



GRC MATURITY INDEX

**MENGUKUR TINGKAT KEMATANGAN GOVERNANCE, RISK MANAGEMENT
& COMPLIANCE MENUJU KINERJA BERPRINSIP DAN BERKELANJUTAN**

APA ITU PENILAIAN MATURITAS GRC?

Penilaian Maturitas GRC atau GRC Maturity Index (GRC-MI) dapat membantu organisasi mengetahui posisi kematangan penerapan GRC, mengidentifikasi kesenjangan prioritas, dan menyusun peta jalan peningkatan yang terukur untuk mendukung Kinerja Berprinsip serta menghasilkan dan menjaga nilai Produce and Preserve Value.

GRC-MI adalah proses penilaian yang dilakukan secara sistematis untuk mengukur seberapa matang/efektif desain, penerapan, pemantauan, dan pembelajaran dalam penerapan GRC di organisasi. Pertimbangan utamanya mencakup:

1. Kecukupan kebijakan dan kerangka.
2. Kejelasan struktur, peran, dan akuntabilitas.
3. Konsistensi implementasi.
4. Keterhubungan antar unit dan antar fungsi.
5. Integrasi dengan strategi dan proses bisnis.
6. Efektivitas pengendalian dan asuran.
7. Pemanfaatan data dan teknologi.
8. Kualitas budaya dan kompetensi.
9. Implikasi GRC terhadap kinerja dan proposisi nilai.

KEUNGGULAN PROGRAM

Penilaian maturitas GRC dapat membantu organisasi, khususnya keberadaan manajemen dalam menjawab empat pertanyaan utama, yakni:

1. Di mana posisi tingkat kematangan GRC organisasi saat ini?
2. Elemen apa yang telah kuat dan elemen apa yang masih lemah?
3. Kesenjangan mana yang paling berdampak terhadap tujuan dan nilai organisasi?
4. Program peningkatan apa yang harus diprioritaskan?

PRINSIP PENILAIAN MATURITAS GRC

Penilaian dilakukan berdasarkan Empat Lapisan Pembuktian, yakni:

1. Design Adequacy

Apakah kebijakan, struktur, proses, metodologi, dan pengendalian telah dirancang secara memadai?

2. Implementation Consistency

Apakah desain tersebut benar-benar diterapkan secara konsisten pada unit dan proses bisnis?

3. Operating Effectiveness

Apakah penerapan tersebut efektif mencegah, mendeteksi, merespons, dan memperbaiki permasalahan?

4. Performance and Value Impact

Apakah GRC berkontribusi terhadap pencapaian sasaran, kualitas keputusan, ketahanan, integritas, kepatuhan, dan nilai organisasi?

ALASAN UTAMA MENGAPA PENTING MENILAI MATURITAS GRC

Penerapan Tata Kelola, manajemen kinerja, risiko, dan kepatuhan, termasuk keberadaan fungsi asuran pada umumnya cenderung dijalankan secara silo. Selain itu, strategi, risiko, kepatuhan, dan pengendalian dikelola dalam sistem yang berbeda. Hal ini dapat tercermin dari:

1. Adanya tumpang tindih atau kekosongan peran antar unit.
2. Kebijakan tersedia, namun belum diterapkan secara konsisten, terkoneksi dan terintegrasi.
3. Risiko dan isu kepatuhan belum menjadi pertimbangan utama dalam pengambilan keputusan.
4. Pelaporan masih berorientasi pada aktivitas, bukan efektivitas dan dampak.
5. Data GRC tersebar, belum konsisten, atau belum menghasilkan peringatan dini.
6. Temuan audit dan insiden yang sama terus berulang.
7. Program peningkatan kinerja dilakukan tanpa prioritas dan peta jalan yang jelas.
8. Skor maturitas belum sepenuhnya didukung oleh bukti implementasi.
9. Investasi teknologi GRC belum memberikan manfaat yang terukur.

Atas dasar pertimbangan tersebut, memiliki banyak kebijakan, struktur, aplikasi, laporan risiko, fungsi kepatuhan, dan aktivitas audit belum tentu menunjukkan bahwa GRC telah berjalan efektif.

TINGKAT MATURITAS GRC

Tingkat	Kategori	Karakteristik Umum
Level 1	<i>Initial and Fragmented</i>	Penerapan bersifat reaktif, individual, dan belum terdokumentasi secara memadai.
Level 2	<i>Developing</i>	Kerangka dan praktik mulai dibangun, tetapi belum diterapkan secara konsisten.
Level 3	<i>Defined and Consistent</i>	Kebijakan, proses, peran, dan pelaporan telah ditetapkan dan dijalankan secara relatif konsisten.
Level 4	<i>Integrated and Measured</i>	GRC telah terintegrasi dengan strategi, proses bisnis, pengambilan keputusan, serta diukur efektivitasnya.
Level 5	<i>Optimizing</i>	GRC bersifat prediktif, berbasis data, adaptif, terus diperbaiki, dan terbukti menghasilkan serta menjaga nilai.



METODOLOGI, STANDAR, DAN RUJUKAN PENILAIAN

Penilaian Maturitas GRC menggunakan pendekatan multi-framework dan evidence-based assessment. Penilaian tidak hanya menggunakan satu daftar periksa, tetapi menyelaraskan berbagai standar dan praktik yang relevan dengan karakteristik organisasi, yakni:

1. Kerangka GRC Utama:

OCEG GRC Capability Model 3.5 yang menggunakan siklus:

- **Learn:** memahami konteks, budaya, tujuan, pemangku kepentingan, peluang, ancaman, dan kewajiban.
- **Align:** menyelaraskan strategi, tujuan, risiko, kepatuhan, sumber daya, dan kriteria pengambilan keputusan.
- **Perform:** melaksanakan tindakan, pengendalian, komunikasi, dan pengelolaan GRC secara terintegrasi.
- **Review:** memantau, memberikan asuran, mengevaluasi efektivitas, dan melakukan perbaikan berkelanjutan.

