepsi Perencanaan Pengawasan Intern Berbasis Risiko
   Bagian ini membahas gambaran umum perencanaan pengawasan intern berbasis risiko yang meliputi karakteristik umum perencanaan pengawasan intern berbasis risiko.
III. Tahapan Perencanaan Pengawasan Intern Berbasis Risiko
   Bagian ini menguraikan pendekatan yang dapat digunakan APIP dalam mengklasifikasikan Peta Auditan (*audit universe*), mengidentifikasi dan menilai risiko, memprioritaskan rencana kegiatan pengawasan, serta mendokumentasikan dan mengkomunikasikan rencana pengawasan intern berbasis risiko.

## II. KONSEPSI PERENCANAAN PENGAWASAN INTERN BERBASIS RISIKO

### A. RISIKO DAN MANAJEMEN RISIKO

Pengertian risiko menurut SAIPI adalah kemungkinan terjadinya suatu peristiwa atau kejadian yang akan berdampak pada pencapaian tujuan (AAIPI, 2013). SAIPI mendefinisikan manajemen risiko sebagai proses untuk mengidentifikasi, menilai, mengelola, dan mengendalikan peristiwa atau situasi potensial untuk memberikan keyakinan memadai tentang pencapaian tujuan organisasi (AAIPI, 2013).

Proses manajemen risiko dimulai dengan mengidentifikasi peristiwa yang mungkin timbul dan dapat mengganggu pencapaian tujuan organisasi. Risiko yang melekat di suatu organisasi sebelum manajemen mengambil tindakan untuk mempengaruhi tingkat keterjadian maupun dampak risiko tersebut dikenal dengan istilah risiko inheren (*inherent risk*). Sedangkan, risiko yang masih ada setelah manajemen menetapkan dan menerapkan respon atas suatu risiko, disebut sebagai risiko residual (*residual risk*). Tingkat risiko residual harus berada pada level yang dapat diterima oleh manajemen (*risk appetite*).

Manajemen menilai risiko melalui dua perspektif, yaitu tingkat keterjadian (*likelihood*) dan dampak *(impact*). Tingkat keterjadian adalah kemungkinan suatu kejadian/peristiwa muncul, sedangkan dampak merupakan efek yang ditimbulkan oleh kejadian/peristiwa tersebut. Organisasi akan menyusun dan memutakhirkan register risiko (*risk register*), yaitu sebuah daftar atas semua risiko signifikan yang mungkin berdampak pada kemampuan organisasi untuk mencapai tujuannya.

Dalam *the Three Lines of Defense in Effective Risk Management and Control*, IIA (2013) menguraikan sebuah model yang terdiri dari:

1. Lini pertahanan pertama yang meliputi manajer operasional sebagai pemilik kegiatan sekaligus pengelola risiko;
2. Lini pertahanan kedua yang meliputi fungsi yang mengawasi risiko, seperti fungsi manajemen risiko atau fungsi ketaatan; dan
3. Lini pertahanan ketiga yaitu fungsi audit intern yang memberikan keyakinan terhadap efektivitas tata kelola, manajemen risiko dan pengendalian.

Berdasarkan model tersebut, peran utama APIP sebagai lini pertahanan ketiga terkait manajemen risiko adalah menilai efektivitas manajemen risiko yang diterapkan lini pertahanan pertama, yaitu manajemen organisasi. Lebih lanjut, IIA (2009) merumuskan peran utama APIP dalam manajemen risiko yang meliputi:

1. Melakukan kegiatan penjaminan atas proses manajemen risiko;
2. Melakukan kegiatan penjaminan bahwa risiko telah dievaluasi dengan benar;
3. Mengevaluasi proses manajemen risiko;
4. Mengevaluasi pelaporan risiko utama;
5. Mereviu pengelolaan risiko utama.

## B. PENGAWASAN INTERN BERBASIS RISIKO

Pengertian pengawasan intern berbasis risiko (*risk-based internal auditing*) menurut *The Institute of Internal Auditors*/IIA adalah metodologi yang menghubungkan pengawasan intern dengan kerangka kerja manajemen risiko suatu organisasi (Chartered IIA, 2014). Pengawasan intern berbasis risiko tersebut memungkinkan APIP Daerah untuk memberikan keyakinan memadai bahwa proses manajemen risiko telah mengelola risiko secara efektif berdasarkan selera risiko atau tingkat risiko yang dapat diterima suatu organisasi.

