



YAYASAN PRIMA AGUS TEKNIK



# MANAJEMEN RISIKO PERUSAHAAN DAGANG BERBASIS ARTIFICIAL INTELLIGENCE

Konsep, Kerangka, Identifikasi, Analisis, Mitigasi,  
Implementasi, dan Audit



**Sri Wahyuning S.Kom, M.Si**  
UNIVERSITAS STEKOM SEMARANG



# **MANAJEMEN RISIKO PERUSAHAAN DAGANG BERBASIS ARTIFICIAL INTELLIGENCE**

**Konsep, Kerangka, Identifikasi, Analisis, Mitigasi,  
Implementasi, dan Audit**

**Sri Wahyuning, S.Kom., M.Si**



YAYASAN PRIMA AGUS TEKNIK

**PENERBIT :**

**YAYASAN PRIMA AGUS TEKNIK**  
Jl. Majapahit No. 605 Semarang  
Telp. (024) 6723456. Fax. 024-6710144  
Email : [penerbit\\_ypat@stekom.ac.id](mailto:penerbit_ypat@stekom.ac.id)

ISBN 978-634-7695-57-4 (PDF)



9

786347

695574

# **MANAJEMEN RISIKO PERUSAHAAN DAGANG BERBASIS ARTIFICIAL INTELLIGENCE**

Konsep, Kerangka, Identifikasi, Analisis, Mitigasi, Implementasi, dan Audit

**Penulis :**

Sri Wahyuning, S.Kom., M.Si

**ISBN : 978-634-7695-57-4 (PDF)**

**Editor :**

Eni Endaryati, S.Kom, M.Si

**Penyunting :**

Vivi Kumalasari Subroto, S.E, M.Si. Ak.

**Desain Sampul dan Tata Letak :**

Irdha Yunianto, S.Ds., M.Kom

**Penebit :**

Yayasan Prima Agus Teknik Bekerja sama dengan  
Universitas Sains & Teknologi Komputer (Universitas STEKOM)

**Anggota IKAPI No:** 279 / ALB / JTE / 2023

**Redaksi :**

Jl. Majapahit no 605 Semarang

Telp. 08122925000

Fax. 024-6710144

Email : [penerbit\\_ypat@stekom.ac.id](mailto:penerbit_ypat@stekom.ac.id)

**Distributor Tunggal :**

**Universitas STEKOM**

Jl. Majapahit no 605 Semarang

Telp. 08122925000

Fax. 024-6710144

Email : [info@stekom.ac.id](mailto:info@stekom.ac.id)

Hak cipta dilindungi undang-undang

Dilarang memperbanyak karya tulis ini dalam bentuk dan dengan cara  
apapun tanpa ijin dari penulis

## KATA PENGANTAR

Puji syukur ke hadirat Tuhan Yang Maha Esa atas segala rahmat, karunia, dan pertolongan-Nya, sehingga buku yang berjudul ***“Manajemen Risiko Perusahaan Dagang Berbasis Artificial Intelligence”*** ini dapat diselesaikan dengan baik. Buku ini disusun sebagai salah satu referensi untuk memahami perkembangan manajemen risiko pada perusahaan dagang di tengah perubahan lingkungan bisnis yang semakin dinamis, kompleks, dan berbasis teknologi digital.

Perkembangan teknologi digital dan Artificial Intelligence (AI) telah membawa perubahan besar dalam cara perusahaan menjalankan kegiatan bisnis, mengolah data, mengambil keputusan, serta mengidentifikasi dan mengendalikan berbagai bentuk risiko. Perusahaan dagang saat ini tidak hanya menghadapi risiko yang bersumber dari kegiatan operasional, keuangan, pemasaran, dan rantai pasok, tetapi juga menghadapi risiko yang berkaitan dengan data, keamanan siber, privasi, ketergantungan terhadap teknologi, penggunaan algoritma, serta perubahan perilaku pasar. Oleh karena itu, diperlukan pendekatan manajemen risiko yang tidak hanya bersifat reaktif, tetapi juga mampu memanfaatkan data dan teknologi cerdas untuk mendeteksi, menganalisis, memprediksi, serta memitigasi risiko secara lebih efektif.

Buku ini disusun secara sistematis agar pembaca memperoleh pemahaman yang utuh, mulai dari konsep fundamental manajemen risiko perusahaan dagang hingga penerapan sistem manajemen risiko berbasis AI dan proses auditnya. Pembahasan diawali dengan Bab 1, Konsep Dasar Manajemen Risiko dalam Perusahaan Dagang, yang memberikan landasan mengenai pengertian risiko dan karakteristik risiko bisnis dagang. Bab ini membahas berbagai sumber risiko dalam aktivitas perdagangan, perbedaan antara risiko operasional, finansial, dan strategis, serta pentingnya manajemen risiko bagi keberlanjutan usaha dagang. Selain itu, dibahas pula peran teknologi digital dalam mendorong evolusi pengelolaan risiko dari pendekatan konvensional menuju pendekatan yang lebih terintegrasi dan berbasis data.

Selanjutnya, Bab 2, Kerangka Kerja Manajemen Risiko Perusahaan, membahas prinsip-prinsip dasar manajemen risiko korporasi dan pendekatan Enterprise Risk Management (ERM). Pembahasan diarahkan pada bagaimana perusahaan dapat membangun kerangka pengelolaan risiko yang sesuai dengan karakteristik dan skala organisasi. Bab ini juga menguraikan pentingnya integrasi ERM dengan tata kelola perusahaan serta bagaimana kerangka manajemen risiko dapat diadaptasi sehingga mampu mendukung kebutuhan perusahaan dalam menghadapi perubahan lingkungan bisnis.

Bab 3, Transformasi Digital dan Peran AI dalam Manajemen Risiko, menjadi jembatan antara konsep manajemen risiko konvensional dengan pemanfaatan teknologi cerdas. Bab ini menguraikan evolusi digitalisasi dalam bisnis perdagangan, konsep dasar Artificial Intelligence dan Machine Learning, serta perubahan pola identifikasi risiko melalui teknologi cerdas. Pembaca juga diperkenalkan pada manfaat AI dalam pengambilan keputusan berbasis data, tantangan penerapan AI di sektor perdagangan, serta perbedaan antara AI, Big Data, dan

Automation. Pemahaman tersebut menjadi dasar untuk melihat AI bukan hanya sebagai alat otomatisasi, tetapi sebagai teknologi yang dapat mendukung proses pengelolaan risiko secara lebih adaptif dan prediktif.

Pada Bab 4, Identifikasi Risiko Perusahaan Dagang Berbasis AI, pembahasan difokuskan pada bagaimana risiko dapat diidentifikasi dengan mengombinasikan teknik tradisional dan pendekatan berbasis data. Bab ini membandingkan teknik identifikasi risiko konvensional dengan teknik berbasis data, menjelaskan pemanfaatan AI untuk memetakan risiko operasional dan risiko pasar, serta menguraikan bagaimana data transaksi dapat dianalisis untuk menemukan pola-pola yang berpotensi menjadi indikator risiko. Dengan demikian, perusahaan dapat beralih dari identifikasi risiko yang hanya mengandalkan pengalaman menuju pendekatan yang lebih sistematis dan didukung oleh bukti data.

Kemudian, Bab 5, Analisis dan Penilaian Risiko Berbasis Data dan AI, membahas proses analisis dan penilaian risiko secara lebih mendalam. Bab ini dimulai dengan orientasi analisis dan penilaian risiko, dilanjutkan dengan pembahasan mengenai data sebagai fondasi penilaian risiko serta berbagai teknik analisis yang relevan bagi perusahaan dagang. Selanjutnya, dibahas model risk scoring berbasis AI, evaluasi risiko residual, dan penyusunan portofolio risiko. Pembahasan tersebut memberikan pemahaman mengenai bagaimana data dan AI dapat digunakan untuk membantu perusahaan menentukan tingkat prioritas risiko dan mendukung pengambilan keputusan mitigasi.

Pemanfaatan AI dalam manajemen risiko tidak dapat dilepaskan dari aspek tata kelola. Oleh karena itu, Bab 6, Etika, Privasi, Keamanan, dan Kepatuhan AI, membahas berbagai aspek penting yang harus terintegrasi dalam penerapan AI. Bab ini mencakup isu keadilan dan bias algoritma, dampak AI terhadap pemangku kepentingan, transparansi, explainability, dan akuntabilitas. Selain itu, dibahas perlindungan data pribadi dan pendekatan Privacy by Design, keamanan siber dan ancaman khusus AI, kepatuhan terhadap kerangka regulasi nasional maupun internasional, penilaian dampak AI, serta pengelolaan hak kekayaan intelektual dan konten. Bab ini menegaskan bahwa keberhasilan penerapan AI tidak hanya ditentukan oleh kecanggihan teknologinya, tetapi juga oleh kemampuan perusahaan dalam memastikan bahwa teknologi tersebut digunakan secara bertanggung jawab.

Selanjutnya, Bab 7, Strategi Mitigasi Risiko dalam Penggunaan AI, menguraikan langkah-langkah yang dapat dilakukan perusahaan untuk mengendalikan risiko yang muncul akibat pemanfaatan AI. Pembahasan meliputi strategi mitigasi sebagai sistem pengendalian, tata kelola dan pembagian tanggung jawab, kebijakan penggunaan AI serta pengendalian Shadow AI, pengawasan manusia yang bermakna, dan kontrol teknis melalui pendekatan MLOps dan LLMOps. Bab ini juga membahas literasi, budaya organisasi, manajemen perubahan, manajemen vendor dan pihak ketiga, serta respons terhadap insiden dan keberlangsungan bisnis. Sebagai ilustrasi penerapan, disertakan studi kasus sistem harga dinamis PT Niaga Nusantara untuk memberikan gambaran mengenai bagaimana risiko AI dapat dikelola dalam konteks aktivitas bisnis nyata.

Setelah memahami strategi mitigasi, pembaca diarahkan pada aspek implementasi melalui Bab 8, Implementasi Sistem Manajemen Risiko AI Perusahaan Dagang. Bab ini

menjelaskan proses penerjemahan kebijakan menjadi sistem operasional yang dapat diterapkan dalam organisasi. Pembahasannya mencakup penetapan mandat, ruang lingkup, dan sasaran; inventarisasi serta klasifikasi AI use case; penerapan pendekatan stage-gate dalam siklus hidup AI; organisasi, RACI, dan mekanisme pengambilan keputusan; serta pengelolaan data, model, dan dokumentasi. Bab ini juga membahas validasi, persetujuan, peluncuran terkendali, monitoring, Key Risk Indicator (KRI), dashboard, pelaporan, manajemen perubahan dan *material change*, respons insiden, keberlangsungan, serta komunikasi.

Untuk membantu pembaca memahami penerapan secara lebih praktis, Bab 8 juga menyajikan peta jalan implementasi selama 12 bulan, studi kasus terpadu pada PT Niaga Nusantara, serta tahapan dalam merancang sistem manajemen risiko AI perusahaan dagang. Dengan pendekatan tersebut, pembaca tidak hanya memperoleh pemahaman konseptual, tetapi juga gambaran mengenai bagaimana suatu organisasi dapat membangun sistem manajemen risiko AI secara bertahap dan terukur.

Tahapan pengelolaan risiko tidak berhenti setelah sistem diterapkan. Oleh sebab itu, Bab 9, Audit, Kepatuhan, dan Peningkatan Berkelanjutan, membahas mekanisme evaluasi dan assurance untuk memastikan bahwa tata kelola AI berjalan sesuai dengan kebijakan, standar, dan tujuan organisasi. Bab ini menguraikan peran audit dan assurance dalam tata kelola AI, audit universe dan perencanaan audit berbasis risiko, pemahaman sistem dan penelusuran siklus hidup AI, serta audit terhadap data dan privasi. Selanjutnya dibahas audit model, kinerja, fairness, dan explainability, audit keamanan dan ketahanan, audit operasi, monitoring dan perubahan, audit vendor dan kontrak, serta penggunaan bukti audit, sampling, dan analitik. Melalui proses audit dan evaluasi yang berkelanjutan, perusahaan diharapkan mampu melakukan perbaikan terhadap sistem manajemen risiko AI secara konsisten.

Selain sembilan bab utama tersebut, buku ini dilengkapi dengan Glosarium yang memuat istilah-istilah penting dalam manajemen risiko, AI, tata kelola, keamanan, dan audit sehingga dapat membantu pembaca memahami terminologi yang digunakan sepanjang buku. Buku ini juga menyediakan sejumlah lampiran praktis yang dapat digunakan sebagai referensi maupun instrumen awal dalam penerapan manajemen risiko AI di perusahaan dagang. Lampiran tersebut meliputi Formulir Usulan Use Case AI, Template AI Risk Register, Template AI Impact Assessment, Dataset Sheet, Model Card/System Card, Checklist Due Diligence Vendor AI, Formulir Insiden AI, serta Program Audit AI dan Formulir Temuan. Kehadiran berbagai instrumen tersebut diharapkan dapat membantu pembaca menghubungkan konsep yang dipelajari dengan kebutuhan implementasi di lingkungan organisasi.

Untuk memperkuat proses pembelajaran, pada bagian akhir buku juga disediakan Latihan Soal Akhir Buku dan Soal Diskusi. Materi tersebut dirancang untuk membantu mahasiswa, dosen, praktisi, maupun pembaca umum menguji pemahaman terhadap konsep dan penerapan manajemen risiko perusahaan dagang berbasis AI, sekaligus mendorong kemampuan analitis dan pemecahan masalah dalam menghadapi kasus-kasus bisnis yang berkembang.

Dengan demikian, buku “**Manajemen Risiko Perusahaan Dagang Berbasis Artificial Intelligence**” diharapkan dapat menjadi referensi yang bermanfaat bagi mahasiswa, akademisi, praktisi manajemen, pengelola risiko, auditor, pengelola teknologi informasi, pengambil keputusan, maupun pelaku usaha yang ingin memahami hubungan antara manajemen risiko, transformasi digital, dan Artificial Intelligence. Buku ini tidak hanya menempatkan AI sebagai teknologi yang mampu meningkatkan efisiensi, tetapi juga sebagai bagian dari ekosistem bisnis yang membutuhkan tata kelola, pengawasan, keamanan, etika, kepatuhan, serta perbaikan berkelanjutan.

Penulis menyadari bahwa perkembangan Artificial Intelligence dan teknologi digital berlangsung sangat cepat. Oleh karena itu, buku ini masih memiliki kemungkinan untuk terus dikembangkan dan disempurnakan sejalan dengan munculnya teknologi, regulasi, standar, risiko, dan praktik bisnis baru. Kritik, saran, serta masukan yang konstruktif dari para pembaca sangat diharapkan demi meningkatkan kualitas dan relevansi buku ini pada masa mendatang. Akhir kata, semoga buku ini dapat memberikan kontribusi bagi pengembangan pengetahuan dan praktik manajemen risiko, khususnya dalam membangun perusahaan dagang yang adaptif, tangguh, berbasis data, bertanggung jawab, dan mampu memanfaatkan Artificial Intelligence secara aman serta berkelanjutan. Semoga buku ini memberikan manfaat dan menjadi referensi yang berguna bagi setiap pembacanya.

*Semangat dan Selamat Membaca...!!!*

Semarang, September 2026  
Penulis

Sri Wahyuning, S.Kom., M.Si.