2. Standar Internasional:

- ISO 37000 — Governance of Organizations, sebagai pedoman tata kelola organisasi dan pengambilan keputusan yang berorientasi pada tujuan serta keberlanjutan jangka panjang.
- ISO 31000:2018 — Risk Management Guidelines, untuk menilai prinsip, kerangka, proses, integrasi, pemantauan, dan perbaikan manajemen risiko
- ISO 37301:2021 — Compliance Management Systems, untuk menilai desain, penerapan, evaluasi, pemeliharaan, dan peningkatan sistem manajemen kepatuhan.
- ISO 30401:2018 beserta amendemen yang berlaku — Knowledge Management Systems, untuk menilai pengelolaan pengetahuan sebagai penghubung antara manusia, proses, dan teknologi.
- Standar lain yang relevan, seperti ISO 22301, ISO/IEC 27001, ISO 37001, ISO 14001, dan standar sektoral sesuai kebutuhan organisasi.

3. Kerangka Pengendalian dan Assurance:

- COSO Enterprise Risk Management—Integrating with Strategy and Performance, untuk menilai integrasi risiko dengan strategi, penetapan tujuan, pelaksanaan, dan kinerja.
- COSO Internal Control—Integrated Framework, untuk menilai desain dan efektivitas pengendalian internal.
- The IIA Three Lines Model, untuk menilai pembagian peran governing body, manajemen, fungsi lini kedua, dan internal audit serta koordinasi antar peran tersebut.

4. Regulasi Nasional dan Sektoral

yang disesuaikan dengan bentuk dan sektor organisasi, antara lain:

- Peraturan dan ketentuan Otoritas Jasa Keuangan;
- Ketentuan Bank Indonesia;
- Peraturan kementerian atau lembaga teknis;
- Regulasi sektoral mengenai tata kelola, risiko, kepatuhan, ESG, keamanan informasi, dan perlindungan data;
- Ketentuan internal grup perusahaan; serta
- Kebijakan pemegang saham.

5. Perusahaan dan anak perusahaan dikelola Danantara

rujukan dapat mencakup:

- PER-2/MBU/03/2023 tentang Pedoman Tata Kelola dan Kegiatan Korporasi Signifikan BUMN.
- SK-8/DKU.MBU/12/2023 tentang Petunjuk Teknis Penilaian Indeks Kematangan Risiko, sepanjang relevan dan masih berlaku bagi ruang lingkup perusahaan.

MANFAAT SPESIFIK ATAS PENILAIAN MATURITAS GRC

Bagi Dewan Komisaris atau Dewan Pengawas

- Memperoleh gambaran independen mengenai kualitas pengawasan GRC.
- Mengetahui risiko dan kesenjangan yang memerlukan perhatian khusus.
- Memperkuat dasar pemberian arahan kepada Direksi.
- Memastikan kecukupan sistem assurance dan jalur eskalasi.

Bagi Direksi dan Manajemen Eksekutif

- Mengetahui posisi kematangan GRC secara objektif.
- Menentukan prioritas investasi dan transformasi GRC.
- Memperkuat integrasi GRC dengan strategi, RKAP, dan pengambilan keputusan.
- Mengurangi duplikasi proses, aplikasi, komite, dan pelaporan.
- Memperoleh dasar penyusunan target maturitas dan indikator keberhasilan.

Bagi Fungsi GRC dan Unit Bisnis

- COSO Enterprise Risk Management—Integrating with Strategy and Performance, untuk menilai integrasi risiko dengan strategi, penetapan tujuan, pelaksanaan, dan kinerja.
- COSO Internal Control—Integrated Framework, untuk menilai desain dan efektivitas pengendalian internal.
- The IIA Three Lines Model, untuk menilai pembagian peran governing body, manajemen, fungsi lini kedua, dan internal audit serta koordinasi antar peran tersebut.



Hasil yang Diterima Organisasi

- Laporan tingkat maturitas GRC.
- Skor keseluruhan dan skor per elemen.
- Heatmap kekuatan dan kesenjangan.
- Analisis desain dan efektivitas implementasi.
- Daftar temuan dan akar penyebab.
- Rekomendasi quick wins dan program strategis.
- Peta jalan peningkatan jangka pendek, menengah, dan panjang.
- Target tingkat maturitas dan indikator keberhasilan.
- Executive presentation kepada Direksi dan Dewan Komisaris/Dewan Pengawas.
- Dashboard pemantauan tindak lanjut.





PT LPK MSI Indonesia

Graha 415, Jalan Ciputat Raya.47, RT.1/RW.7, Pondok Pinang,
Kecamatan Kebayoran Lama, Kota Jakarta Selatan,
Daerah Khusus Ibukota Jakarta 12310 T: (+6221) 38805906 (Hotline)
Email: info@msiinstitute.id



Contact Us:

MSI Institute (085811598140)



www.msiinstitute.id



[msi.institute](https://www.instagram.com/msi.institute)



[MSI Institute](https://www.linkedin.com/company/msi-institute)



[MSI Institute](https://www.facebook.com/MSI-Institute)



[msiinstitute](https://open.spotify.com/artist/msiinstitute)