Menurut Chartered IIA (2014), pengawasan intern berbasis risiko bukanlah tentang kegiatan pengawasan terhadap risiko melainkan kegiatan pengawasan terhadap manajemen risiko. Pengawasan intern berbasis risiko fokus pada dua hal, yaitu (i) respon terhadap masing-masing risiko; dan (ii) proses manajemen risiko yang digunakan untuk menilai, merespon, memantau respon, dan melaporkan risiko kepada Pucuk Pimpinan.

Pendekatan yang diterapkan manajemen Pemerintah Daerah dalam menilai risiko dapat dimanfaatkan oleh APIP Daerah dalam perencanaan pengawasan intern berbasis risiko. Perencanaan pengawasan intern berbasis risiko disusun berdasarkan register risiko Pemerintah Daerah dan perencanaan tersebut memfasilitasi perbaikan kerangka kerja manajemen risiko yang diterapkan di suatu Pemerintah Daerah.

## III. TAHAPAN PERENCANAAN PENGAWASAN INTERN BERBASIS RISIKO

Tahapan dalam penyusunan perencanaan pengawasan intern berbasis risiko dapat dibagi dalam lima tahapan sebagaimana diilustrasikan dalam Gambar 1. Kelima tahapan tersebut meliputi penyusunan Peta Auditan (*audit universe*), penilaian tingkat kematangan manajemen risiko, penentuan risiko utama, penyusunan perencanaan pengawasan intern, dan penyampaian informasi ke Pimpinan Pemerintah Daerah.


Gambar 1 – Tahapan Perencanaan pengawasan intern berbasis Risiko
Sumber: Data Olah Penulis

### A. PENYUSUNAN PETA AUDITAN

Peta Auditan merupakan titik awal dalam menyusun perencanaan pengawasan. *Internal Audit Community of Practice* (IA CoP, 2014) mendefinisikan Peta Auditan sebagai semua obyek audit yang dapat dilakukan audit intern atau dapat dimasukkan dalam ruang lingkup tugas audit intern (*auditable unit*). Tahapan penyusunan Peta Auditan dimulai dari pemahaman atas proses bisnis Pemerintah Daerah. Pemahaman tersebut diperlukan untuk memudahkan pengkategorian yang digunakan APIP Daerah dalam menyusun Peta Auditan dan memastikan obyek audit yang dimasukkan ke dalam Peta Auditan masih relevan.

Dalam konteks Indonesia, tidak terdapat persyaratan dalam Standar Audit maupun peraturan perundang-undangan yang mengatur pendekatan APIP Daerah dalam menyusun Peta Auditan. IIA *Government Survey* memberikan contoh pengkategorian obyek audit dalam Peta Auditan berdasarkan departemen, proses, unit organisasi/lokasi, program, kegiatan, jenis layanan dan portofolio risiko (IA CoP, 2014). Selanjutnya, dalam

menyusun Peta Auditan, APIP Daerah perlu memperhatikan dan mempertimbangkan beberapa informasi antara lain:

1. Tujuan strategis organisasi;
2. Proses bisnis organisasi dan struktur organisasi;
3. Kegiatan utama dari organisasi;
4. Lokasi dari unit-unit kerja organisasi;
5. Profil risiko organisasi dan selera;
6. Hasil reviu atas pengendalian internal dan manajemen risiko organisasi;
7. Sumber daya dan kemampuan tim audit intern;
8. Regulasi terkait; dan
9. Jasa penjaminan dari pihak eksternal (Chartered IIA, 2018).

## B. PENILAIAN TINGKAT KEMATANGAN MANAJEMEN RISIKO

Kematangan Manajemen Risiko (*risk maturity*) adalah sejauhmana pendekatan manajemen risiko diadopsi dan diterapkan oleh manajemen di seluruh tingkatan organisasi dalam mengidentifikasi, menilai, merespon, dan melaporkan risiko (IIA, 2009). Penilaian atas tingkat kematangan manajemen risiko yang dimiliki organisasi *(risk maturity assessment)* menjadi rujukan bagi tahap penentuan risiko utama yang dihadapi oleh manajemen yang akan menjadi obyek pengawasan.