## DAFTAR ISI

|                                                                                   |           |
|-----------------------------------------------------------------------------------|-----------|
| <b>KATA PENGANTAR.....</b>                                                        | <b>ii</b> |
| <b>DAFTAR ISI .....</b>                                                           | <b>ii</b> |
| <b>BAB 1 KONSEP DASAR MANAJEMEN RISIKO DALAM PERUSAHAAN DAGANG.....</b>           | <b>1</b>  |
| 1.1 Pengertian Risiko Dan Karakteristik Risiko Bisnis Dagang.....                 | 2         |
| 1.2 Sumber Risiko Dalam Aktivitas Perdagangan.....                                | 4         |
| 1.3 Perbedaan Risiko Operasional, Finansial, Dan Strategis .....                  | 6         |
| 1.4 Pentingnya Manajemen Risiko Dalam Keberlanjutan Usaha Dagang.....             | 9         |
| 1.5 Peran Teknologi Digital Dalam Evolusi Pengelolaan Risiko.....                 | 12        |
| <b>BAB 2 KERANGKA KERJA MANAJEMEN RISIKO PERUSAHAAN.....</b>                      | <b>18</b> |
| 2.1 Prinsip Dasar Manajemen Risiko Korporasi .....                                | 19        |
| 2.2 Pendekatan <i>Enterprise Risk Management</i> (ERM) .....                      | 22        |
| 2.3 Kebutuhan Adaptasi Manajemen Risiko Berdasarkan Skala Perusahaan.....         | 23        |
| 2.4 Integrasi Erm Dengan Tata Kelola Perusahaan .....                             | 25        |
| 2.5 Adaptasi Kerangka Risiko Untuk Perusahaan.....                                | 27        |
| <b>BAB 3 TRANSFORMASI DIGITAL DAN PERAN AI DALAM MANAJEMEN RISIKO.....</b>        | <b>33</b> |
| 3.1 Evolusi Digitalisasi Dalam Bisnis Perdagangan.....                            | 34        |
| 3.2 Konsep Dasar <i>Artificial Intelligence</i> Dan <i>Machine Learning</i> ..... | 39        |
| 3.3 Perubahan Pola Identifikasi Risiko Dengan Teknologi Cerdas .....              | 44        |
| 3.4 Manfaat AI Dalam Pengambilan Keputusan Berbasis Data .....                    | 48        |
| 3.5 Tantangan Implementasi Ai Di Sektor Perdagangan.....                          | 51        |
| 3.6 Perbedaan AI, Big Data, Dan Automation .....                                  | 57        |
| <b>BAB 4 IDENTIFIKASI RESIKO PERUSAHAAN DAGANG BERBASIS AI .....</b>              | <b>61</b> |
| 4.1 Pengantar Bab .....                                                           | 62        |
| 4.2 Teknik Identifikasi Risiko Tradisional Vs Berbasis Data.....                  | 63        |
| 4.3 Pemanfaatan AI Untuk Memetakan Risiko Operasional Dan Pasar.....              | 69        |
| 4.4 Analisis Data Transaksi Untuk Mendeteksi Pola Risiko .....                    | 73        |
| <b>BAB 5 ANALISIS DAN PENILAIAN RISIKO BERBASIS DATA DAN AI.....</b>              | <b>75</b> |
| 5.1 Orientasi Analisis Dan Penilaian Risiko.....                                  | 76        |
| 5.2 Data Sebagai Fondasi Penilaian Risiko .....                                   | 78        |
| 5.3 Teknik Analisis Yang Relevan Bagi Perusahaan Dagang .....                     | 80        |
| 5.4 Model Skoring Risiko Berbasis AI .....                                        | 82        |
| 5.5 Evaluasi Risiko Residual Dan Portofolio Risiko .....                          | 84        |
| <b>BAB 6 ETIKA, PRIVASI, KEAMANAN, DAN KEPATUHAN AI.....</b>                      | <b>90</b> |
| 6.1 Mengapa Etika, Privasi, Keamanan, Dan Kepatuhan Harus Terintegrasi.....       | 91        |
| 6.2 Keadilan, Bias, Dan Dampak Terhadap Pemangku Kepentingan .....                | 92        |
| 6.3 Transparansi, Explainability, Dan Akuntabilitas .....                         | 93        |
| 6.4 Perlindungan Data Pribadi Dan <i>Privacy By Design</i> .....                  | 94        |
| 6.5 Keamanan Siber Dan Ancaman Khusus AI .....                                    | 95        |

|                    |                                                                        |            |
|--------------------|------------------------------------------------------------------------|------------|
| 6.6                | Kepatuhan Nasional Dan Kerangka Internasional.....                     | 96         |
| 6.7                | Penilaian Dampak Ai.....                                               | 98         |
| 6.8                | Pengelolaan Hak Kekayaan Intelektual Dan Konten .....                  | 99         |
| <b>BAB 7</b>       | <b>STRATEGI MITIGASI RISIKO DALAM PENGGUNAAN AI.....</b>               | <b>103</b> |
| 7.1                | Strategi Mitigasi Sebagai Sistem Pengendalian .....                    | 104        |
| 7.2                | Tata Kelola Dan Pembagian Tanggung Jawab .....                         | 105        |
| 7.3                | Kebijakan Penggunaan Dan Pengendalian Shadow AI.....                   | 106        |
| 7.4                | Pengawasan Manusia Yang Bermakna.....                                  | 106        |
| 7.5                | Kontrol Teknis, MLOPS, Dan LLMOPS .....                                | 107        |
| 7.6                | Literasi, Budaya, Dan Manajemen Perubahan.....                         | 108        |
| 7.7                | Manajemen Vendor Dan Pihak Ketiga .....                                | 109        |
| 7.8                | Respons Insiden Dan Keberlangsungan .....                              | 110        |
| 7.9.               | Sistem Harga Dinamis PT Niaga Nusantara.....                           | 110        |
| <b>BAB 8</b>       | <b>IMPLEMENTASI SISTEM MANAJEMEN RISIKO AI PERUSAHAAN DAGANG .....</b> | <b>114</b> |
| 8.1                | Dari Kebijakan Menuju Sistem Operasional.....                          | 115        |
| 8.2                | Menetapkan Mandat, Ruang Lingkup, Dan Sasaran .....                    | 115        |
| 8.3                | Inventarisasi Dan Klasifikasi <i>Use Case</i> AI.....                  | 116        |
| 8.4                | <i>Stage-Gate</i> Siklus Hidup AI.....                                 | 117        |
| 8.5                | Organisasi, Raci, Dan Mekanisme Keputusan .....                        | 118        |
| 8.6                | Pengelolaan Data, Model, Dan Dokumentasi .....                         | 119        |
| 8.7                | Validasi, Persetujuan, Dan Peluncuran Terkendali .....                 | 119        |
| 8.8                | Monitoring, KRI, Dashboard, Dan Pelaporan .....                        | 120        |
| 8.9                | Manajemen Perubahan Dan Material Change.....                           | 121        |
| 8.10               | Respons Insiden, Keberlangsungan, Dan Komunikasi.....                  | 122        |
| 8.11               | Peta Jalan Implementasi 12 Bulan .....                                 | 123        |
| 8.12               | Studi Kasus Terpadu Pada PT Niaga Nusantara .....                      | 124        |
| 8.13               | Merancang Sistem Manajemen Risiko AI.....                              | 125        |
| <b>BAB 9</b>       | <b>AUDIT, KEPATUHAN, DAN PENINGKATAN BERKELANJUTAN .....</b>           | <b>128</b> |
| 9.1                | Peran Audit dan Assurance dalam Tata Kelola AI .....                   | 129        |
| 9.2                | Audit Universe Dan Perencanaan Berbasis Risiko.....                    | 129        |
| 9.3                | Memahami Sistem Dan Menelusuri Siklus Hidup .....                      | 130        |
| 9.4                | Audit Data Dan Privasi.....                                            | 132        |
| 9.5                | Audit Model, Kinerja, Fairness, Dan Explainability .....               | 132        |
| 9.6                | Audit Keamanan Dan Ketahanan .....                                     | 133        |
| 9.7                | Audit Operasi, Monitoring, Dan Perubahan.....                          | 134        |
| 9.8                | Audit Vendor Dan Kontrak .....                                         | 134        |
| 9.9                | Bukti Audit, Sampling, Dan Analitik.....                               | 135        |
| <b>GLOSARIUM</b>   | <b>.....</b>                                                           | <b>142</b> |
| <b>LAMPIRAN A.</b> | <b>FORMULIR USULAN USE CASE AI .....</b>                               | <b>146</b> |
| <b>LAMPIRAN B.</b> | <b>TEMPLATE AI RISK REGISTER .....</b>                                 | <b>147</b> |
| <b>LAMPIRAN C.</b> | <b>TEMPLATE AI IMPACT ASSESSMENT .....</b>                             | <b>148</b> |

|                                                        |     |
|--------------------------------------------------------|-----|
| LAMPIRAN D. DATASET SHEET .....                        | 150 |
| LAMPIRAN E. MODEL CARD / SYSTEM CARD .....             | 151 |
| LAMPIRAN F. CHECKLIST DUE DILIGENCE VENDOR AI .....    | 152 |
| LAMPIRAN G. FORMULIR INSIDEN AI .....                  | 153 |
| LAMPIRAN H. PROGRAM AUDIT AI DAN FORMULIR TEMUAN ..... | 154 |
| LATIHAN SOAL AKHIR BUKU .....                          | 156 |
| SOAL DISKUSI .....                                     | 172 |
| DAFTAR PUSTAKA .....                                   | 183 |



# BAB 1

## KONSEP DASAR MANAJEMEN RISIKO DALAM PERUSAHAAN DAGANG

---

Mengapa ketidakpastian harus dikelola sejak aktivitas pembelian, persediaan, hingga penjualan?

## 1.1 PENGERTIAN RISIKO DAN KARAKTERISTIK RISIKO BISNIS DAGANG

Mari kita duduk sejenak dan coba renungkan ini secara lebih mendalam. Sering kali, dalam obrolan santai di koridor kantor atau saat diskusi di ruang kelas, orang-orang bicara soal manajemen risiko seolah itu hanyalah deretan angka dingin di atas kertas laporan keuangan. Padahal, kalau mau jujur, bisnis dagang itu sebenarnya adalah tentang keberanian kita untuk tetap berdiri tegak di tengah badai ketidakpastian yang sangat dinamis. Risiko itu bukan sesuatu yang bisa dihilangkan sepenuhnya hanya dengan coretan rumus matematika di papan tulis. Bayangkan saja, risiko itu seperti bayangan yang selalu mengikuti ke mana pun langkah perniagaan kita pergi. Begitu seseorang membulatkan tekad untuk menyetor modal dan mulai menumpuk barang di gudang, di detik itulah risiko sebenarnya sudah lahir—ia sudah menjadi bagian dari napas usaha tersebut.

Secara akademis, kalau kita melirik sedikit pada literatur klasik yang sering dibahas, seperti pemikiran Vaughan (1997), risiko dipandang sebagai sebuah kondisi di mana terdapat kemungkinan terjadinya penyimpangan dari hasil yang semula diharapkan. Ada ketidakpastian yang bersifat objektif di sana. Dalam realita dunia dagang yang keras, ini berarti ada peluang besar munculnya peristiwa yang meleset dari rencana-rencana indah kita. Bayangkan rasanya ketika barang yang sudah kita stok tiba-tiba tidak laku karena tren bergeser secepat embusan angin. Atau, harga pasar yang mendadak anjlok dalam semalam, padahal kita baru saja membeli stok dengan harga tinggi. Bahkan, ada hal-hal kecil yang terlihat sepele namun bisa berakibat fatal, seperti masalah kelembapan di pojok gudang yang merusak kualitas stok barang. Rasanya memang tidak adil, tapi itulah seni dalam berdagang—kemampuan untuk tetap navigasi meski kompas kadang menunjukkan arah yang membingungkan.

Pada akhirnya, memahami risiko bukan berarti kita harus jadi penakut. Justru, pemahaman ini memberikan kita "sabuk pengaman" agar saat guncangan itu datang—dan pasti akan datang—kita tidak langsung jatuh terjerembap. Manajemen risiko yang baik adalah tentang bagaimana kita menjaga agar niat baik dan modal yang sudah kita kumpulkan tidak habis terbakar oleh ketidaktahuan kita sendiri akan karakter pasar yang memang sulit ditebak. Dunia dagang memiliki karakteristik risiko yang sangat unik dan, yah, bisa dibilang cukup melelahkan kalau tidak dipahami polanya sejak awal. Sifatnya tidak pernah statis. Ambil contoh fluktuasi harga; hari ini mungkin harga beli terasa murah, tapi besok bisa jadi pasar dibanjiri produk serupa dari kompetitor dengan harga yang jauh di bawah modal kita. Hal ini membuat risiko bisnis dagang terasa begitu personal. Ada juga masalah keterikatan modal pada inventaris. Uang yang berputar di sana adalah "uang mati" sampai barang itu benar-benar laku terjual. Kalau prediksinya meleset sedikit saja, arus kas bisa langsung macet total, dan ini sering kali bukan karena kesalahan teknis yang rumit, tapi sesederhana selera konsumen yang berubah secepat embusan angin.



**Gambar 1.1:** Ilustrasi gudang dengan tumpukan barang yang melimpah di tengah grafik harga pasar yang sedang menurun. Ini merepresentasikan risiko likuiditas dan penurunan nilai aset (*inventory risk*) yang sering menghantui pedagang.

Karakteristik lainnya yang cukup krusial adalah ketergantungan yang sangat tinggi pada rantai pasok. Dalam dagang, tidak ada yang benar-benar bisa berdiri sendiri di pulau terpencil. Jika pemasok telat mengirimkan barang, atau ada gangguan di jalur distribusi karena masalah cuaca maupun regulasi, yang menanggung beban utamanya adalah reputasi toko di mata pelanggan. Ini adalah risiko operasional yang memiliki efek domino yang luar biasa. Memang terasa tidak adil, tapi itulah realita lapangan yang harus dihadapi setiap hari. Ketidakpastian ini tidak perlu ditakuti sampai membuat kita berhenti melangkah, namun memang harus dipetakan dengan saksama agar tidak berubah menjadi kerugian yang mematikan usaha.



**Gambar 1.2:** Diagram Alir Risiko Rantai Pasok

Keterangan Gambar: Diagram yang menunjukkan titik-titik kerentanan mulai dari keterlambatan pengiriman bahan baku hingga kegagalan distribusi ke tangan konsumen akhir, menyoroti betapa rapuhnya lini bisnis dagang terhadap faktor eksternal.

Mengelola semua ini membutuhkan ketajaman intuisi yang didukung oleh pemahaman data yang kuat. Kadang, orang terlalu fokus pada risiko besar yang terlihat bombastis di depan mata, tapi justru risiko kecil yang berulang—seperti penyusutan stok yang tidak terdata atau selisih pembukuan yang dianggap receh—yang perlahan tapi pasti menggerus keuntungan. Memahami karakter risiko berarti tahu di mana harus menempatkan perhatian ekstra dan di mana bisa sedikit melonggarkan kendali. Itulah seni dalam berdagang yang tidak pernah benar-benar bisa diajarkan secara teori murni di ruang kelas, melainkan harus dirasakan langsung lewat jatuh bangunnya interaksi pasar.

## 1.2 SUMBER RISIKO DALAM AKTIVITAS PERDAGANGAN (PEMBELIAN, PERSEDIAAN, PENJUALAN)

Pernahkah, kita membayangkan bagaimana rasanya kalau semua transaksi dalam hidup ini hanya berdasarkan janji? Beli barang, bayar nanti. Jual barang, kasih dulu, tagih kemudian. Aman tidak, ya? Sebenarnya, itulah yang terjadi di hampir semua perusahaan dagang setiap hari. Mereka bekerja di atas kepercayaan. Tapi kepercayaan itu, tanpa sistem yang menjaganya, bisa berubah jadi lubang yang menganga di laporan keuangan. Dan celakanya, lubang itu sering tidak terlihat sampai semuanya terlambat.

- **Pertama**, kita mulai dari hulu: pembelian.

Orang sering berpikir, "ah, beli barang gampang". Ada uang, cari supplier, transfer, barang datang. Tapi di situlah letak naifnya. Sebenarnya, fungsi pembelian itu seperti pintu air. Kalau pintunya bocor dari awal, seluruh danau akan keruh.

Di sinilah risiko pertama mengintai: pemilihan pemasok. Idealnya, setiap pemasok harus melalui seleksi. Harganya dibandingkan, kualitasnya diuji, reputasinya dicek. Tapi dalam praktiknya—apalagi kalau perusahaan sedang terburu-buru—proses ini sering dilompati. Staf pengadaan beli dari orang yang sama terus-menerus. Bukan karena itu pilihan terbaik, tapi karena itu yang paling tidak merepotkan. Atau, lebih rumit lagi, karena ada hubungan keluarga, hubungan pertemanan lama, atau semacam perjanjian di bawah meja yang tidak pernah tercatat di dokumen resmi.

Pernah ada kasus di sebuah perusahaan konstruksi. Setiap bulan mereka membeli pasir dan batu dari satu pemasok. Harganya sedikit di atas pasar, tapi masih masuk akal. Tidak ada yang curiga. Sampai suatu hari, pemilik perusahaan kebetulan makan siang di warung dekat lokasi proyek. Dia berdiskusi dengan mandor, dan tanpa sengaja mandor bilang, "Bos, supplier kita itu, mobilnya masuk lewat jalan belakang, tidak lewat pintu utama. Katanya biar cepet, tidak antre." Pemiliknya diam. Besoknya dia periksa sendiri. Ternyata, selama dua tahun, mereka membeli material dari perusahaan yang tidak pernah terdaftar sebagai vendor resmi. Tidak ada kontrak. Tidak ada evaluasi. Hanya ada faktur bulanan yang ditandatangani. Orang di bagian pengadaan? Ternyata adik ipar dari pemasok itu sendiri.

ini bukan soal selisih harga kecil. Ini soal bagaimana kepercayaan yang longgar menciptakan celah yang bisa dimasuki siapa saja.

Tapi risiko pembelian tidak selalu menyenamkan itu. Kadang ia hadir dalam bentuk yang lebih halus, lebih administratif, lebih membosankan—tapi tidak kalah merusak. Misalnya, ketidakcocokan dokumen. Purchase order mengatakan barang A, surat jalan mengatakan barang A, tapi faktur mengatakan barang A dengan harga berbeda. Atau, spesifikasi teknis tidak ditulis dengan jelas. Barang datang, warnanya beda tipis, ukurannya beda sedikit, tapi masih bisa dipakai. Akhirnya diterima. Masuk gudang. Tapi enam bulan kemudian, pelanggan komplain karena barang cepat rusak. Ketika ditelusuri, ternyata materialnya memang grade-nya di bawah standar. Saat pembelian dulu, petugas penerimaan hanya melihat fisik luar, tidak melakukan uji sampling. Sekarang, perusahaan harus menanggung biaya retur, biaya perbaikan reputasi, dan—yang paling sakit—kehilangan kepercayaan pelanggan.

- **Kedua, persediaan.**

Kalau ada satu area dalam akuntansi yang sering dianggap sebagai "kuburan" kesalahan masa lalu, itu adalah persediaan. Banyak perusahaan yang bangkrut bukan karena tidak laku, tapi karena mereka tidak tahu persis apa yang mereka miliki di gudang.

Bayangkan. Sebuah gudang bisa seluas dua lapangan bola. Ada ribuan SKU, ratusan kardus, puluhan palet. Setiap hari barang masuk dan keluar. Setiap hari ada yang dipindah, ada yang diretur, ada yang rusak. Dan di tengah hiruk-pikuk itu, seorang staf gudang harus mencatat semuanya secara akurat. Tanpa kesalahan. Tanpa kelupaan.

Salah satu risiko klasik di persediaan adalah salah klasifikasi. Barang yang seharusnya dihapuskan karena rusak, masih dicatat dengan nilai penuh. Barang yang sudah ketinggalan model, masih dianggap sebagai aset berharga. Saya ingat, waktu masih sering berkunjung ke perusahaan ritel, saya pernah melihat sendiri bagaimana gudang mereka menyimpan ribuan kaus koleksi dua tahun lalu. Kaus itu bagus, masih baru, masih terbungkus plastik. Tapi siapa yang mau beli? Fashion sudah berganti. Desainnya sudah out of date. Di catatan, nilainya masih Rp100.000 per potong. Di pasar, bahkan didiskon 70% pun orang pikir-pikir dulu.

Ini dilema yang nyata. Kalau perusahaan mau jujur, mereka harus menuliskan nilai barang itu turun drastis. Tapi kalau nilai diturunkan, laba ikut turun. Kalau laba turun, bonus karyawan bisa berkurang, harga saham bisa melemah, investor bisa bertanya-tanya. Maka, yang sering terjadi adalah penundaan. Ah, tahun depan saja dihapusnya. Atau, nanti kalau sudah clear out sale. Tapi tahun depan tidak pernah benar-benar datang. Barang itu terus mengendap, dan laporan keuangan terus menunjukkan aset yang sebenarnya sudah tidak bernilai.

Ini bukan hanya soal ketidakakuratan. Ini soal distorsi. Ketika persediaan overvalued, semua keputusan strategis jadi bias. Perusahaan merasa lebih kaya dari yang sebenarnya. Mereka mungkin merencanakan ekspansi, mengambil utang baru, atau membagikan dividen, padahal dagingnya sudah banyak yang busuk.

- **Ketiga, penjualan.**

Di sinilah semua energi dikerahkan. Target, komisi, piala penghargaan, standing ovation di rapat tahunan. Tapi juga di sinilah risiko paling menggoda.

Yang pertama dan paling sering terjadi adalah pengakuan pendapatan yang terlalu dini. Semua orang tahu aturannya: pendapatan diakui ketika barang diserahkan dan risiko kepemilikan berpindah. Tapi menjelang akhir kuartal, atau menjelang tutup tahun buku, aturan itu sering diregangkan. Sedikit saja. hanya beberapa hari. hanya beberapa transaksi.

Pernah dengar istilah *cut-off error*? Ini bukan kesalahan teknis semata, ini kesalahan yang memiliki konsekuensi besar. Sebuah perusahaan bisa melaporkan pertumbuhan 15% di kuartal IV, padahal sebenarnya barang baru sampai di pelanggan di kuartal I tahun berikutnya. Mereka mencatat penjualan di Desember, padahal faktur baru diterbitkan Januari. Mereka mengakui pendapatan, padahal pembayaran belum pasti. Ini bukan soal selisih waktu yang tidak penting. Ini soal integritas pelaporan. Karena ketika satu periode di-*overstate*, periode berikutnya otomatis di-*understate*. Investor yang membaca laporan keuangan tanpa mengetahui manipulasi ini akan mengambil keputusan berdasarkan data yang salah. Dan ketika kebenaran terbuka, kepercayaan runtuh dalam sekejap.

Risiko kedua di area penjualan adalah piutang. Ini seperti parasit yang diam-diam menggerogoti. Perusahaan mencatat penjualan, laba naik, semua orang senang. Tapi uangnya belum masuk. Piutang membengkak, aging schedule memanjang, *allowance for doubtful accounts* tetap kecil. Padahal, di lapangan, *collection tim* sudah kewalahan. Pelanggan A sudah tiga bulan tidak membayar. Pelanggan B mengirim cek kosong dua kali berturut-turut. Pelanggan C *pailit*, tapi kabar itu belum sampai ke bagian akuntansi. Di sinilah pentingnya keberanian untuk mengestimasi secara konservatif. Bukan karena pesimis, tapi karena akuntansi memang mengajarkan kehati-hatian. Lebih baik mengakui kerugian lebih awal dan ternyata tidak terjadi, daripada terlambat mengakui dan semuanya sudah terlanjur kacau.

Tapi, apakah semua perusahaan memiliki keberanian itu? Tidak selalu. Karena mengakui piutang tak tertagih berarti mengakui bahwa penjualan kemarin tidak sebaik yang dikira. Itu tidak nyaman. Apalagi kalau penjualan itu dilakukan oleh manajer bintang, atau tim yang baru saja mendapat penghargaan.

Maka, risiko piutang sering dibiarkan mengendap. Tidak dihapus, tidak dibentuk cadangan yang memadai. Dan seperti bola salju, semakin lama menggelinding, semakin besar.

### 1.3 PERBEDAAN RISIKO OPERASIONAL, FINANSIAL, DAN STRATEGIS

Bayangkan sedang duduk di sebuah kafe dekat kampus. Mungkin sambil menunggu jadwal seminar berikutnya, atau sekadar mencari udara segar setelah berjam-jam di perpustakaan. Lalu seorang teman—mungkin dari jurusan manajemen, atau akuntansi juga—tiba-tiba bertanya, "Sebenarnya, apa bedanya risiko operasional, finansial, dan strategis? Di

kuliah semuanya terdengar mirip." Pertanyaan yang sederhana. Tapi jawabannya tidak sesederhana itu. Dan justru dari situ, kita bisa masuk ke dalam diskusi yang cukup dalam, tanpa perlu merasa sedang di ruang sidang skripsi.

- **Pertama**, mari kita bicara soal risiko operasional.

Ini adalah risiko yang paling dekat dengan keseharian. Paling membumi. Paling mudah dibayangkan karena ia terjadi setiap hari, di setiap sudut perusahaan. Risiko operasional adalah risiko yang muncul dari tidak berfungsinya proses internal, baik karena manusia, sistem, teknologi, atau bahkan karena faktor eksternal yang langsung mengganggu kegiatan sehari-hari.

Salah satu definisi yang cukup dikenal datang dari *Basel Committee on Banking Supervision*—badan yang biasanya bicara soal perbankan, tapi definisinya ternyata relevan juga untuk perusahaan dagang atau manufaktur. Mereka bilang, risiko operasional adalah risiko kerugian yang disebabkan oleh ketidakcukupan atau kegagalan proses internal, manusia, sistem, atau akibat kejadian eksternal.

Bayangkan sebuah gudang. Sore hari menjelang tutup. Seorang petugas gudang menerima kiriman seratus kardus barang, tapi karena sudah capek dan ingin segera pulang, ia hanya menghitungnya sekilas. Dua hari kemudian, bagian akuntansi menerima faktur, staf administrasi mencocokkan dengan laporan penerimaan barang, dan ternyata ada selisih. Kardus yang diterima hanya sembilan puluh delapan, tapi faktur tetap seratus. Selisih dua kardus. Nilainya mungkin tidak besar. Tapi kejadian ini adalah contoh klasik risiko operasional. Bukan karena ada niat jahat. Tapi karena prosedur tidak dijalankan dengan ketat. Atau karena sistem tidak memiliki peringatan otomatis kalau ada ketidaksesuaian.

Atau contoh lain. Sistem komputer di bagian penjualan tiba-tiba down selama setengah hari. Karyawan tidak bisa mengakses data harga, tidak bisa mencetak faktur. Pelanggan menunggu, lalu akhirnya pergi. Penjualan hilang. Ini juga risiko operasional. Bukan karena kesalahan orang, tapi karena sistem yang tidak andal.

Yang menarik dari risiko operasional adalah, ia sering tidak dramatis. Ia tidak muncul dalam pemberitaan ekonomi seperti krisis keuangan atau gejolak pasar. Tapi ia hadir setiap hari, dalam sunyi, menggerogoti efisiensi dan perlahan-lahan mengubah laba menjadi ongkos.

- **Kedua**, kita melompat ke wilayah yang lebih abstrak, tapi tidak kalah nyata: risiko finansial.

Ini adalah risiko yang berkaitan dengan uang. Tapi bukan uang sebagai hasil penjualan, melainkan uang sebagai struktur. Uang sebagai sumber daya. Uang sebagai kewajiban. Secara sederhana, risiko finansial adalah risiko yang timbul dari keputusan perusahaan dalam mengelola keuangan—bagaimana mereka mendapatkan dana, bagaimana mereka menempatkannya, dan bagaimana mereka menghadapi perubahan variabel keuangan seperti suku bunga, nilai tukar, atau likuiditas.

Salah satu definisi klasik datang dari Brigham dan Houston, yang mengatakan bahwa risiko finansial adalah tambahan risiko yang ditanggung oleh pemegang saham sebagai

akibat dari penggunaan utang. Artinya, ketika perusahaan meminjam uang, mereka sebenarnya sedang menciptakan semacam pisau bermata dua. Di satu sisi, utang bisa memperbesar laba kalau bisnis sedang bagus. Di sisi lain, utang menjadi beban tetap yang harus dibayar, tidak peduli apakah penjualan sedang lesu atau pasar sedang terpuruk.

Bayangkan perusahaan yang terlalu optimis. Mereka meminjam besar untuk ekspansi, membangun pabrik baru, merekrut ratusan karyawan. Dua tahun kemudian, permintaan pasar turun. Penjualan merosot. Tapi cicilan utang tetap jalan. Bunga tetap jalan. Kontrak dengan bank tidak bisa dinegosiasi ulang. Perusahaan mulai kesulitan membayar gaji. Apa yang tadinya dianggap sebagai strategi pertumbuhan, tiba-tiba berubah menjadi jerat.

Itulah risiko finansial. Ia tidak muncul dari kesalahan operasional, bukan karena barang rusak atau faktur salah. Ia muncul dari keputusan strategis yang salah dalam menentukan komposisi pendanaan.

Bentuk lain dari risiko finansial adalah risiko nilai tukar. Untuk perusahaan yang melakukan impor bahan baku atau ekspor produk, fluktuasi kurs bisa menjadi mimpi buruk. Rupiah melemah sepuluh persen dalam sebulan, tiba-tiba harga bahan baku naik, margin menyusut, dan semua perencanaan laba harus direvisi. Padahal, secara operasional, tidak ada yang berubah. Produktivitas sama, kualitas terjaga, penjualan stabil. Tapi nilai uangnya berubah.

Ini yang kadang terasa tidak adil dalam bisnis. Bekerja keras, efisien, disiplin, tapi tetap bisa merugi hanya karena gejolak makroekonomi. Tapi memang seperti itulah risiko finansial: ia tidak selalu sebanding dengan kinerja internal. Kadang ia datang dari luar, seperti tamu tak diundang, lalu duduk lama tanpa permisi.

- **Ketiga**, kita naik ke tingkat paling atas, ke ruang di mana keputusan-keputusan besar dibuat: risiko strategis.

Risiko strategis adalah risiko yang timbul dari keputusan fundamental tentang arah bisnis. Pasar mana yang akan dimasuki, produk apa yang akan dikembangkan, apakah akan akuisisi atau organik, apakah akan fokus di segmen tertentu atau melebar. Ini adalah keputusan yang tidak diambil setiap hari. Tapi ketika diambil, konsekuensinya besar dan jangka panjang.

Definisi dari Kaplan dan Mikes, yang banyak dikutip dalam literatur manajemen risiko, menyebutkan bahwa risiko strategis adalah risiko yang secara inherent melekat pada strategi yang dipilih. Bukan karena strateginya salah dieksekusi, tapi karena strateginya sendiri—meskipun dijalankan dengan sempurna—bisa tetap gagal karena asumsi-asumsi yang mendasarinya ternyata keliru.

Contoh klasik adalah perusahaan fotografi Kodak. Mereka tahu teknologi digital dari awal, bahkan menciptakan kamera digital pertama. Tapi mereka memilih untuk tetap fokus pada film karena itu sumber laba utama mereka. Secara operasional, mereka menjalankan bisnis dengan sangat baik. Produk berkualitas, distribusi luas, merek kuat.

Tapi strateginya salah. Mereka mempertahankan masa lalu terlalu lama. Dan ketika sadar, semuanya sudah terlambat.

Itulah risiko strategis. Ia tidak terlihat dalam laporan harian. Tidak muncul di catatan gudang. Tapi ia menentukan hidup matinya perusahaan.

Risiko operasional itu dekat, kasatmata, sehari-hari. Ia bisa dikelola dengan prosedur, pelatihan, sistem, dan pengawasan. Risiko finansial itu lebih makro, berkaitan dengan struktur modal dan eksposur keuangan. Ia bisa dikelola dengan lindung nilai, diversifikasi sumber dana, atau sekadar tidak meminjam terlalu banyak. Dan risiko strategis itu fundamental, berkaitan dengan pilihan arah. Ia tidak bisa dikelola dengan checklist, tapi dengan kepekaan terhadap perubahan dan keberanian untuk mengubah haluan ketika diperlukan.

Ketiganya tidak berdiri sendiri. Sering kali, satu jenis risiko memicu yang lain. Strategi ekspansi yang agresif (risiko strategis) biasanya membutuhkan utang besar (risiko finansial). Utang besar membuat arus kas tegang, memaksa perusahaan menekan efisiensi, dan ketika efisiensi dilakukan dengan tergesa-gesa, prosedur operasional mulai longgar (risiko operasional). Maka, kecelakaan besar dalam bisnis jarang datang dari satu sumber. Ia adalah akumulasi, seperti gelombang yang tidak kelihatan dari pantai, tapi ketika sampai di darat, kekuatannya menghancurkan.

Jadi, ketika seseorang bertanya, "Risiko mana yang paling berbahaya?" jawabannya mungkin tidak akan pernah tunggal. Untuk startup teknologi, risiko strategis bisa menjadi penentu: salah pilih produk, mati. Untuk perusahaan dagang dengan margin tipis, risiko operasional bisa menggerogoti perlahan: kebocoran kecil di gudang, lama-lama jadi danau. Untuk perusahaan yang sedang ekspansi besar-besaran, risiko finansial bisa menjadi pisau gantung: utang menggunung, arus kas macet, reputasi runtuh.

Tapi satu hal yang pasti: tidak ada perusahaan yang bisa mengabaikan salah satunya. Karena ketiganya bukan pilihan. Mereka adalah kenyataan yang harus dihadapi setiap hari, oleh setiap orang, di setiap level organisasi. Dari staf gudang yang memeriksa kardus, hingga direktur utama yang memutuskan akuisisi.

Maka, ketika membaca laporan keuangan atau menyusun strategi bisnis, coba ingat-ingat lagi tiga lingkaran itu. Operasional, finansial, strategis. Mereka tidak akan pernah muncul dengan label jelas di halaman depan. Tapi mereka ada di sana, di setiap angka, di setiap catatan kaki, di setiap asumsi yang tidak dituliskan.

#### **1.4 PENTINGNYA MANAJEMEN RISIKO DALAM KEBERLANJUTAN USAHA DAGANG**

Pernahkan kita membayangkan, sebuah perusahaan yang sudah berjalan puluhan tahun, tiba-tiba harus gulung tikar bukan karena kalah saing, bukan karena pasar hilang, tapi karena sesuatu yang sebenarnya sudah terlihat sejak lama tapi tidak pernah dianggap serius? Mungkin seperti orang yang tiba-tiba sakit keras, padahal gejala-gejalanya sudah muncul bertahun-tahun—hanya saja selalu diabaikan dengan alasan, "Ah, nanti juga sembuh sendiri." Dalam dunia bisnis, gejala-gejala itu adalah risiko. Dan yang membuat perusahaan tetap hidup, tetap bernapas di tengah badai, bukanlah keberuntungan semata. Tapi karena mereka

memiliki sesuatu yang sering disebut sebagai manajemen risiko. Tapi jangan bayangkan manajemen risiko sebagai tumpukan buku tebal berdebu di rak direksi. Lebih dari itu, ini tentang bagaimana sebuah perusahaan memilih untuk jujur pada dirinya sendiri, tentang apa yang bisa salah, dan apa yang akan mereka lakukan ketika itu benar-benar terjadi.