Hal-hal yang perlu dilakukan oleh APIP Daerah dalam menilai tingkat kematangan manajemen risiko antara lain:

1. Menggali tingkat pemahaman pemahaman jajaran manajemen akan manajemen risiko dan proses-proses apa saja yang telah dilakukan dalam rangka membangun manajemen risiko organisasi selama ini.
2. Mengumpulkan berbagai informasi dan dokumen yang terkait dengan manajemen risiko, seperti tujuan organisasi, bagaimana risiko dianalisis dari sisi dampak maupun keterjadian, proses penilaian risiko, selera risiko organisasi, bagaimana manajemen mempertimbangkan dan memandang risiko dalam penentuan keputusan, dan register risiko.
3. Menyimpulkan tingkat kematangan manajemen risiko. Berdasarkan informasi dan dokumen yang diperoleh, audit intern menentukan tingkat kematangan risiko yaitu *risk naive, risk aware, risk defined, risk managed,* dan *risk enabled*. Penjelasan tingkat masing-masing tingkat kematangan disajikan pada tabel berikut:

| No | Tingkat Kematangan | Penjelasan Singkat |
|---|---|---|
| 1 | Risk Naive (Level 1) | Organisasi dengan tingkat kematangan manajemen risiko risk naive belum memiliki pendekatan formal dalam menerapkan manajemen risiko. |
| 2 | Risk Aware (Level 2) | Organisasi dengan tingkat kematangan manajemen risiko risk aware memiliki karakteristik pendekatan manajemen risiko yang masih silo. |
| 3 | Risk Defined (Level 3) | Organisasi yang risk defined telah memiliki strategi dan kebijakan terkait manajemen risiko serta telah dikomunikasikan, selain itu manajemen organisasi juga telah menetapkan selera risiko. |
| 4 | Risk Managed (Level 4) | Organisasi dengan status risk managed telah menggunakan pendekatan secara menyeluruh (enterprise approach) dalam mengembangkan manajemen risiko. Organisasi juga telah mengkomunikasikan penerapan manajemen risiko |
| 5 | Risk Enabled (Level 5) | Organisasi dengan tingkat kematangan manajemen risiko risk optimized memiliki karakteristik utama yaitu manajemen risiko dan pengendalian internal telah sepenuhnya menyatu pada kegiatan operasional organisasi |

Tabel 1 – Tingkat Kematangan Manajemen Risiko
Sumber: Diolah dari Chartered IIA, 2014. *Risk Based Internal Auditing. Appendix A – Assessing the organisation's risk maturity.*

Dalam menilai tingkat kematangan manajamen risiko, APIP Daerah dapat menggunakan pendekatan yang disusun oleh Chartered IIA (2014) sebagaimana disajikan dalam Lampiran 1. Alternatif lain sebagai langkah awal penerapan PPBR, dalam penilaian Maturitas Manajemen Risiko, APIP Daerah dapat mengadopsi Skor Maturitas SPIP.

Tingkat maturitas penyelenggaraan SPIP merupakan kerangka kerja yang memuat karakteristik dasar yang menunjukkan tingkat kematangan penyelenggaraan SPIP yang terstruktur dan berkelanjutan (BPKP, 2016). APIP Daerah dapat mengadopsi skor maturitas SPIP yang telah diterapkan oleh organisasi yang bersangkutan. Namun perlu dipahami bahwa dalam pengambilan skor maturitas ini, APIP Daerah harus berfokus kepada skor maturitas SPIP pada setiap unsur secara menyeluruh (kelima unsur) bukan hanya pada elemen 2 yang terkait dengan penilaian risiko. Dari skor tersebut, audit internal dapat mengetahui skor kematangan penilaian risiko dari organisasi. APIP Daerah dapat menggunakan hasil penilaian risiko dan rencana tindak pengendalian dalam SPIP apabila skor maturitas SPIP berada pada level 4 atau 5 dimana semua unsur harus memiliki skor minimal 4.