Salah satu definisi yang cukup membumi datang dari buku *Manajemen Keuangan Strategik* karangan Tatang Ary Gumanti yang diterbitkan Universitas Terbuka. Di situ dijelaskan bahwa manajemen risiko adalah bagian dari lima keputusan utama dalam perusahaan—bersama dengan keputusan pendanaan, investasi, dividen, dan tata kelola. Artinya, mengelola risiko bukanlah pekerjaan sampingan yang dilakukan kalau ada waktu luang. Ia adalah fungsi inti, sama pentingnya dengan memutuskan mau meminjam ke bank mana atau mau ekspansi ke kota mana.

Tapi definisi yang lebih teknis—dan menurut hemat saya lebih manusiawi—datang dari artikel *Proxis Consulting* yang menyebut manajemen risiko sebagai strategi perusahaan di era ketidakpastian. Kata kuncinya di sini adalah "ketidakpastian". Karena dunia bisnis memang tidak pernah pasti. Hari ini orderan deras, minggu depan pelanggan besar bisa saja pindah ke kompetitor hanya karena selisih harga seribu rupiah. Hari ini nilai tukar rupiah stabil, tiga bulan lagi bisa melemah drastis dan mengerek harga bahan baku impor.

Manajemen risiko hadir bukan untuk menghilangkan ketidakpastian itu—karena itu mustahil—tapi untuk membuat perusahaan tetap bisa berjalan meskipun ketidakpastian itu terjadi. Ia semacam pagar pengaman di tepi jurang. Tidak mencegah kita mendekati jurang, tapi menahan kalau terpeleset. Sekarang, mari kita lihat lebih dekat, kenapa ini penting sangat, terutama untuk usaha dagang.

### **Manajemen risiko itu soal kelangsungan hidup.**

Ada studi kasus menarik dari PT. KP, sebuah perusahaan general trading di Cikarang yang sudah beroperasi 22 tahun. Dua puluh dua tahun! Itu bukan waktu yang sebentar. Tapi perusahaan ini nyaris terpuruk karena satu hal: dead stock. Barang menumpuk, tidak laku, dan nilainya mencapai Rp 4,5 miliar. Coba bayangkan, uang sebanyak itu mengendap di gudang, tidak bisa diputar, sementara biaya operasional tetap jalan, gaji karyawan tetap harus dibayar, cicilan utang tetap harus dipenuhi.

Apa penyebabnya? Bukan karena pemasok curang, bukan juga karena kualitas barang jelek. Tapi karena mereka salah memperkirakan permintaan pasar. Mereka memesan terlalu banyak, dengan asumsi pasar akan terus tumbuh. Tapi ternyata tidak. Dan karena tidak ada mekanisme deteksi dini, risiko itu membesar diam-diam, sampai akhirnya meledak.

Untungnya, mereka kemudian melakukan analisis risiko dengan pendekatan ISO 31000:2009, mengidentifikasi sepuluh risiko prioritas, dan berhasil menurunkan nilai dead stock sebesar Rp 900 juta hanya dalam enam bulan. Angka itu mungkin tidak mengembalikan semuanya, tapi setidaknya menunjukkan satu hal: ketika risiko dikelola, perusahaan bisa selamat. Ketika tidak, perusahaan bisa tenggelam.

Ini pelajaran berharga. Bahwa perusahaan yang sudah berpuluh tahun pun, kalau lengah terhadap risiko, bisa jatuh dalam waktu singkat. Sebaliknya, perusahaan yang relatif muda, kalau sadar risiko sejak awal, memiliki peluang lebih besar untuk bertahan.

**Manajemen risiko juga soal kepercayaan.**

Pernah dengar istilah GRC? *Governance, Risk, and Compliance*. Ini adalah tiga pilar yang makin sering dibicarakan dalam diskusi tata kelola perusahaan. Menurut Prof. Mardiasmo, Ketua Umum Komite Nasional Kebijakan Governansi, dalam situasi dunia yang penuh ketidakpastian seperti sekarang, GRC yang terintegrasi bisa mengubah sesuatu yang "*unpredictable*" menjadi "*predict*". Artinya, dengan manajemen risiko yang baik, perusahaan tidak hanya sekadar bereaksi ketika masalah datang. Mereka sudah memiliki antenna, sudah memiliki radar, sudah memiliki rencana cadangan. Dan ini yang dilihat oleh investor, dilihat oleh bank, dilihat oleh mitra bisnis.

Bayangkan Anda seorang bankir. Datang dua perusahaan mengajukan kredit. Perusahaan pertama memiliki catatan penjualan bagus, tapi tidak bisa menunjukkan bagaimana mereka mengelola risiko—tidak ada dokumen, tidak ada kebijakan, tidak ada bukti bahwa mereka pernah memikirkan skenario terburuk. Perusahaan kedua, omzetnya mungkin sedikit lebih kecil, tapi mereka memiliki kerangka manajemen risiko yang jelas, memiliki laporan identifikasi risiko, memiliki rencana mitigasi. Siapa yang akan Anda kasih kredit? Jawabannya, hampir pasti yang kedua. Kepercayaan itu tidak datang tiba-tiba. Ia dibangun dari bukti bahwa perusahaan tidak hanya mengejar keuntungan, tapi juga menjaga agar keuntungan itu tidak hilang begitu saja karena hal-hal yang sebenarnya bisa diantisipasi.

**Manajemen risiko itu soal efisiensi dalam diam.**

Sering tidak sadar, biaya-biaya kecil yang muncul dari risiko yang tidak dikelola itu sebenarnya lebih besar dari yang kita kira. Kerugian karena barang rusak, karena faktur salah, karena piutang macet, karena denda keterlambatan, karena kehilangan pelanggan—semua itu kalau diakumulasi, bisa mencapai angka yang mencengangkan.

**Manajemen risiko juga bicara soal keberlanjutan.**

Prinsip Tata Kelola Perusahaan G20/OECD 2023 menyebutkan bahwa kerangka tata kelola harus memberikan insentif bagi perusahaan untuk membuat keputusan dan mengelola risiko dengan cara yang berkontribusi terhadap keberlanjutan dan ketahanan perusahaan. Ini penting, karena investor sekarang tidak hanya melihat laba hari ini, tapi juga apakah perusahaan masih akan ada sepuluh atau dua puluh tahun lagi.

Risiko keberlanjutan itu macam-macam. Ada risiko lingkungan, risiko sosial, risiko perubahan regulasi. Misalnya, perusahaan yang masih menggunakan bahan baku yang tidak ramah lingkungan, suatu saat bisa kena pajak karbon atau denda lingkungan. Perusahaan yang mengabaikan hak-hak pekerja, bisa menghadapi demo atau boikot. Perusahaan yang tidak peduli pada komunitas sekitar, bisa kehilangan "izin sosial" untuk beroperasi.

Ini bukan wacana aktivis lingkungan, ini sudah masuk ke ranah bisnis nyata. Banyak perusahaan besar sekarang mewajibkan pemasok mereka untuk memiliki sertifikasi keberlanjutan. Bank-bank mulai mempertimbangkan aspek *Environmental, Social, and Governance* (ESG) dalam pemberian kredit. Kalau perusahaan dagang tidak mengelola risiko-risiko ini, mereka bisa tersingkir dari rantai pasok global.

**Manajemen risiko adalah tentang budaya.**

PT Sarana Multigriya Finansial (SMF) dalam salah satu kegiatan sosialisasinya menekankan pentingnya "budaya sadar risiko". Bukan sekadar prosedur, bukan sekadar dokumen, tapi kesadaran yang melekat pada setiap orang di perusahaan. Dari staf gudang, staf penjualan, sampai direktur utama.

Mengapa budaya penting? Karena risiko tidak selalu datang dalam bentuk besar yang terlihat. Ia sering hadir dalam keputusan-keputusan kecil sehari-hari. Staf pembelian yang memilih pemasok karena "sudah langganan" tanpa membandingkan harga. Staf penjualan yang memberi diskon terlalu besar hanya untuk mencapai target bulanan. Staf gudang yang lupa mencatat barang masuk karena terburu-buru. Semua ini, kalau dibiarkan, akan menjadi budaya. Dan budaya yang longgar terhadap risiko, pada akhirnya akan melahirkan bencana.

Budaya sadar risiko berarti setiap orang, di level mana pun, memiliki pertanyaan sederhana di kepalanya: "Apa yang bisa salah dari keputusan ini?" Dan ketika mereka menemukan jawabannya, mereka memiliki keberanian untuk mengatakannya, atau bahkan menghentikan proses kalau diperlukan. Ini tidak mudah, apalagi di perusahaan yang hierarkis. Tapi inilah yang membedakan perusahaan yang sekadar besar dengan perusahaan yang benar-benar tangguh.

*Sekarang, setelah kita berkeliling membahas pentingnya manajemen risiko, mungkin kita bisa menarik satu kesimpulan sederhana.*

Manajemen risiko bukanlah tentang membuat perusahaan takut melangkah. Bukan tentang membungkus semua keputusan dengan lapisan-lapisan prosedur yang membuat gerak jadi lambat. Justru sebaliknya. Manajemen risiko yang baik adalah tentang memberi perusahaan keberanian untuk melangkah, karena mereka tahu persis apa yang bisa salah dan sudah menyiapkan jaring pengamannya.

Perusahaan dagang pun begitu. Persaingan akan tetap keras, pasar akan tetap berfluktuasi, pelanggan akan tetap berubah selera. Tapi perusahaan yang memiliki manajemen risiko yang baik, akan tetap bisa berlayar di tengah badai. Mungkin oleng, mungkin lambat, tapi tidak tenggelam.

Dan pada akhirnya, itulah arti keberlanjutan yang sebenarnya. Bukan sekadar bertahun-tahun eksis, tapi mampu melewati berbagai musim, berbagai krisis, berbagai tantangan, tanpa kehilangan arah. Karena mereka sadar: risiko tidak akan pernah hilang, tapi dengan dikelola, ia bisa menjadi teman perjalanan, bukan ancaman.

**1.5 PERAN TEKNOLOGI DIGITAL DALAM EVOLUSI PENGELOLAAN RISIKO**

Pernahkah, kita membayangkan bagaimana rasanya jadi manajer risiko di sebuah perusahaan besar di era sekarang? Bukan seperti di film-film Hollywood yang penuh ketegangan dengan layar-layar berkedip dan alarm berbunyi. Lebih membosankan dari itu, sebenarnya. Tapi juga lebih menegangkan, karena tanggung jawabnya nyata. Setiap hari harus memikirkan hal-hal yang mungkin salah, yang belum terjadi, yang bahkan belum terpikirkan

oleh orang lain. Dan tantangannya sekarang: semua itu harus dilakukan di tengah banjir data yang setiap detik terus mengalir, transaksi yang terjadi dalam hitungan milidetik, dan risiko yang muncul bukan lagi dari satu arah, tapi dari berbagai penjuru sekaligus.

### **Konsep dan Peran Teknologi Digital dalam Pengelolaan Risiko**

Kalau kita baca di artikel *Proxis Consulting*, peran teknologi dalam kepatuhan dan manajemen risiko adalah pemanfaatan solusi digital mutakhir untuk mentransformasi pendekatan tradisional menjadi sistem yang proaktif, terintegrasi, dan berbasis data. Artinya, teknologi tidak lagi sekadar alat bantu—semacam kalkulator canggih—tapi sudah menjadi fondasi utama. Ia mengubah cara perusahaan melihat risiko, dari yang tadinya reaktif (menunggu masalah lalu memperbaikinya) menjadi proaktif (mendeteksi sebelum masalah terjadi).

Ini pergeseran yang cukup fundamental. Dulu, manajemen risiko sering dianggap sebagai beban. Sesuatu yang menghabiskan biaya, memperlambat proses, dan hasilnya tidak kelihatan langsung. Makanya, banyak perusahaan menempatkan fungsi ini sebagai "anak tiri"—ada, tapi tidak terlalu diperhatikan. Tapi sekarang, dengan teknologi, fungsi ini mulai berubah menjadi value creator. Ia bisa memberikan wawasan strategis, membantu pengambilan keputusan, bahkan menciptakan keunggulan kompetitif.

### **Jenis Teknologi Digital dalam Pengelolaan Risiko**

*Artificial Intelligence* dan *Machine Learning*, misalnya. Teknologi ini tidak hanya digunakan untuk membuat chatbot atau aplikasi pengenalan wajah. Dalam manajemen risiko, AI bisa digunakan untuk predictive modeling—memprediksi risiko apa yang mungkin muncul berdasarkan pola-pola data masa lalu. Ia juga bisa mendeteksi anomali dalam transaksi yang mungkin menunjukkan indikasi kecurangan. Bahkan, dengan *Natural Language Processing*, AI bisa membaca dan menganalisis ribuan halaman dokumen regulasi dalam hitungan menit, sesuatu yang kalau dilakukan manusia bisa berminggu-minggu.

Bayangkan, sebuah perusahaan dagang yang melakukan ribuan transaksi setiap hari. Dengan metode manual, mendeteksi satu transaksi mencurigakan saja bisa seperti mencari jarum di tumpukan jerami. Tapi dengan AI, pola-pola mencurigakan itu bisa langsung terdeteksi secara *real-time*. Sebuah studi kasus dari ElysianNxt, perusahaan *software* solusi risiko, menunjukkan bahwa klien mereka bisa mengurangi waktu perhitungan data kepatuhan regulasi dari 24 jam menjadi kurang dari 1 jam menggunakan teknologi berbasis cloud dan AI. Bayangkan efisiensi yang bisa didapat.

Kemudian ada Blockchain. Ini sering dikaitkan dengan *cryptocurrency*, tapi sebenarnya aplikasinya jauh lebih luas. Dalam manajemen risiko, blockchain digunakan untuk menciptakan *immutable* audit trails—jejak audit yang tidak bisa diubah. Setiap transaksi, setiap perubahan data, tercatat secara permanen dan transparan. Ini sangat berguna untuk memastikan integritas data dan mencegah manipulasi. Dengan *smart contracts*, kepatuhan terhadap aturan tertentu bisa dijalankan secara otomatis. Misalnya, kontrak dengan pemasok yang secara otomatis membayar ketika barang diterima dan diverifikasi, tanpa perlu campur tangan manusia yang rawan konflik kepentingan.

*Cloud Computing* dan *platform SaaS* juga mengubah cara perusahaan mengelola risiko. Dulu, untuk memiliki sistem manajemen risiko yang canggih, perusahaan harus investasi besar untuk *hardware*, *software*, dan tim IT yang memeliharanya. Sekarang, dengan model langganan, perusahaan kecil dan menengah pun bisa mengakses teknologi yang sama dengan perusahaan besar. Ini mendemokratisasi akses terhadap manajemen risiko yang baik.

Bahkan *Internet of Things* (IoT) ikut ambil peran. Sensor-sensor yang dipasang di gudang, di jalur distribusi, atau di peralatan produksi, bisa memberikan data real-time tentang kondisi barang, suhu penyimpanan, getaran saat pengiriman, dan sebagainya. Kalau ada penyimpangan—misalnya suhu *cold storage* naik di atas batas aman—sistem bisa langsung memberi peringatan sebelum barang rusak. Ini bentuk pencegahan risiko yang tidak mungkin dilakukan dengan inspeksi manual.

### **Contoh Penerapan Teknologi Digital dalam Pengelolaan Risiko di Indonesia**

Ada. Dan cukup menarik. PT Dahana, sebuah BUMN yang bergerak di industri pertahanan, baru saja meluncurkan aplikasi bernama E-Manrisk pada November 2025. Ini adalah aplikasi digital manajemen risiko terintegrasi yang dirancang untuk mempermudah proses identifikasi, penilaian, dan mitigasi risiko secara real-time.

Yang menarik dari peluncuran ini bukan hanya aplikasinya, tapi juga konteksnya. Direktur Keuangan PT Dahana, Mohamad Nur Sodiq, dalam sambutannya menekankan bahwa manajemen risiko bukan hanya tanggung jawab pimpinan puncak, tapi harus menjadi nafas dalam setiap eksekusi pekerjaan di lapangan. Dan E-Manrisk ini adalah alat untuk mewujudkan itu. Dengan aplikasi ini, setiap karyawan di level operasional bisa melaporkan potensi risiko yang mereka lihat, dan manajemen bisa merespons lebih cepat. Dari sini kita mulai melihat pola: teknologi mengubah manajemen risiko dari fungsi administratif menjadi fungsi strategis.

Konsep ini kemudian berkembang menjadi apa yang disebut sebagai GRC 4.0 atau Digitalisasi GRC (*Governance, Risk, and Compliance*). Menurut *Proxis Consulting*, digitalisasi GRC adalah transformasi fundamental yang mengubah proses manual dan terfragmentasi menjadi sistem otomatis, terintegrasi, dan berbasis data. Ini bukan sekadar mengotomasi proses yang sudah ada, tapi mentransformasi model operasional dari reaktif menjadi proaktif, dari berbasis sampel menjadi berbasis populasi data penuh, dan dari terisolasi menjadi terintegrasi penuh dengan operasi bisnis.

Artinya, dengan digitalisasi, manajemen risiko tidak lagi dilakukan oleh satu departemen secara terpisah. Ia melekat dalam setiap proses bisnis. Ketika staf penjualan memasukkan order, sistem otomatis memeriksa limit kredit pelanggan. Ketika staf gudang mencatat penerimaan barang, sistem otomatis mencocokkan dengan purchase order. Ketika manajer keuangan melihat laporan arus kas, ia juga bisa melihat simulasi dampak jika nilai tukar berubah lima persen.

Semua ini terjadi dalam hitungan detik, tanpa perlu menunggu laporan bulanan atau rapat koordinasi. Tapi, apakah semua perusahaan sudah siap dengan transformasi ini? Ternyata tidak sesederhana itu.



**Gambar 1.3.** Ruang pemantauan risiko terintegrasi di sebuah perusahaan logistik. Teknologi menyediakan data real-time, tapi diskusi manusia tetap menjadi inti pengambilan keputusan. Di sinilah evolusi pengelolaan risiko terjadi: bukan teknologi menggantikan manusia, tapi teknologi memperkuat manusia.

Sebuah survei yang dilakukan oleh Airmic di Inggris pada pertengahan 2025 menunjukkan gambaran yang menarik. Di satu sisi, ada optimisme tentang transformasi digital. Tapi di sisi lain, adopsi teknologi untuk fungsi manajemen risiko masih terhambat oleh berbagai faktor. Fakta yang cukup mengejutkan: 12% responden sama sekali tidak menggunakan platform komersial untuk manajemen risiko. Dan mayoritas—hampir 60%—masih sering menggunakan Excel untuk aktivitas terkait risiko. Padahal, kita tahu Excel memiliki keterbatasan: rawan kesalahan manual, sulit diaudit, tidak *real-time*, dan tidak terintegrasi.

Apa penghalang terbesar? Biaya. Dua pertiga responden menyebut biaya sebagai hambatan utama. Biaya implementasi, lisensi, dan pemeliharaan sistem baru memang tidak murah, terutama untuk perusahaan menengah. Tapi selain biaya, ada juga tantangan teknis, resistensi karyawan terhadap perubahan, kurangnya dukungan manajemen puncak, dan kekhawatiran tentang keamanan data. Yang menarik, resistensi terhadap perubahan disebut sebagai hambatan signifikan. Orang-orang sudah nyaman dengan cara lama—mungkin karena sudah puluhan tahun menggunakan Excel, atau karena takut dengan teknologi baru yang mereka tidak pahami. Ini menunjukkan bahwa transformasi digital bukan hanya soal teknologi, tapi juga soal manusia dan budaya.

Survei yang sama juga menemukan bahwa hanya 2% responden yang sudah sepenuhnya mengintegrasikan generative AI dalam proses mereka. Dua persen! Artinya, meskipun AI sedang digembar-gemborkan di mana-mana, adopsinya di fungsi manajemen risiko masih sangat awal. Tapi minatnya tinggi. Banyak perusahaan sedang mencoba

memahami bagaimana mereka bisa menggunakan alat-alat ini, sambil tetap berhati-hati dengan risikonya.

### **Arah dan Masa Depan Pengelolaan Risiko Berbasis Teknologi Digital**

Frost & Sullivan, dalam laporannya tentang *Enterprise Risk Mitigation and Management* (ERMM) untuk 2026, mengidentifikasi beberapa tren besar.

#### **Pertama, ada integrasi GenAI dalam alur kerja ERMM.**

Generative AI tidak hanya digunakan untuk analisis data, tapi juga untuk mengotomasi deteksi kejadian risiko, menghasilkan ringkasan untuk pemangku kepentingan, bahkan menyusun draf komunikasi *respons* awal. Ini mengurangi waktu respons dari berjam-jam menjadi hanya hitungan menit. Bayangkan ketika terjadi krisis, perusahaan bisa langsung mengeluarkan pernyataan resmi dalam waktu singkat, bukan berjam-jam setelah rapat berkepanjangan.

#### **Kedua, ada penggabungan data ERMM, ESG, dan keamanan siber menjadi "Enterprise Trust Score".**

Ini semacam skor kredit, tapi untuk menilai kepercayaan terhadap perusahaan secara keseluruhan. Skor ini menggabungkan stabilitas rantai pasok, metrik keberlanjutan, dan postur keamanan siber menjadi satu nilai dinamis. Digunakan oleh tim pengadaan, perusahaan asuransi, dan investor untuk membuat keputusan yang lebih informasi. Perusahaan dengan skor tinggi akan lebih mudah mendapatkan mitra, asuransi murah, dan investasi.

#### **Ketiga, ada pengakuan terhadap "climate volatility" sebagai risiko inti.**

Perubahan iklim tidak lagi dianggap sebagai isu lingkungan semata, tapi risiko bisnis yang nyata. Dengan teknologi seperti citra satelit dan sensor IoT, perusahaan bisa memantau risiko fisik seperti ketersediaan air, gelombang panas, atau banjir, serta risiko transisi seperti perubahan regulasi.

#### **Keempat, ada pergeseran menuju kerangka manajemen risiko sistemik.**

Organisasi mulai mengadopsi pendekatan yang mengakui bahwa krisis global—pandemi, perubahan iklim, ketegangan geopolitik—saling terkait dan bisa terjadi bersamaan. Tidak lagi dilihat sebagai ancaman terpisah, tapi sebagai jaringan risiko yang saling mempengaruhi. Tapi dari semua perkembangan ini, ada satu pelajaran penting yang sering terlupakan.

Di tengah semua kecanggihan teknologi, di tengah AI yang bisa memprediksi, blockchain yang mencatat tanpa bisa diubah, dan IoT yang memantau 24 jam, manusia tetap menjadi faktor penentu. Survei Airmic menunjukkan bahwa resistensi karyawan bisa menggagalkan proyek teknologi. Sebaliknya, dukungan manajemen puncak bisa mempercepat adopsi. PT Dahana, dalam peluncuran E-Manrisk, tidak hanya meluncurkan aplikasi, tapi juga menggelar seminar untuk membangun pemahaman tentang manajemen risiko di semua level. Mereka sadar bahwa teknologi saja tidak cukup. Harus ada perubahan mindset. Ini yang kadang luput dari diskusi tentang transformasi digital. Kita terlalu fokus pada teknologi—AI-nya, *blockchain*-nya, *cloud*-nya—tapi lupa bahwa yang menjalankan teknologi itu tetap manusia. Dan manusia memiliki kebiasaan, memiliki ketakutan, memiliki zona

nyaman. Kalau aspek manusianya tidak dikelola, teknologi secanggih apa pun hanya akan menjadi pajangan mahal.

**Tabel 1.1** Contoh Nyata Pentingnya Manajemen Risiko AI

| Kasus                  | Penjelasan Risiko                                                                                                                                 |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| Chatbot Diskriminatif  | Sebuah chatbot AI yang belajar dari percakapan internet menjadi rasis dan seksis karena datanya tidak disaring. Risiko reputasi dan etika muncul. |
| Sistem Kredit Otomatis | Algoritma perbankan menolak pengajuan kredit secara bias terhadap kelompok tertentu. Risiko hukum dan sosial muncul.                              |
| Mobil Otonom           | AI gagal membaca situasi jalan, menyebabkan kecelakaan. Risiko hukum dan nyawa menjadi taruhannya.                                                |

## KESIMPULAN

1. Teknologi digital mengubah manajemen risiko dari fungsi reaktif dan administratif menjadi kemampuan strategis yang proaktif, memungkinkan deteksi dini dan respons cepat terhadap berbagai ancaman.
2. Meskipun adopsi teknologi seperti AI dan blockchain semakin meluas, hambatan utama tetap pada faktor manusia: resistensi terhadap perubahan, biaya, dan keterbatasan keahlian digital.
3. Masa depan pengelolaan risiko terletak pada integrasi yang harmonis antara kecanggihan teknologi dan kebijaksanaan manusia, di mana data real-time memperkuat—bukan menggantikan—pengambilan keputusan di semua level organisasi

## Latihan

1. Jawablah pertanyaan dengan jelas
2. Jelaskan pengertian dari Manajemen risiko
3. Jelaskan tentang alasan utama mengapa manajemen risiko diperlukan pada perusahaan dagang
4. Sebutkan berapa alasan mengapa manajemen risiko penting dalam perusahaan dagang

## BAB 2

# KERANGKA KERJA MANAJEMEN RISIKO PERUSAHAAN

---

Bagaimana prinsip, tata kelola, dan ERM membentuk organisasi yang tangguh?

### CAPAIAN PEMBELAJARAN

- Menjelaskan delapan prinsip ISO 31000:2018.
- Membandingkan pendekatan ISO 31000 dan COSO ERM.
- Menjelaskan integrasi ERM dengan tata kelola.
- Menyesuaikan kerangka dengan skala perusahaan.
- Mengevaluasi peran budaya dan tiga lini.

## 2.1 PRINSIP DASAR MANAJEMEN RISIKO KORPORASI

Sebenarnya apa yang membuat sebuah perusahaan bisa bertahan puluhan tahun, sementara yang lain tumbang di tengah jalan? Bukan soal besarnya modal, bukan juga soal pintarnya direktur utama. Lebih dari itu, sering kali jawabannya ada pada satu hal yang sederhana tapi sulit: kemampuan perusahaan untuk mengenali dan mengelola risikonya sendiri. Dan di balik kemampuan itu, ada seperangkat prinsip yang menjadi fondasinya. Prinsip-prinsip ini bukan sekadar teori yang harus dihafal untuk ujian, tapi lebih seperti nilai-nilai yang hidup dalam keseharian organisasi. Mari kita bahas pelan-pelan, seperti sedang berdiskusi di teras kampus sambil menunggu hujan reda.

### Konsep Dasar Manajemen Risiko Korporasi

Kalau kita membuka standar internasional yang paling banyak dirujuk di dunia, yaitu ISO 31000:2018 tentang Risk management — *Guidelines*, di situ disebutkan delapan prinsip yang menjadi fondasi bagi setiap organisasi yang ingin mengelola risikonya secara efektif (ISO, 2018). Prinsip-prinsip ini bukan sekadar aturan kaku, melainkan "*essential qualities*" yang harus melekat dalam sistem manajemen risiko.

Standar yang sama ini juga memberikan definisi yang cukup mendasar. Risiko adalah "efek dari ketidakpastian terhadap pencapaian sasaran organisasi" (ISO, 2018). Sedangkan manajemen risiko didefinisikan sebagai "aktivitas-aktivitas terkoordinasi yang dilakukan dalam rangka mengelola dan mengontrol sebuah organisasi terkait dengan risiko yang dihadapinya" (ISO, 2018). Manajemen risiko korporasi atau *Enterprise Risk Management* (ERM) dengan demikian adalah sistem yang diterapkan untuk mengelola dan mengontrol risiko bisnis perusahaan atau korporat, dengan harapan sasaran perusahaan dapat tercapai.

### Manajemen risiko menciptakan dan melindungi nilai (ISO, 2018).

Ini mungkin yang paling mendasar. Kadang orang berpikir manajemen risiko hanya soal mencegah kerugian, padahal lebih dari itu. Ia juga soal menciptakan nilai. Sebuah perusahaan yang mampu mengelola risikonya dengan baik akan lebih dipercaya oleh pelanggan, mitra, dan pemangku kepentingan lainnya. Kepercayaan itu adalah nilai yang tidak terlihat tapi sangat nyata dampaknya. Bayangkan dua perusahaan yang sama-sama memproduksi barang sejenis. Perusahaan A memiliki reputasi bahwa mereka selalu tepat waktu dan produknya konsisten berkualitas. Perusahaan B sering terlambat karena "ada masalah di gudang" atau "ada kendala teknis". Konsumen, tanpa sadar, akan lebih memilih perusahaan A meskipun harganya sedikit lebih mahal. Itulah nilai yang diciptakan oleh manajemen risiko yang baik. Bahkan, dalam kerangka COSO ERM yang banyak digunakan di seluruh dunia, ditekankan bahwa fokus utama ERM adalah pada penciptaan, pemeliharaan, dan realisasi nilai (COSO, 2017). Jadi, manajemen risiko bukan sekadar biaya, tapi investasi untuk menjaga nilai perusahaan tetap utuh.

### Manajemen risiko merupakan bagian terintegrasi dari seluruh proses organisasi (ISO, 2018).

Ini yang sering luput. Banyak perusahaan menempatkan fungsi manajemen risiko sebagai unit terpisah yang bekerja sendiri. Padahal, prinsipnya justru sebaliknya. Manajemen risiko harus melekat dalam setiap proses, setiap pengambilan keputusan, setiap aktivitas operasional. Bukan sesuatu yang dilakukan setelah keputusan diambil, tapi bagian dari

pertimbangan sejak awal. Dalam praktiknya, ini berarti ketika staf pembelian memilih pemasok, ia secara otomatis mempertimbangkan risiko keterlambatan atau risiko kualitas. Ketika tim pemasaran menetapkan target penjualan, mereka memikirkan risiko piutang macet. Ketika direksi memutuskan ekspansi ke kota baru, mereka sudah memetakan risiko persaingan dan regulasi. Semua itu berjalan natural, bukan karena diperintah, tapi karena sudah menjadi cara berpikir. Integrasi ini juga tercermin dalam pendekatan *Three Lines of Defense* yang banyak diadopsi perusahaan. Di mana fungsi bisnis menjadi garis pertahanan pertama (*risk owner*), unit manajemen risiko menjadi garis kedua, dan audit internal menjadi garis ketiga (IIA, 2020). Semua bekerja dalam satu kesatuan, bukan silo-silo terpisah.

**Manajemen risiko adalah bagian dari pengambilan keputusan (ISO, 2018).**

Setiap keputusan yang diambil perusahaan, dari yang strategis hingga yang operasional, mengandung konsekuensi dan ketidakpastian. Manajemen risiko membantu para pengambil keputusan untuk memahami *trade-off* yang ada, mempertimbangkan berbagai skenario, dan memilih opsi yang paling sesuai dengan tujuan organisasi. Dengan mengetahui potensi risiko, perusahaan dapat membuat keputusan yang lebih terinformasi. Dalam praktiknya, ini berarti setiap usulan investasi, setiap rencana pengembangan produk, setiap kebijakan baru, harus disertai dengan analisis risikonya. Bukan untuk membuat takut atau menghambat, tapi untuk memastikan bahwa keputusan diambil dengan pemahaman yang utuh.

Pernah ada kasus di mana sebuah perusahaan ritel memutuskan untuk memperluas gerai ke kota baru tanpa analisis risiko yang memadai. Mereka hanya melihat potensi pasarnya besar. Tapi setelah beroperasi setahun, ternyata biaya logistiknya jauh lebih tinggi dari perkiraan, perizinan lebih rumit, dan persaingan lebih ketat. Akhirnya gerai itu tutup dengan kerugian besar. Seandainya sejak awal mereka memasukkan analisis risiko dalam pengambilan keputusan, mungkin hasilnya berbeda.

**Manajemen risiko secara eksplisit menangani ketidakpastian (ISO, 2018).**

Ini terdengar seperti pernyataan yang *obvious*, tapi sebenarnya penting. Manajemen risiko tidak berurusan dengan hal-hal yang sudah pasti, tapi dengan hal-hal yang belum pasti. Ia mengakui bahwa masa depan tidak dapat diprediksi dengan sempurna, dan karena itu kita perlu bersiap. Dalam praktiknya, ini berarti perusahaan tidak hanya membuat satu rencana, tapi juga skenario-skenario alternatif. Tidak hanya mengandalkan satu pemasok, tapi juga memiliki cadangan. Tidak hanya mengejar satu segmen pasar, tapi juga mulai menjajaki segmen lain. Semua itu adalah cara untuk mengakui dan merespons ketidakpastian.