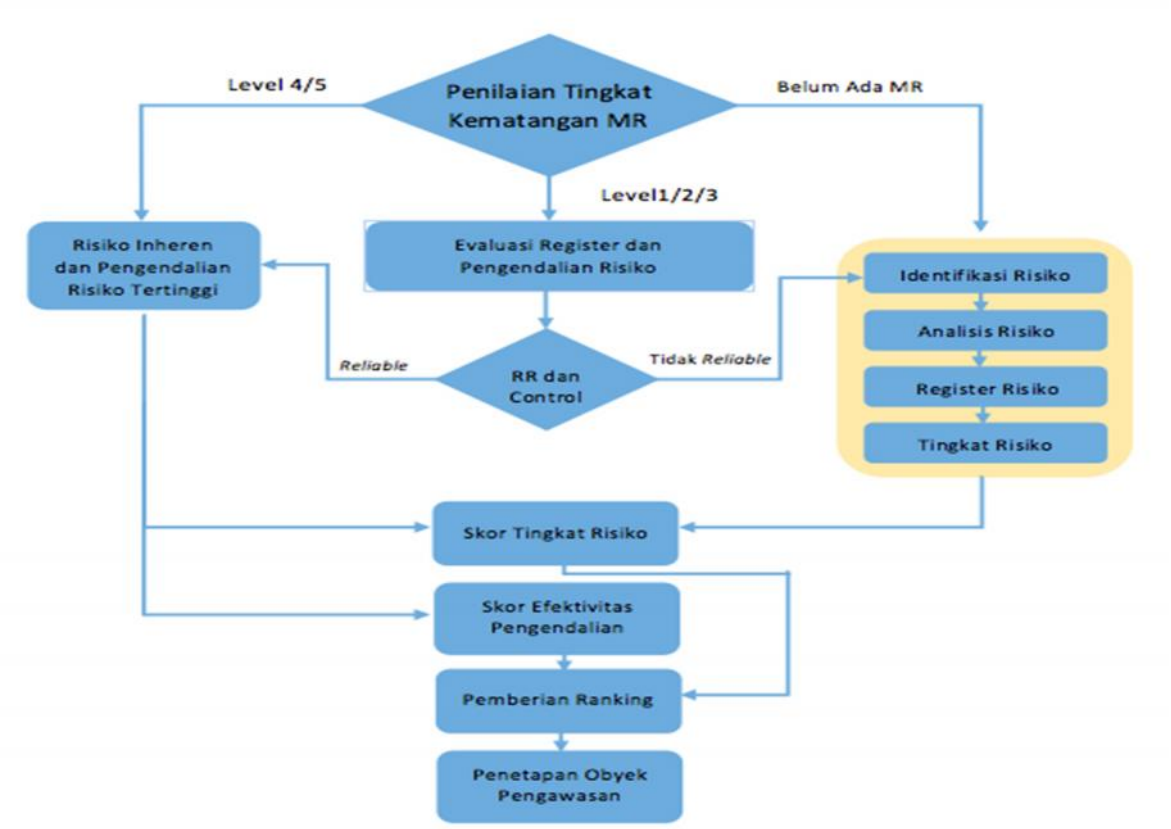
Perencanaan pengawasan intern berbasis risiko dapat diterapkan secara optimal pada kondisi *risk enabled* dan *risk managed* (Chartered IIA, 2014). Terhadap organisasi dengan tingkat kematangan manajemen risiko di bawah kedua level *risk enabled* dan *risk managed* tersebut, APIP Daerah mengevaluasi proses perumusan untuk menilai keakuratan register risiko sebelum digunakan dalam perencanaan pengawasan. Selain itu APIP Daerah juga melakukan kegiatan pengawasan yang bersifat layanan konsultansi

untuk mendorong manajemen melakukan identifikasi dan penilaian risiko serta menyusun register risiko sehingga register risiko sebagai hasil penilaian risiko organisasi tersebut dapat digunakan dalam penyusunan perencanaan pengawasan.

## C. PENENTUAN RISIKO UTAMA

Setelah APIP Daerah menentukan atau memperoleh informasi tingkat kematangan manajemen risiko (atau tingkat kematangan SPIP), maka tahap berikutnya adalah menentukan dasar yang digunakan untuk menyusun prioritas risiko utama organisasi. Langkah ini merupakan langkah yang sangat krusial dalam pembuatan perencanaan pengawasan intern berbasis risiko.

Tingkat kematangan manajemen risiko akan menentukan data mana yang akan digunakan dalam penentuan prioritas risiko utama organisasi. Hubungan tingkat kematangan manajemen risiko dengan penentuan prioritas risiko utama organisasi disajikan pada Gambar 2.




Gambar 2 – Tingkat Kematangan Manajemen Risiko dan
Penentuan Prioritas Risiko Utama Organisasi

APIP Daerah menggunakan register risiko yang disusun oleh manajemen jika tingkat kematangan manajemen risiko organisasi berada pada *risk managed* (Level 4) atau *risk enabled* (Level 5). Apabila organisasi belum memiliki kerangka manajemen risiko dan

register risiko, APIP Daerah melakukan kegiatan pengawasan yang bersifat layanan konsultansi dengan bertindak sebagai fasilitator untuk mendorong manajemen melakukan identifikasi dan penilaian risiko serta menyusun register risiko untuk meningkatkan tingkat kematangan manajemen risiko organisasi sehingga register risiko sebagai hasil penilaian risiko organisasi tersebut dapat digunakan dalam penyusunan perencanaan pengawasan.

Selanjutnya, jika tingkat kematangan manajemen risiko organisasi sudah berada pada level 1 (*risk naive*), level 2 (*risk aware*), atau level 3 (*risk defined*), APIP Daerah mengevaluasi tingkat keandalan rencana tindak pengendalian/register risiko. APIP Daerah harus memastikan bahwa semua risiko telah diindentifikasi, penilaian dampak dan keterjadian telah dilakukan dengan memadai, dan pengendalian yang memadai telah diterapkan. Bila manajemen risiko dianggap sudah andal, APIP Daerah dapat menggunakan informasi tingkat risiko dalam register risiko untuk penentuan prioritas dalam perencanaan pengawasan. Namun jika belum andal, APIP Daerah harus melakukan fasilitasi penerapan manajemen risiko.

Dalam menentukan risiko utama organisasi, APIP Daerah dapat menjalankan langkah-langkah sebagai berikut:

**1. Memperoleh Register Risiko**

APIP Daerah menggunakan register risiko yang dibuat secara mandiri oleh manajemen atau hasil fasilitasi auditor intern untuk menyusun perencanaan audit internal. Register risiko tersebut telah mencakup hasil identifikasi risiko dan penanganan risiko di seluruh unit/kegiatan/proyek dan satuan kerja lain di organisasi.

Untuk menentukan signifikasi dari risiko, internal auditor dapat menggunakan dua variabel yang sering digunakan dalam pembuatan register risiko, yaitu dampak dan tingkat keterjadian dari risiko tersebut. Data ini juga dapat diperoleh dari register risiko yang disusun oleh manajemen.

APIP harus lebih fokus ke area yang memiliki risiko inheren tinggi (Griffiths, 2005). Langkah ini sangat penting untuk APIP Daerah agar sumber daya yang dimiliki dapat dialokasikan secara efektif untuk area yang memiliki paparan risiko tertinggi yang akan berdampak pada tujuan organisasi serta risiko yang ditangani dengan tidak baik oleh organisasi. Dengan demikian, APIP Daerah akan dapat mengurangi paparan risiko yang dihadapi oleh Pemerintah Daerah. Selain itu APIP Daerah perlu mempertimbangkan efektivitas pengendalian yang diterapkan oleh manajemen jika kondisi penerapan manajemen risiko telah berada pada level 4 ataupun 5.

## 2. Penentuan Prioritas Risiko untuk Menjadi Target Pengawasan

Dalam penentuan prioritas risiko untuk menjadi target pengawasan, auditor internal memeringkatkan/mengurutkan risiko berdasarkan pertimbangan sebagai berikut (Chartered IIA, 2014; IIA, 2017):

a. Skor risiko inheren

   Risiko inheren yang paling signifikan harus menjadi fokus dari APIP Daerah. Risiko inheren digunakan karena pengawasan yang akan dilakukan oleh APIP Daerah akan mengevaluasi efektivitas dari pengendalian yang ada. Besar kecilnya risiko inheren merupakan salah satu kriteria utama dalam penentuan prioritas risiko.

b. Efektivitas pengendalian dalam menurunkan risiko inheren.

   Semakin manajemen memiliki keyakinan yang tinggi atas efektivitas suatu pengendalian yang diterapkannya untuk menurunkan risiko, semakin tinggi prioritasnya bagi APIP Daerah untuk masuk perencanaan pengawasan. APIP Daerah harus melihat skor pengendalian (risiko inheren dikurangi risiko residual) yang ada, sehingga semakin besar skor pengendalian *(control)* maka semakin tinggi prioritasnya untuk menjadi obyek pengawasan.

c. Jasa penjaminan lain yang telah ada.

   Risiko yang telah menjadi obyek pengawasan oleh pihak pemberi penjaminan lainnya maka semakin rendah prioritasnya. Bila dirasa jasa penjaminan yang telah ada mampu untuk menjamin bahwa pengendalian telah berjalan secara efektif, maka audit internal bisa mengabaikan risiko tersebut.

d. Permintaan dari *stakeholder* yang terkait.

   Kategori risiko yang menurut Pimpinan Daerah perlu dilakukan *assurance* (penjaminan) yang objektif setiap periode maka makin tinggi prioritasnya.