**Manajemen risiko bersifat sistematis, terstruktur, dan tepat waktu (ISO, 2018).**

Ini soal metodologi. Manajemen risiko yang baik tidak dilakukan secara sporadis atau hanya ketika ada masalah. Ia harus sistematis, mengikuti proses yang jelas: identifikasi risiko, analisis risiko, evaluasi risiko, penanganan risiko, dan pemantauan. Proses ini dilakukan secara konsisten dan berulang. Selain itu, ia juga harus tepat waktu. Risiko pasar bisa berubah dalam hitungan jam. Risiko reputasi bisa meledak dalam hitungan menit di era media sosial. Karena itu, deteksi dini menjadi sangat penting. Organisasi seharusnya menetapkan indikator

peringatan dini (*early warning indicators*) untuk aktivitas bisnis kritis, sehingga ketika ambang tertentu tercapai, tindakan korektif bisa segera diambil.

**Manajemen risiko didasarkan pada informasi terbaik yang tersedia (ISO, 2018).**

Keputusan tentang risiko hanya sebaik informasi yang mendasarinya. Karena itu, perusahaan perlu mengumpulkan data dari berbagai sumber, menganalisisnya dengan metode yang tepat, dan memastikan bahwa informasi yang digunakan adalah yang terkini dan relevan. Tapi ini juga berarti mengakui bahwa informasi tidak pernah sempurna. Ada keterbatasan data, ada bias, ada hal-hal yang tidak diketahui. Karena itu, manajemen risiko yang baik juga mencakup kesadaran akan keterbatasan informasi itu sendiri.

**Manajemen risiko disesuaikan (*tailored*) (ISO, 2018).**

Tidak ada satu pendekatan manajemen risiko yang cocok untuk semua perusahaan. Setiap organisasi memiliki konteks yang unik: ukurannya, struktur organisasinya, budaya manajemennya, tingkat kematangan risikonya, dan lingkungan di mana ia beroperasi. Karena itu, kerangka manajemen risiko harus disesuaikan dengan karakteristik masing-masing. Perusahaan startup teknologi memiliki profil risiko yang berbeda dengan perusahaan manufaktur tua. Perusahaan multinasional memiliki tantangan yang berbeda dengan UMKM lokal. Prinsip ini mengingatkan bahwa manajemen risiko bukanlah soal mengkopi-paste prosedur dari perusahaan lain, tapi merancang sistem yang memang sesuai dengan kebutuhan sendiri.

**Manajemen risiko mempertimbangkan faktor manusia dan budaya (ISO, 2018).**

Ini yang sering dilupakan. Kita terlalu sibuk dengan model matematis, matriks risiko, dan prosedur baku, tapi lupa bahwa yang menjalankan semua itu adalah manusia. Dan manusia memiliki psikologi, memiliki bias, memiliki ketakutan, memiliki zona nyaman. Faktor budaya juga sangat menentukan. Di perusahaan dengan budaya hierarkis yang kaku, karyawan mungkin enggan melaporkan risiko karena takut dianggap tidak kompeten. Di perusahaan dengan budaya menyalahkan, setiap masalah akan disembunyikan bukan diselesaikan. Sebaliknya, perusahaan dengan budaya sadar risiko akan mendorong setiap orang untuk berbicara terbuka tentang potensi masalah.

Prinsip ini mengingatkan bahwa membangun sistem saja tidak cukup. Harus ada upaya simultan untuk membangun budaya. Di PT Dahana, misalnya, dalam peluncuran aplikasi manajemen risiko mereka, ditekankan bahwa manajemen risiko harus menjadi "nafas dalam setiap eksekusi pekerjaan di lapangan" dan bahwa implementasinya didukung dengan komitmen penuh dari jajaran direksi, manajemen, dan karyawan (Dahana, 2025).

**Prinsip kesembilan: Manajemen risiko bersifat transparan dan inklusif (ISO, 2018).**

Manajemen risiko yang baik melibatkan pemangku kepentingan yang relevan. Bukan hanya manajemen puncak, tapi juga karyawan di level operasional, mitra bisnis, bahkan kadang regulator dan masyarakat. Keterlibatan ini penting karena setiap pemangku kepentingan memiliki perspektif yang berbeda tentang risiko. Komunikasi yang jelas tentang risiko dan pengelolaannya untuk seluruh stakeholder perusahaan sangat penting. Laporan risiko secara berkala kepada manajemen puncak dan pemangku kepentingan membantu dalam mengambil keputusan yang tepat. Dan yang tak kalah penting, membangun saluran

komunikasi yang terbuka untuk melaporkan risiko yang muncul atau kesalahan dalam implementasi mitigasi.

**Manajemen risiko bersifat dinamis, iteratif, dan responsif terhadap perubahan (ISO, 2018).**

Risiko tidak pernah statis. Lingkungan berubah, teknologi berubah, pasar berubah, regulasi berubah. Karena itu, manajemen risiko juga harus berubah. Apa yang dianggap risiko besar tahun lalu, mungkin tahun ini sudah tidak relevan. Sebaliknya, risiko yang dulu diabaikan, tiba-tiba bisa menjadi ancaman serius. Proses manajemen risiko karena itu harus dilakukan secara terus-menerus, bukan sekali setahun. Identifikasi, analisis, evaluasi, dan penanganan risiko harus menjadi siklus yang berulang. Dan setiap kali ada perubahan signifikan, prosesnya harus dijalankan lagi.

**Manajemen risiko memfasilitasi perbaikan berkelanjutan organisasi (ISO, 2018).**

Yang terakhir ini mungkin yang paling visioner. Manajemen risiko yang baik tidak hanya melindungi dari kerugian, tapi juga mendorong organisasi untuk terus belajar dan berkembang. Setiap kejadian risiko, setiap near-miss, setiap keberhasilan mitigasi, adalah kesempatan untuk meningkatkan kemampuan. Organisasi yang tertarik pada perbaikan berkelanjutan harus mengembangkan strategi untuk meningkatkan kematangan risiko mereka. Evaluasi berkala terhadap sistem manajemen risiko sangat penting untuk memastikan efektivitas dan relevansinya. Apakah mitigasi yang diterapkan sudah efektif? Apakah ada risiko baru yang muncul? Apakah ada cara yang lebih baik untuk mengelola risiko yang sama? Pertanyaan-pertanyaan ini harus diajukan secara rutin.

Mungkin, kalau direnungkan lebih dalam, prinsip-prinsip ini bukan hanya tentang manajemen risiko korporasi. Ia juga bisa menjadi metafora tentang bagaimana kita menjalani hidup. Menciptakan dan melindungi nilai—apa yang benar-benar penting bagi kita. Terintegrasi dalam setiap keputusan—bukan sekadar rencana di atas kertas. Menangani ketidakpastian—mengakui bahwa kita tidak tahu segalanya. Sistematis tapi juga manusiawi—ada prosedur tapi juga empati. Dan terus belajar, terus berkembang, karena dunia tidak pernah berhenti berubah. Pada akhirnya, perusahaan yang sehat bukanlah yang tidak pernah mengalami masalah. Tapi yang ketika masalah datang, ia memiliki fondasi untuk tetap berdiri. Dan fondasi itu, delapan prinsip ini, adalah batu-batu pertama yang harus diletakkan dengan hati-hati. Bukan untuk dipajang, tapi untuk dihidupi setiap hari, oleh setiap orang, di setiap level organisasi.

## **2.2 PENDEKATAN ENTERPRISE RISK MANAGEMENT (ERM)**

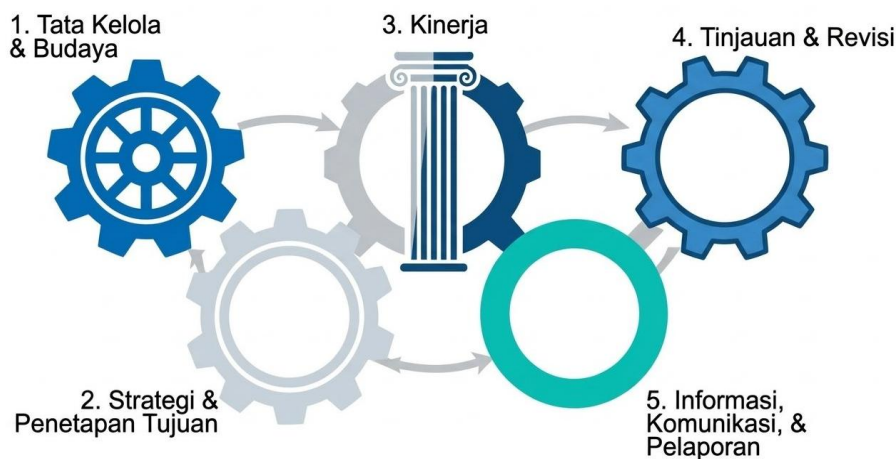
Membedah *Enterprise Risk Management* (ERM) itu sebenarnya mirip seperti kita sedang belajar menakhodai sebuah kapal pesiar raksasa di tengah samudra yang cuacanya tidak pernah bisa ditebak. Kadang tenang, tapi di bawah permukaan ada arus yang sangat kuat, dan di cakrawala badai bisa muncul kapan saja. Selama ini, mungkin banyak dari kita—termasuk para praktisi bisnis kawakan sekalipun—terjebak dalam pola pikir kalau risiko itu harus dikotak-kotakkan. Bagian keuangan hanya pusing soal fluktuasi mata uang, tim operasional stres kalau mesin produksi macet, sementara anak-anak IT begadang karena takut ada serangan siber. Tapi, mari kita jujur sejenak. Apakah di dunia nyata risiko itu sesopan itu

sampai mau mengantre satu per satu? Tentu saja tidak. Risiko itu saling berkelindan, saling bernapas, dan sering kali memicu reaksi berantai yang tidak terduga. Inilah alasan mengapa pendekatan "Silo" atau manajemen risiko tradisional yang terpisah-pisah sudah kuno. Kita butuh sesuatu yang lebih holistik, yang kita sebut dengan Enterprise Risk Management.

### Memahami Akar dan Filosofi ERM

Secara mendalam, ERM ini bukan sekadar alat atau perangkat lunak mahal yang dibeli perusahaan agar terlihat canggih di depan investor. ERM adalah sebuah filosofi. Jika kita melihat dari kacamata akademis, salah satu rujukan paling kuat adalah COSO (*Committee of Sponsoring Organizations of the Treadway Commission*). Dalam publikasi mereka yang monumental, *Enterprise Risk Management — Integrated Framework* (2004), ERM didefinisikan sebagai sebuah proses yang dipengaruhi oleh dewan direksi, manajemen, dan personel lainnya, yang diterapkan dalam pengaturan strategi di seluruh perusahaan. Tujuannya sederhana namun sangat ambisius: untuk mengidentifikasi peristiwa potensial yang mungkin memengaruhi entitas, dan mengelola risiko agar tetap berada dalam "selera risiko" (*risk appetite*) mereka. Intinya, ERM ingin memastikan bahwa organisasi tidak hanya "bertahan hidup" secara kebetulan, tapi benar-benar memiliki kendali atas nasibnya sendiri.

### COSO ERM - Mengintegrasikan dengan Strategi dan Kinerja



**Gambar 2.1:** Kerangka Kerja COSO ERM *Integrated Framework*

### 2.3 KEBUTUHAN ADAPTASI MANAJEMEN RISIKO BERDASARKAN SKALA PERUSAHAAN

Bayangkan sebuah bank yang hanya fokus pada risiko kredit tapi mengabaikan risiko reputasi di media sosial. Atau sebuah pabrik yang memiliki pengamanan fisik luar biasa tapi membiarkan sistem kontrol digitalnya tanpa proteksi yang memadai. Dalam manajemen risiko tradisional, setiap departemen merasa sudah melakukan tugasnya dengan baik, tapi tidak ada yang melihat gambaran besarnya. Akibatnya? Muncul "*blind spot*" atau titik buta yang sangat berbahaya.

ERM masuk untuk menghancurkan tembok-tembok pemisah tersebut. Pendekatan ini memaksa setiap kepala departemen untuk duduk di meja yang sama dan bertanya: "Kalau departemen saya bermasalah, bagaimana pengaruhnya ke departemenmu?" Di sinilah aspek

humanis dari manajemen risiko muncul. Kita bukan lagi bicara soal angka di Excel, tapi soal komunikasi, kepercayaan, dan budaya kerja. Tanpa transparansi, ERM hanya akan menjadi tumpukan dokumen yang berdebu di lemari audit.

### Standar Global sebagai Navigasi

Selain COSO, kita juga memiliki ISO 31000:2018. Standar internasional ini memberikan perspektif yang sedikit lebih luwes namun tetap kokoh. ISO menekankan bahwa manajemen risiko harus terintegrasi, terstruktur, komprehensif, inklusif, dan—ini yang paling penting—dinamis. Risiko tidak pernah statis. Apa yang kita anggap aman hari ini, bisa jadi adalah ancaman terbesar besok pagi karena adanya perubahan regulasi atau munculnya teknologi baru seperti AI generatif. Bagi organisasi yang ingin menerapkan ERM secara serius, mereka harus menyadari bahwa ini adalah investasi jangka panjang. Tidak ada jalan pintas. Anda harus mulai dari membangun "*Risk Culture*". Artinya, setiap staf, mulai dari satpam di depan hingga CEO di lantai teratas, harus paham bahwa mereka adalah "*Risk Owner*". Jika seorang staf di bagian gudang melihat ada kabel yang terkelupas dan segera melaporkannya, dia sebenarnya sedang menjalankan praktik ERM. Dia mencegah risiko operasional berubah menjadi risiko finansial (kebakaran) dan risiko keselamatan jiwa.



**Gambar 2.2:** Proses Manajemen Risiko ISO 31000] Keterangan Gambar: Alur melingkar yang menekankan pada pentingnya "*Scope, Context, and Criteria*" sebagai awal dari setiap penilaian risiko, serta peran sentral komunikasi dan konsultasi yang terus-menerus.

### Tantangan Implementasi: Antara Teori dan Realita

Mari kita bicara jujur: menerapkan ERM itu melelahkan dan penuh drama. Kenapa? Karena manusia secara alami tidak suka diawasi. Banyak manajer yang merasa bahwa proses ERM hanya menambah birokrasi dan memperlambat pengambilan keputusan. "Kita ini mau berjualan atau mau ngurusin daftar risiko terus?" Begitu biasanya keluhan yang muncul. Di sinilah peran kepemimpinan diuji. ERM tidak akan jalan kalau hanya dianggap sebagai proyek sampingan tim kepatuhan (*compliance*). Ia harus menjadi bagian dari setiap keputusan strategis. Saat perusahaan ingin melakukan ekspansi ke negara baru, pertanyaannya bukan hanya "Berapa untungnya?", tapi "Apa profil risiko di sana dan apakah kita sanggup menanggungnya?".

Kadang, penjelasan mengenai risiko ini memang tidak bisa sempurna. Kita sering berhadapan dengan data yang tidak lengkap atau ketidakpastian yang benar-benar baru (*unknown unknowns*). Namun, dengan kerangka kerja yang sudah mapan seperti ERM, setidaknya kita memiliki bahasa yang sama untuk mendiskusikan ketidakpastian tersebut. Kita memiliki alat untuk mengukur dan memprioritaskan mana api yang harus segera dipadamkan dan mana asap yang masih bisa kita pantau dari jauh.

### Menuju Organisasi yang Resilien

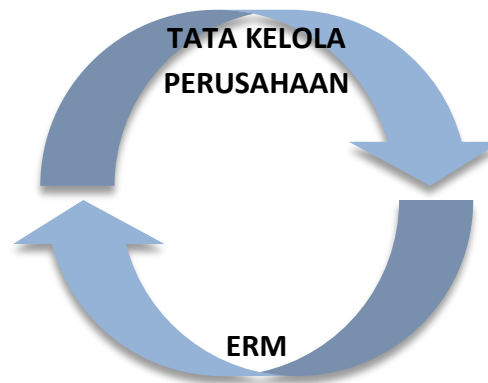
Pada akhirnya, ERM bukan tentang menghilangkan risiko—karena hanya orang yang tidak melakukan apa-apa yang tidak memiliki risiko. ERM adalah tentang "*Risk-Informed Decision Making*". Dengan memahami seluruh spektrum risiko secara mendalam dan menyeluruh, organisasi justru menjadi lebih berani untuk mengambil peluang yang mungkin dihindari oleh pesaingnya. Mereka berani karena mereka tahu di mana letak payungnya saat hujan turun, dan mereka tahu seberapa kuat mesin kapalnya saat harus menembus ombak besar. Dunia bisnis ke depan akan semakin liar. Pandemi, perubahan iklim, hingga disrupsi teknologi adalah pengingat bahwa ketangguhan (*resilience*) adalah mata uang baru yang sangat berharga. Dan ERM adalah fondasi utama untuk membangun ketangguhan itu.

## 2.4 INTEGRASI ERM DENGAN TATA KELOLA PERUSAHAAN

Integrasi antara *Enterprise Risk Management* (ERM) dengan *Corporate Governance* atau tata kelola perusahaan sebenarnya adalah soal bagaimana kita membangun "kecerdasan kolektif". Tata kelola memberikan kerangka etika, struktur pelaporan, dan akuntabilitas, sementara ERM masuk ke dalam sela-sela struktur itu untuk memberikan informasi yang jujur mengenai ancaman dan peluang yang mungkin dihadapi. Tanpa integrasi ini, tata kelola hanya akan menjadi tumpukan dokumen administratif yang kaku, sementara manajemen risiko hanya akan menjadi latihan teknis yang tidak memiliki pengaruh pada keputusan strategis di tingkat atas.

Bicara soal sumber, kita tidak bisa hanya terpaku pada ISO atau COSO yang sudah sangat populer itu. Ada perspektif menarik dari James Lam (2014) dalam bukunya *Enterprise Risk Management: From Incentives to Controls*. Lam menekankan bahwa ERM seharusnya bukan sekadar fungsi kontrol, melainkan bagian integral dari proses penetapan strategi dan manajemen kinerja. Ia berpendapat bahwa tata kelola yang efektif mensyaratkan dewan

direksi untuk memahami profil risiko perusahaan secara menyeluruh, sehingga keputusan yang diambil bukan berdasarkan keberuntungan, melainkan berdasarkan kalkulasi yang matang terhadap nilai perusahaan (*shareholder value*). Ini adalah pandangan yang sangat "manusiawi" karena mengakui bahwa di balik angka-angka ekonomi, ada keputusan manajerial yang harus dipertanggungjawabkan secara etis.



**Gambar 2.3:** Visualisasi hubungan simbiotik antara tata kelola perusahaan dengan ERM, di mana kebijakan dari atas (*top-down*) bertemu dengan identifikasi risiko dari bawah (*bottom-up*) untuk menciptakan ekosistem organisasi yang resilien.

Namun, mari kita bicarakan realitanya di lapangan yang sering kali tidak seindah teori di buku teks. Banyak organisasi yang merasa sudah melakukan integrasi hanya karena mereka memiliki "Komite Manajemen Risiko" yang bertemu tiga bulan sekali. Padahal, integrasi sejati itu terasa pada cara seorang staf di lapangan berani melaporkan anomali tanpa rasa takut, karena dia tahu tata kelola perusahaannya menjamin transparansi. Integrasi ini menuntut perubahan budaya yang radikal. Risiko bukan lagi tanggung jawab satu departemen khusus di pojok gedung, melainkan menjadi tanggung jawab setiap orang, mulai dari staf di garda depan hingga pimpinan di lantai teratas.

Kita sering melihat kegagalan besar pada perusahaan-perusahaan raksasa bukan karena mereka tidak memiliki ahli manajemen risiko, tapi karena ada "putus sambung" antara informasi risiko dengan pengambilan keputusan di tingkat direksi. Inilah yang oleh Monks dan Minow (2011) dalam literatur tata kelola mereka disebut sebagai kegagalan sistem pengawasan. Jika informasi risiko disembunyikan demi terlihat "baik-baik saja" di depan pemegang saham, maka tata kelola tersebut sebenarnya sudah runtuh dari dalam. Integrasi ERM memberikan "lampu depan" yang terang bagi tata kelola agar para pengambil kebijakan bisa melihat lubang di jalan sebelum mereka menabraknya. Rasanya memang melelahkan dan penuh drama ketika kita mencoba menyatukan banyak kepala yang memiliki kepentingan berbeda-beda. Manajer penjualan mungkin merasa prosedur risiko hanya menghambat target mereka, sementara tim tata kelola dianggap sebagai "polisi" yang kerjanya hanya mencari kesalahan. Di sinilah seni dari integrasi itu muncul. Ia bukan soal melarang orang mengambil risiko, melainkan soal memberikan navigasi agar risiko yang diambil itu "sepadan" dengan visi organisasi.

Pada akhirnya, sebuah perusahaan yang benar-benar dewasa akan menyadari bahwa manajemen risiko yang terintegrasi adalah bentuk tertinggi dari rasa hormat terhadap para pemangku kepentingan. Kita memastikan bahwa setiap rupiah yang diinvestasikan, setiap keringat karyawan, dan setiap janji kepada pelanggan dijaga oleh sistem pengawasan yang cerdas dan jujur. Memang tidak ada sistem yang sempurna—pasti akan ada kesalahan di sana-sini—tapi dengan integrasi yang kuat, kita setidaknya tidak sedang berjalan dalam kegelapan tanpa pegangan sama sekali.

## 2.5 ADAPTASI KERANGKA RISIKO UNTUK PERUSAHAAN DAGANG

Mengapa ada perusahaan dagang kecil di pasar tradisional yang bisa bertahan puluhan tahun, sementara perusahaan besar dengan gedung megah tiba-tiba ambruk dalam hitungan bulan? Kadang jawabannya bukan soal modal. Bukan juga soal jaringan. Tapi soal bagaimana mereka membaca dan merespons risiko dengan cara yang cocok untuk ukuran mereka sendiri.

Ini menarik, karena kalau kita bicara soal manajemen risiko, seringkali yang terbayang adalah perusahaan multinasional dengan gedung pencakar langit, tim analis data, dan perangkat lunak canggih. Padahal, seorang pedagang sembako di pasar juga perlu mengelola risiko—hanya caranya yang beda. Dia mungkin tidak membuat register risiko formal, tapi dia tahu persis berapa banyak utang yang bisa dikasih ke langganan, kapan harus restok barang, dan supplier mana yang suka telat kirim. Di sinilah letak tantangan sekaligus keindahannya. Kerangka manajemen risiko seperti ISO 31000 atau COSO ERM itu bukan barang sakral yang hanya bisa dipakai perusahaan besar. Justru, kekuatan terbesar dari kerangka-kerangka ini adalah fleksibilitasnya. Mereka bisa ditarik, dilembungkan, atau dipotong sesuai kebutuhan. Seperti baju yang bisa dijahit agar pas di badan, bukan badan yang dipaksa masuk ke baju.

### Memahami Peta Jalan: Kerangka Itu Seperti Peta, Bukan Jalur Kereta Api

Sebelum kita masuk ke dalam adaptasi, kita harus sepakat dulu soal satu hal. Kerangka manajemen risiko itu fungsinya memberi arah, bukan mengikat. ISO 31000, misalnya, dengan delapan prinsipnya yang terkenal itu, sejak awal dirancang sebagai pedoman yang bisa diterapkan di organisasi mana pun, terlepas dari ukuran atau jenis industrinya. Artinya, standar ini mengakui bahwa setiap organisasi itu unik. Tidak ada satu ukuran yang cocok untuk semua. Hal yang sama berlaku untuk COSO ERM. Kerangka yang diperbarui tahun 2017 ini memang terlihat rumit dengan lima komponen dan dua puluh prinsipnya. Tapi kalau kita baca lebih dalam, sebenarnya COSO juga mendorong fleksibilitas. Prinsip-prinsip itu bisa diimplementasikan dengan cara yang berbeda-beda, tergantung pada kompleksitas, kapasitas, dan kebutuhan organisasi. Jadi, ketika kita bicara adaptasi untuk perusahaan dagang dari skala kecil hingga besar, kita sebenarnya sedang bicara tentang spektrum. Di ujung sana ada UMKM yang dikelola keluarga dengan omzet puluhan juta per bulan. Di ujung sini ada korporasi dagang dengan cabang di seluruh Indonesia, ribuan karyawan, dan rantai pasok yang melibatkan belasan negara. Keduanya butuh manajemen risiko. Tapi bentuknya pasti beda.

### Yang Kecil Tetap Bisa Berlindung: Adaptasi untuk UMKM dan Perusahaan Dagang Skala Kecil

Mari kita mulai dari yang kecil. Bayangkan sebuah toko kelontong atau distributor kecil di kota. Siapa yang biasanya jadi "manajer risiko"? Ya pemiliknya sendiri. Semua keputusan ada di tangannya. Ini sebenarnya bentuk manajemen risiko yang paling sederhana tapi paling intensif. Karena pemilik melihat langsung setiap transaksi, mengenal setiap pelanggan, dan tahu persis kondisi keuangan usahanya. Tapi kelemahannya, ketika usaha mulai agak besar—misalnya memiliki dua tiga karyawan atau buka cabang—penglihatan langsung ini mulai terbatas. Di sinilah kerangka formal mulai dibutuhkan, meskipun dalam bentuk yang sangat sederhana.



**Gambar 2.4:** Perbandingan fokus adaptasi risiko; di mana skala kecil lebih fokus pada keberlangsungan arus kas harian, sedangkan skala besar bergerak menuju integrasi strategi dan reputasi global

- **Pertama, soal identifikasi risiko.**

Untuk perusahaan kecil, risikonya biasanya terpusat di tiga area: kelangsungan usaha (bisakah toko tetap buka setiap hari?), arus kas (cukup tidak uang buat beli stok?), dan pelanggan (mereka bayar tepat waktu tidak?). Ini semua bisa diidentifikasi tanpa bantuan konsultan. Cukup dengan duduk sebentar di akhir bulan sambil ngopi, lalu bertanya: "Apa saja yang membuat saya pusing bulan ini?" Dari situ, risiko-risiko utama akan muncul sendiri.

Penelitian tentang penerapan ISO 31000 pada perusahaan dagang ABC Computer menunjukkan bahwa pendekatan sederhana ini bisa sangat efektif. Dalam studi itu, mereka mengidentifikasi bahwa faktor manusia ternyata menjadi sumber risiko tertinggi, sementara risiko dari lingkungan dan infrastruktur justru rendah. Ini pelajaran penting. Untuk perusahaan kecil, orang-orang di dalamnya—baik pemilik maupun karyawan—adalah sumber risiko terbesar sekaligus sumber solusi terbaik.

- **Kedua, soal analisis dan evaluasi risiko.**

Perusahaan kecil tidak perlu membuat matriks risiko yang rumit dengan skala 5x5 atau analisis statistik yang membuat pusing. Cukup dengan kategorisasi sederhana: risiko yang bisa membuat toko tutup besok (prioritas satu), risiko yang membuat rugi tapi masih bisa jalan (prioritas dua), dan risiko yang mengganggu tapi tidak fatal (prioritas tiga). Prioritaskan yang pertama, pikirkan yang kedua, catat yang ketiga.

- **Ketiga, soal perlakuan risiko.**

Di sinilah kreativitas pemilik kecil seringkali lebih unggul dari perusahaan besar. Karena mereka terbiasa hidup dengan keterbatasan, solusi yang ditemukan seringkali sederhana tapi efektif. Misalnya, untuk risiko kehabisan stok, mereka bisa membuat catatan sederhana di buku tulis tentang pola pembelian pelanggan. Untuk risiko piutang macet, mereka batasi jumlah utang maksimal per pelanggan atau terapkan sistem "utang hari ini, bayar besok lusa" yang ketat.

Salah satu instrumen yang kini mulai banyak dilirik UMKM adalah asuransi. Tapi tantangannya, banyak UMKM merasa biaya premi menjadi beban tambahan yang memberatkan. Padahal, produk seperti asuransi pengiriman (cargo insurance) dan asuransi kredit perdagangan (trade credit insurance) bisa menjadi pelindung yang sangat efektif. Pemerintah pun sebenarnya mulai mendorong ini, karena kontribusi UMKM terhadap ekspor nasional yang masih rendah—baru 15,7 persen di tahun 2023—salah satunya disebabkan oleh ketakutan menghadapi risiko perdagangan internasional.

- **Keempat, soal pemantauan.**

Untuk perusahaan kecil, pemantauan paling efektif adalah dengan rutin—misalnya setiap minggu—melihat kembali catatan-catatan sederhana itu. Apakah ada pelanggan yang mulai menunggak lebih dari batas? Apakah ada supplier yang mulai sering telat? Apakah ada produk yang mulai jarang laku? Ini semua adalah indikator dini yang bisa langsung direspons.

### **Yang Besar Butuh Struktur: Adaptasi untuk Perusahaan Dagang Skala Menengah**

Ketika perusahaan mulai membesar—mungkin sudah memiliki beberapa cabang, karyawan puluhan, dan transaksi ratusan per hari—pendekatan sederhana tadi mulai tidak cukup. Di sinilah kerangka seperti COSO ERM mulai relevan untuk diadopsi secara lebih utuh. Penelitian pada Narma Toserba, sebuah perusahaan ritel, menunjukkan bagaimana COSO ERM bisa diterapkan untuk mengevaluasi pengendalian internal, khususnya di siklus pembelian. Dengan delapan komponen COSO ERM versi lama—*internal environment*, *objective setting*, *event identification*, *risk assessment*, *risk response*, *control activities*, *information and communication*, dan *monitoring*—mereka bisa melihat secara sistematis bagian mana dari proses pembelian yang masih lemah.

Hasilnya menarik. Narma Toserba sebenarnya sudah memiliki sistem informasi akuntansi yang baik. Tapi ternyata masih ada kekurangan di kebijakan dan prosedur. Ini menunjukkan bahwa perusahaan menengah seringkali sudah memiliki infrastruktur, tapi

belum memiliki disiplin proses yang konsisten. Dengan evaluasi berbasis COSO ERM, mereka bisa melihat celah-celah yang selama ini tidak kelihatan.

Penelitian lain di PT XYZ, sebuah perusahaan dagang dan distribusi peralatan industri, menggunakan COSO ERM 2017 yang lebih baru dengan lima komponen dan dua puluh prinsipnya. Hasilnya, meskipun perusahaan sudah memiliki struktur organisasi dan kebijakan yang mendukung manajemen risiko, masih banyak kelemahan. Mereka tidak memiliki komite audit atau komite risiko, tidak memiliki dokumen formal tentang selera risiko (*risk appetite*), dan implementasi respons risiko masih belum lengkap. Yang paling menarik, fungsi manajemen risiko di perusahaan ini tidak pernah dinilai oleh pihak independen dan tidak memiliki sistem pelaporan pelanggaran (*whistleblowing system*).

Ini pelajaran penting untuk perusahaan menengah yang sedang bertumbuh. Seringkali, yang kurang bukanlah kemauan, tapi formalitas dan struktur. Padahal, di sinilah letak perbedaan antara manajemen risiko yang sekadar "ada" dan yang benar-benar efektif. Dokumen formal tentang selera risiko, misalnya, bukan sekadar ceremonial. Ia menjadi acuan bagi semua karyawan tentang seberapa jauh mereka boleh mengambil risiko dalam menjalankan tugas sehari-hari. Tanpa itu, keputusan jadi inkonsisten, tergantung siapa yang memutuskan dan bagaimana suasana hatinya hari itu.

### **Yang Besar Harus Terintegrasi: Adaptasi untuk Korporasi Dagang Skala Besar**

Sekarang kita melompat ke level tertinggi: korporasi dagang besar dengan skala nasional bahkan multinasional. Di level ini, manajemen risiko tidak bisa lagi hanya diurus oleh satu orang atau satu departemen. Ia harus terintegrasi ke dalam seluruh proses bisnis, dari hulu ke hilir, dari lini terdepan hingga ruang rapat direksi. Di sinilah konsep *Enterprise Risk Management* (ERM) menjadi relevan. Bukan lagi sekadar mengelola risiko masing-masing departemen secara terpisah, tapi melihat portofolio risiko perusahaan secara keseluruhan. Bagaimana risiko di bagian pembelian berinteraksi dengan risiko di bagian penjualan? Bagaimana risiko pasar di luar negeri mempengaruhi strategi ekspansi domestik? Pertanyaan-pertanyaan ini hanya bisa dijawab kalau manajemen risiko sudah terintegrasi.

Skala identifikasi seperti ini hanya mungkin dilakukan oleh perusahaan besar dengan sumber daya memadai. Tapi justru di situlah tantangannya. Semakin banyak risiko yang diidentifikasi, semakin besar risiko untuk tenggelam dalam detail. Tanpa sistem yang baik, tim manajemen risiko bisa sibuk terus menerus memetakan risiko kecil, sementara risiko besar yang bisa menjatuhkan perusahaan luput dari perhatian.

Oleh karena itu, perusahaan besar perlu membangun budaya sadar risiko di semua level. Bukan hanya tugas manajer risiko, tapi semua karyawan harus paham bahwa mereka adalah "*risk owners*" di area masing-masing. Staf gudang harus paham risiko salah catat stok. Staf penjualan harus paham risiko memberikan diskon terlalu besar. Staf keuangan harus paham risiko fluktuasi kurs. Di level kebijakan publik, pemerintah Indonesia bahkan sedang mengembangkan Indonesia *Single Risk Management* (ISRM) untuk mengintegrasikan profil risiko pelaku usaha dari hulu ke hilir. Sistem ini diharapkan menjadi solusi atas ego sektoral antar kementerian/lembaga yang selama ini menghambat kelancaran arus barang. Bayangkan, sebuah perusahaan sudah mendapat status *Authorized Economic Operator* (AEO)

dari Bea Cukai—artinya profil risikonya rendah—tapi ketika urusan perizinan di kementerian teknis, mereka diperlakukan seperti perusahaan berisiko tinggi. Inilah yang disebut Ketua Umum Asosiasi Perusahaan Jalur Prioritas sebagai disparitas penilaian risiko yang membebani ongkos logistik. Ini menunjukkan bahwa bahkan di level paling atas sekalipun, integrasi manajemen risiko masih menghadapi tantangan berat. Tapi justru di situlah urgensinya. Semakin besar perusahaan, semakin kompleks pula risikonya, dan semakin besar pula kebutuhan untuk mengelola risiko secara terintegrasi.