Jika jumlah *auditable unit* dan risiko di suatu Pemerintah Daerah terlalu banyak, APIP Daerah dapat menggunakan faktor risiko untuk menyeleksi/meranking *auditable unit* yang akan menjadi obyek pengawasan. Faktor risiko dapat diartikan sebagai istilah yang digunakan untuk menggambarkan faktor-faktor umum yang dapat mengindikasikan tingkat risiko yang lebih tinggi dan/atau mempengaruhi prioritas pada suatu bagian dari Peta Auditan (IA CoP, 2014). APIP Daerah dapat menggunakan faktor risiko yang sesuai dengan kondisi dan kebutuhan dari APIP Daerah. Faktor risiko yang paling umum digunakan antara lain materialitas keuangan, kompleksitas kegiatan, lingkungan pengendalian, sensitivitas terhadap reputasi, risiko inheren, tingkat perubahan di organisasi auditan, tingkat kepercayaan terhadap manajemen, potensi kecurangan, waktu terakhir kali diaudit, dan volume transaksi (IA CoP, 2014).

Berdasarkan rangking tersebut, kemudian memilih risiko mana yang akan dikaitkan dengan unit layak audit (*auditable unit*) dalam tahun ini, dan risiko mana yang akan dikaitkan dengan unit layak audit lebih dari setahun sekali. APIP Daerah harus menetapkan kebijakan untuk menetapkan risiko mana yang layak untuk diaudit ataupun seberapa sering audit harus dilakukan. Tidak harus seluruh risiko yang nilainya berada di atas selera risiko diaudit tiap tahun. Contoh kebijakan tersebut dapat disajikan pada Gambar 3.


Gambar 3 – Contoh Kebijakan Risiko *Auditable Unit*

Berdasarkan Gambar 3, terlihat bahwa risiko yang memiliki dampak yang berada pada level sangat signifikan, signifikan dan moderat (level 3 sampai dengan level 5) dan kemungkinan terjadinya cukup tinggi (level 3 sampai dengan level 5) yang diaudit setiap tahun. Sedangkan untuk risiko yang dibawahnya yang memiliki dampak ataupun kemungkinan keterjadian yang lebih kecil, APIP Daerah dapat menetapkan kebijakan untuk mengaudit setiap dua, tiga, atau empat tahun sekali.

## D. PENYUSUNAN PERENCANAAN PENGAWASAN INTERN

Setelah ditentukan *auditable unit* berdasarkan hasil penentuan risiko utama pada langkah sebelumnya, langkah selanjutnya yang ditempuh APIP Daerah adalah menyusun dokumen perencanaan pengawasan. Dokumen tersebut memuat informasi mengenai rencana pengawasan di tahun tahun selanjutnya, antara lain berisi:

- Nama obyek/unit yang akan diaudit.
- Skor risiko inheren.
- Kapan dilaksanakan.

- Sumber daya yang dibutuhkan.
- Berapa lama akan dilaksanakan.
- Siapa personil tim yang akan melaksanakan dan sebagainya.

Penentuan rencana dan jadwal pengawasan tahunan didasarkan pada penyesuaian antara urutan *auditable unit* dengan sumber daya yang tersedia. Selain itu, APIP Daerah juga menyertakan kegiatan pengawasan yang bersifat *mandatory* bagi APIP Daerah tersebut, permintaan Pimpinan Pemerintah Daerah, dan pengaduan masyarakat dalam menyusun dokumen perencanaan pengawasan (IIA, 2017; Moeller, 2005). Usulan perencanaan yang telah selesai disusun, selanjutnya disampaikan kepada Pimpinan APIP Daerah.

Dalam tahap ini, APIP Daerah juga harus membuat analisis terkait risiko dan dampak apabila terdapat rencana pengawasan yang tidak dapat dilaksanakan oleh APIP Daerah maupun apabila ada keterbatasan sumber daya baik itu anggaran maupun sumber daya manusia.

## E. PENYAMPAIAN INFORMASI KE PIMPINAN PEMERINTAH DAERAH

Tahap terakhir dari penyusunan perencanaan pengawasan intern berbasis risiko adalah penyampaian informasi ke Pimpinan Pemerintah Daerah. APIP Daerah harus mengkomunikasikan informasi yang terkait dengan penyusunan perencanaan pengawasan intern berbasis risiko ini. Adapun informasi yang disampaikan antara lain:

1. Peta Auditan;
2. Dokumen Matriks Risiko dan Pengendaliannya;
3. Dokumen Perencanaan pengawasan intern berbasis Risiko;
4. Analisis atas risiko dan dampak adanya keterbatasan anggaran dan sumber daya manusia; dan
5. Analisis atas risiko dan dampak tidak dilaksanakan rencana pengawasan atas risiko yang telah diindentifikasi (IIA, 2017).

**Lampiran 1**
**Penilaian Maturitas Manajemen Risiko**

| | Risk Naive | Risk Aware | Risk Defined | Risk Managed | Risk Enabled | Contoh Pengujian |
|---|---|---|---|---|---|---|
| Karakteristik Utama | | | | | | |
| | Tidak terdapat pendekatan formal dalam manajemen risiko | Pendekatan manajemen risiko yang tidak terintegrasi (silo) | Strategi dan kebijakan telah ada dan dikomunikasikan. Selera risiko telah ditetapkan | Pendekatan secara menyeluruh (enterprise approach) dalam mengembangkan manajemen risiko. Organisasi juga telah mengkomunikasikan penerapan manajemen risiko. | Manajemen risiko dan pengendalian internal telah sepenuhnya menyatu pada kegiatan operasional organisasi | |
| Proses | | | | | | |
| Tujuan Organisasi telah ditetapkan | Mungkin | Ya – namun terdapat kemungkinan pendekatan yang diterapkan tidak konsisten | Ya | Ya | Ya | Cek apakah tujuan organisasi telah ditetapkan dan dikomunikasikan kepada seluruh staf. Cek apakah tujuan dan target lainnya telah sesuai dengan tujuan organisasi. |
| Manajemen telah dilatih untuk memahami risiko dan tanggung jawab manajemen terkait risiko | Tidak | Pelatihan masih terbatas | Ya | Ya | Ya | Wawancara manajer untuk mengkonfirmasi pemahaman mereka terkait risiko dan sejauhmana manajer telah mengelola risiko |
| Sistem skor dalam menilai risiko telah ditetapkan | Tidak | Kemungkinan besar tidak ada sistem skor. Jika terdapat system skor, pendekatannya belum konsisten | Ya | Ya | Ya | Cek apakah sistem skor telah disetujui, dikomunikasikan dan digunakan |

| | Risk Naive | Risk Aware | Risk Defined | Risk Managed | Risk Enabled | Contoh Pengujian |
|---|---|---|---|---|---|---|
| Selera risiko organisasi telah ditetapkan terkait dengan sistem skor | Tidak | Tidak | Ya | Ya | Ya | Cek dokumen yang berisi selera risiko yang telah disetujui oleh Pimpinan. Yakini bahwa selera risiko telah dikomunikasikan dan telah konsisten dengan sistem skor. |
| Proses untuk menentukan risiko telah ditetapkan dan dilaksanakan | Tidak | Kemungkin besar tidak | Ya, namun mungkin belum diterapkan di seluruh tingkatan organisasi | Ya | Ya | Uji apakah proses telah memadai dalam mengidentifikasi semua risiko. Cek apakah proses tersebut digunakan. |
| Seluruh risiko telah dikumpulkan dalam satu daftar register risiko dan dikaitkan dengan masing-masing pemilik risiko (manajer operasional) | Tidak | Daftar register risiko belum lengkap | Ya, namun mungkin belum diterapkan di seluruh tingkatan organisasi | Ya | Ya | Uji register risiko, pastikan bahwa register risiko telah lengkap, direviu secara berkala, dinilai dan digunakan untuk mengelola risiko. Risiko telah dialokasikan kepada para pemilik risiko (manajer operasional) |
| Semua risiko telah dinilai merujuk pada sistem skor yang telah ditetapkan | Tidak | Daftar register risiko belum lengkap | Ya, namun mungkin belum diterapkan di seluruh tingkatan organisasi | Ya | Ya | Cek apakah sistem skor yang digunakan dalam penilaian risiko telah konsisten dengan kebijakan yang ada |
| Respon terhadap risiko telah ditetapkan dan dilaksanakan | Tidak | Beberapa respon telah diidentifikasi | Ya, namun mungkin belum diterapkan di seluruh tingkatan organisasi | Ya | Ya | Uji register risiko untuk memastikan respon yang tepat telah diidentifikasi |
| Manajemen telah merancang sistem untuk memantau pelaksanaan yang tepat atas proses kunci, respon dan rencana tindak (monitoring controls) | Tidak | Beberapa monitoring controls telah ada | Ya, namun mungkin belum diterapkan di seluruh tingkatan organisasi | Ya | Ya | Uji monitoring controls dan pastikan manajemen mengetahui jika terdapat respon atau |

| | Risk Naive | Risk Aware | Risk Defined | Risk Managed | Risk Enabled | Contoh Pengujian |
|---|---|---|---|---|---|---|
| | | | | | | proses yang tidak berjalan atau terdapat rencana tindak yang tidak diimplementasikan |
| Risiko telah direviu oleh organisasi secara berkala | Tidak | Beberapa risiko telah direviu namun tidak secara rutin | Reviu secara berkala (tahunan) | Reviu secara berkala (triwulanan) | Reviu secara berkala (triwulanan) | Buktikan bahwa proses reviu telah dilakukan secara berkala |
| Manajemen melaporkan risiko kepada Pimpinan ketika respon terhadap risiko tidak mampu menurunkan tingkat risiko ke dalam risk appetite | Tidak | Tidak | Ya, namun kemungkinan bukan merupakan proses yang formal | Ya | Ya | Cek apakah Pimpinan telah secara formal diinformasikan jika terdapat risiko yang berada di atas selera risiko |
| Risiko atas proyek/program/kegiatan baru yang signifikan telah secara rutin dinilai | Tidak | Tidak | Hampir sebagian besar | Semua | Semua | Uji apakah terdapat analisis risiko dalam dokumen perencanaan proyek/program/kegiatan |
| Tanggung jawab untuk penentuan, penilaian dan pengelolaan risiko telah dicantumkan dalam job description | Tidak | Tidak | Terbatas | Hampir semua | Ya | Uji job description. |
| Manajer menyediakan assurance atas efektivitas manajemen risiko yang mereka jalankan | Tidak | Tidak | Tidak | Beberapa manajer | Ya | Uji assurance yang disediakan. Terhadap risiko utama, cek apakah pengendalian dan sistem manajemen pemantauan telah berjalan. |
| Kinerja manajemen dalam mengelola risiko dinilai | Tidak | Tidak | Tidak | Beberapa manajer | Ya | Lakukan uji petik, apakah kinerja manajemen risiko juga menjadi dasar dalam menilai kinerja manajemen |

Sumber: Diolah Diolah dari Chartered IIA, 2014. *Risk Based Internal Auditing. Appendix A – Assessing the organisation's risk maturity.*

## DAFTAR TABEL



## DAFTAR GAMBAR

## REFERENSI


Asosiasi Auditor Intern Pemerintah Indonesia (AAIPI). 2013. *Standar Audit Intern Pemerintah Indonesia.*

Badan Pengawasan Keuangan dan Pembangunan. 2016. *Peraturan Kepala BPKP Nomor 4 Tahun 2016 tentang Pedoman Penilaian dan Strategi Peningkatan Maturitas Sistem Pengendalian Intern Pemerintah.*

Chartered Institute of Internal Auditors. 2014. *Risk Based Internal Auditing.* *https://www.iia.org.uk/resources/risk-management/risk-based-internal-auditing?downloadPdf=true*

Chartered Institute of Internal Auditors. 2018. Maret. *Audit Universe.* *https://www.iia.org.uk/audituniverse?downloadPdf=true*

Griffiths, Phil. 2005. *Risk-Based Auditing.* England: Gower Publishing Limited.

Moeller, Robert R. 2005. *Brink's Modern Internal Auditing* (6th Edition). New Jersey, USA: John Wiley & Sons, Inc.

The Institute of Internal Auditors. 2009. *IIA Position Paper: The Role of Internal Auditing in Enterprise-Wide Risk Management.* https://global.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Role%20of%20Internal%20Auditing%20in%20Enterprise%20Risk%20Management.pdf

The Institute of Internal Auditors. 2013. *The Three Lines of Defense in Effective Risk Management and Control*. https://global.theiia.org/standards-guidance/recommended-guidance/Pages/The-Three-Lines-of-Defense-in-Effective-Risk-Management-and-Control.aspx

The Institute of Internal Auditors. 2017*. Implementation Guides.*

**TIM PERUMUS**

**Penanggung Jawab:**

Drs. Gatot Darmasto, Ak, MBA, CRMA, CA, CFrA, QA

**Wakil Penanggung Jawab:**

Adi Gemawan, Ak, MM, CA, CFrA, QIA, AAP

**Tim Penyusun:**

Rini Wartini

Gunawan

Edi Sunardi

Ivan Dwi Jatmiko

Amirullah

Fitria Nur Hidayah

BADAN PENGAWASAN KEUANGAN DAN PEMBANGUNAN
DEPUTI BIDANG PENGAWASAN PENYELENGGARAAN KEUANGAN DAERAH
Alamat: Kantor Pusat BPKP Lantai 10
Jalan Pramuka Nomor 33 Jakarta Timur 13120
Telepon 021-85910031 ext. 1030
E-mail: rendalpkapip@gmail.com