### **Spektrum Adaptasi: Dari yang Paling Sederhana hingga Paling Canggih**

Jadi, kalau kita tarik benang merah dari diskusi panjang ini, adaptasi kerangka risiko untuk perusahaan dagang itu seperti spektrum warna. Di ujung paling sederhana, ada perusahaan kecil yang cukup dengan catatan di buku tulis dan ingatan pemilik. Di tengah, ada perusahaan menengah yang mulai butuh struktur formal dan evaluasi berkala. Di ujung paling canggih, ada korporasi besar yang mengintegrasikan manajemen risiko ke dalam semua proses bisnis, dengan dukungan sistem informasi dan sumber daya manusia khusus.

Yang penting, tidak ada level yang lebih baik dari yang lain. Yang terpenting adalah kecocokan. Jangan paksakan perusahaan kecil menggunakan COSO ERM dengan dua puluh prinsipnya, karena yang terjadi bukan manajemen risiko yang efektif, tapi birokrasi yang membebani. Sebaliknya, jangan biarkan perusahaan besar mengelola risiko dengan cara-cara sederhana yang tidak lagi memadai untuk kompleksitas yang mereka hadapi. Di sinilah peran penting pemahaman tentang konteks organisasi. Sebelum menentukan kerangka mana yang akan digunakan dan bagaimana mengadaptasinya, setiap perusahaan harus paham betul siapa dirinya: seberapa besar, seberapa kompleks, di industri apa, dengan budaya seperti apa, dan menghadapi risiko apa. Dari situ, barulah dirancang sistem manajemen risiko yang pas—tidak kurang, tidak lebih.



**Gambar 2.5:** Siklus manajemen risiko persediaan yang meliputi perencanaan, pengadaan, penyimpanan, hingga penjualan, menunjukkan titik-titik kritis di mana kerugian sering kali terjadi tanpa disadari.

## KESIMPULAN

Adaptasi kerangka risiko dalam bisnis dagang bukanlah tentang menyalin standar global secara buta, melainkan menyesuaikan "kedalaman" pengawasan dengan kompleksitas operasional. Dari toko kecil yang berbasis kepercayaan hingga korporasi besar dengan sistem ERM yang canggih, keberhasilan mitigasi bergantung pada kemampuan organisasi menyinergikan data teknis dengan intuisi manusiawi di lapangan.

## LATIHAN SOAL

1. Banyak manajer tingkat menengah merasa bahwa implementasi Enterprise Risk Management (ERM) hanya menambah beban administratif dan memperlambat pengambilan keputusan. Jika kita berada di posisi Direktur Risiko, bagaimana cara nya menjelaskan kepada mereka bahwa ERM justru merupakan "rem" yang memungkinkan mobil perusahaan melaju lebih kencang, bukan malah menghentikannya?
2. ISO 31000 sering disebut lebih "luwes" dibandingkan COSO ERM yang cenderung "struktural dan auditif". Dalam kondisi pasar yang sangat fluktuatif dan penuh disrupsi teknologi (seperti munculnya kompetitor berbasis AI), mazhab mana yang menurut kita lebih cocok diterapkan oleh perusahaan dagang retail? Berikan alasan logisnya.
3. Jelaskan mengapa integrasi antara tata kelola perusahaan (*Corporate Governance*) dengan ERM dianggap sebagai "kecerdasan kolektif" organisasi. Apa dampaknya bagi kepercayaan investor jika kedua hal ini berjalan sendiri-sendiri?

## BAB 3

# TRANSFORMASI DIGITAL DAN PERAN AI DALAM MANAJEMEN RISIKO

---

Bagaimana teknologi mengubah cara perusahaan mengenali, memantau, dan merespons risiko?

### CAPAIAN PEMBELAJARAN

- Menjelaskan evolusi digitalisasi perdagangan.
- Membedakan AI, machine learning, dan deep learning.
- Menganalisis perubahan pola identifikasi risiko.
- Menilai manfaat AI bagi keputusan berbasis data.
- Mengidentifikasi tantangan implementasi AI.

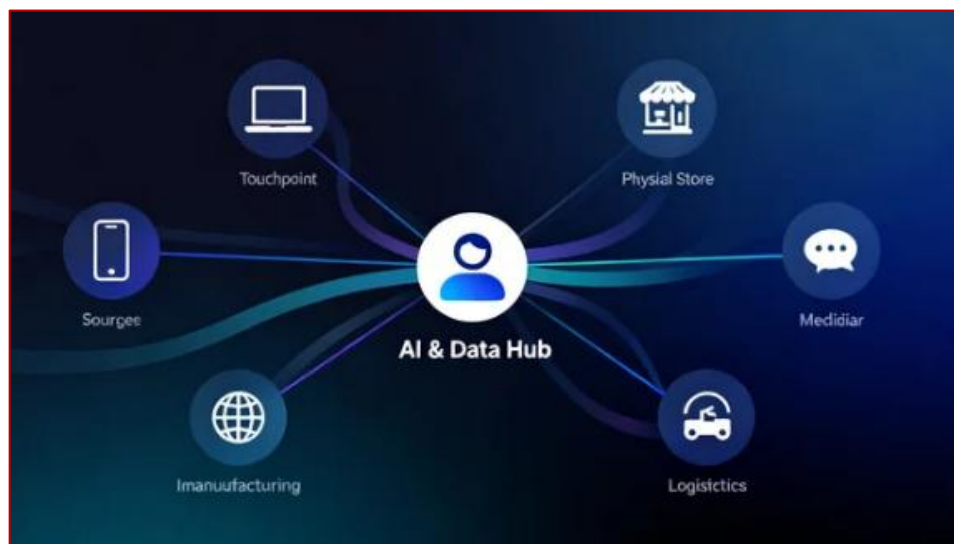
### 3.1 EVOLUSI DIGITALISASI DALAM BISNIS PERDAGANGAN

Pernahkah kita membayangkan, bagaimana rasanya jadi pedagang di era sekarang? Bukan hanya soal berjualan barang, tapi harus paham teknologi, memahami algoritma, bisa membuat konten, dan yang paling membuat pusing harus tetap waras di tengah perubahan yang datangnya cepet sangat. Dulu, jadi pedagang itu cukup memiliki modal, tempat strategis, dan kemampuan nawar yang oke. Sekarang? berjualan bisa dari kamar, pakai live streaming, target pasar bisa seluruh Indonesia bahkan dunia. Tapi di balik kemudahan itu, ada tantangan yang tidak kalah besarnya.

perubahan inilah yang disebut sebagai evolusi digitalisasi dalam bisnis perdagangan. Istilahnya mungkin terdengar berat dan akademis. Tapi kalau kita berdiskusi santai, sebenarnya ini cerita tentang bagaimana teknologi mengubah cara kita berdagang, dari warung kelontong sampai korporasi raksasa, dan bagaimana mereka semua berusaha tetap bertahan di tengah ombak perubahan yang tidak pernah berhenti.

#### Memahami Digitalisasi Perdagangan: Bukan Sekadar berjualan Online

Sebelum kita masuk lebih dalam, kita harus sepakat dulu soal satu hal. Digitalisasi perdagangan itu bukan sekadar pindah berjualan dari toko fisik ke lapak online. Lebih dari itu, ini adalah perubahan fundamental dalam seluruh ekosistem bisnis. Wakil Menteri Perdagangan RI, Dyah Roro Esti, dalam sebuah forum internasional di Kuala Lumpur pada Oktober 2025, menjelaskan bahwa digitalisasi telah menciptakan model kerja baru dan menggeser transaksi dari cara tradisional menjadi transaksi melalui platform digital seperti *e-commerce* dan live shopping. Ini bukan perubahan kecil. Ini pergeseran peradaban dagang.



**Gambar 3.1** Transformasi rantai nilai retail dari model linier tradisional ke ekosistem digital yang terintegrasi, menunjukkan bagaimana data mengalir di setiap titik sentuh konsumen

Di Indonesia sendiri, adaptasi terhadap digitalisasi ini berjalan sangat cepat. Data dari Kementerian Perdagangan menunjukkan bahwa hingga tahun 2024, mereka telah mendorong digitalisasi di 5.419 pasar tradisional dan melibatkan 304.135 pedagang. Bayangkan, ratusan ribu pedagang yang tadinya hanya tahu transaksi tunai dan tatap muka, kini mulai akrab

dengan scan barcode, transfer bank, dan promo online. Ini kerja besar yang tidak bisa diremehkan.

Tapi yang lebih menarik, Wamendag juga menyebut bahwa pemerintah melakukan berbagai upaya untuk mendukung adaptasi ini, mulai dari membuat regulasi yang adil bagi konsumen dan pelaku usaha, memberikan pelatihan bagi UMKM tentang cara menggunakan platform digital, hingga menyediakan *platform InaExport.id* yang menghubungkan pelaku usaha dengan pembeli luar negeri. Sepanjang Januari-Agustus 2025 saja, *platform* ini berhasil memfasilitasi 462 *business matching daring*, menghubungkan 1.482 UMKM dengan calon pembeli global, dan mencapai potensi transaksi 90,9 juta dolar AS. Ini bukti bahwa digitalisasi perdagangan bukan wacana, tapi sudah berjalan dan membuahkan hasil.

#### **Evolusi Model Bisnis: Dari Konvensional ke Digital**

untuk memahami lebih dalam, kita perlu lihat bagaimana model bisnis itu sendiri berevolusi. Artikel dari Telkom University menjelaskan dengan sangat gamblang tentang transisi dari model bisnis tradisional menuju model bisnis digital. Model bisnis tradisional, menurut artikel itu, mengandalkan metode konvensional untuk transaksi, distribusi, dan layanan pelanggan. Contohnya? Manufaktur, ritel fisik, dan layanan berbasis lokasi yang mengharuskan pelanggan datang langsung. Sistem ini menggunakan saluran distribusi konvensional, seperti toko fisik, yang terhubung ke rantai pasokan kompleks. Masalahnya? Biaya operasional tinggi. Perusahaan butuh ruang ritel besar, tenaga kerja banyak, dan sistem logistik rumit. Plus, ketergantungan pada transaksi tatap muka membatasi jangkauan pasar.

Model bisnis digital hadir sebagai solusi. Digitalisasi bisnis bukan hanya penggunaan internet, tapi juga berbagai inovasi teknologi yang memungkinkan pengusaha merancang ulang proses bisnis mereka. Model ini memungkinkan akses ke pasar global yang lebih besar, personalisasi layanan, dan peningkatan efisiensi melalui otomatisasi sistem.

#### **Artikel Telkom University menyebutkan empat dampak utama digitalisasi terhadap model bisnis:**

- Pertama, akses ke pasar lebih luas. Perusahaan bisa menjual produk ke konsumen di seluruh dunia melalui *platform e-commerce*. Ini membuka peluang baru yang sebelumnya tidak terbayangkan.
- Kedua, personalisasi pengalaman pelanggan. Dengan teknologi seperti analitik data dan kecerdasan buatan, perusahaan bisa memberikan rekomendasi produk yang relevan berdasarkan preferensi dan perilaku pelanggan. Ini meningkatkan kepuasan dan loyalitas.
- Ketiga, penurunan biaya operasional. Otomatisasi dan *platform* digital memungkinkan perusahaan beroperasi lebih efisien, mengurangi pemborosan sumber daya, dan meningkatkan profitabilitas.
- Keempat, kemampuan adaptasi cepat. Digitalisasi memungkinkan bisnis merespons perubahan pasar dengan lebih cepat. Mereka bisa memantau tren secara *real-time* dan mengubah strategi seketika.

Contoh perusahaan yang berhasil beralih ke model bisnis digital? Amazon, Netflix, dan Uber. Mereka adalah ikon transformasi digital yang mengubah cara dunia berbelanja, menonton, dan bepergian.



**Gambar 3.2** Otomasi gudang dan logistik dalam perdagangan modern sebagai hasil dari evolusi digital, yang mempercepat pengiriman namun meningkatkan kompleksitas manajemen asset

### Tahapan Transformasi Digital: Jalan Panjang Menuju Modernisasi

Tapi transformasi digital tidak terjadi dalam semalam. Ada proses panjang yang harus dilalui. Artikel Telkom *University* memaparkan beberapa tahapan penting:

- Pertama, evaluasi teknologi yang tersedia. Perusahaan harus memilih platform *e-commerce*, alat analitik data, dan perangkat lunak yang bisa meningkatkan efisiensi operasional.
- Kedua, konstruksi infrastruktur digital. Ini termasuk membangun situs web, aplikasi mobile, dan sistem berbasis cloud yang memungkinkan seluruh bagian bisnis terhubung.
- Ketiga, pengintegrasian proses dan sistem. Sistem yang ada seperti keuangan dan manajemen inventaris harus bisa terintegrasi dengan platform digital secara otomatis.
- Keempat, pelatihan manajer dan karyawan. Ini yang sering dilupakan. Teknologi secanggih apa pun, kalau manusianya tidak siap, percuma. Perubahan budaya perusahaan adalah prasyarat mutlak.
- Kelima, strategi pemasaran online. Ini mencakup penggunaan media sosial, *search engine optimization* (SEO), dan kampanye iklan digital untuk menjangkau audiens lebih besar.

kalau kita perhatikan, tahapan-tahapan ini sejalan dengan temuan di lapangan. Penelitian di Pasar Kahayan, Palangka Raya, misalnya, menunjukkan bahwa digitalisasi telah mengubah dinamika sosial-ekonomi pedagang pakaian. Para pedagang terpaksa mengadopsi strategi

bertahan hidup menurunkan harga, mengurangi biaya operasional, mengubah jenis dagangan, dan menyesuaikan jam buka. Yang menarik, pedagang yang lebih tua cenderung menggunakan strategi lebih pasif karena keterbatasan akses dan pemahaman terhadap teknologi digital. Ini membuktikan bahwa transformasi digital bukan hanya soal teknologi, tapi juga soal kesiapan manusia dan budaya.

### **Teknologi Modern dalam Perdagangan: AI, OMS, dan Digital Twin**

Kalau kita bicara evolusi digitalisasi di level yang lebih canggih terutama untuk perusahaan besar topiknya jadi makin seru. Di tahun 2025 ini, teknologi perdagangan berkembang dengan kecepatan yang mencengangkan. Artikel dari Harrington Starr, sebuah konsultan teknologi finansial, mengidentifikasi empat tren utama yang membentuk masa depan teknologi perdagangan: modernisasi, *modular deployment*, *data-driven OMS*, dan integrasi AI.

Modernisasi menjadi keniscayaan. Banyak perusahaan masih bergantung pada infrastruktur usang yang tidak dirancang untuk kompleksitas perdagangan modern. Padahal, biaya kelambanan (*cost of inaction*) makin tinggi. Perusahaan yang ragu memodernisasi sistemnya akan tertinggal, menghadapi pengawasan regulator lebih ketat, dan kehilangan pangsa pasar. *Modular system deployment* menawarkan pendekatan strategis. Alih-alih merombak total sistem yang berisiko tinggi, perusahaan bisa mulai dengan proyek-proyek kecil meningkatkan algoritma eksekusi, menyempurnakan order routing, atau menerapkan alat manajemen risiko baru. Pendekatan ini memungkinkan mereka melihat manfaat langsung sambil belajar dan beradaptasi.

*Data-driven OMS (Order Management System)* menjadi pusat saraf baru. OMS modern bukan sekadar alat eksekusi order, tapi pusat pemrosesan data, agregasi, dan pengambilan keputusan. Dengan OMS yang canggih, perusahaan bisa meningkatkan kualitas eksekusi melalui analitik prediktif berbasis AI, meningkatkan efisiensi operasional dengan mengotomatiskan alur kerja perdagangan dan pemantauan kepatuhan, serta mendapatkan wawasan pasar lebih dalam melalui integrasi data pasar dan transaksi. Yang paling penting, teknologi sekarang mendukung bisnis, bukan sebaliknya bisnis harus bekerja mengelilingi keterbatasan *platform*. Integrasi AI dan ML menjadi standar industri, bukan lagi sekadar keunggulan kompetitif. Beberapa penggunaan AI dalam perdagangan meliputi:

- *Smart Order Routing*: algoritma eksekusi yang menyesuaikan aliran order secara dinamis berdasarkan kondisi pasar *real-time*.
- *Trade Surveillance*: model ML yang mendeteksi anomali dan potensi penyalahgunaan pasar, mengurangi risiko kepatuhan.
- *Predictive Market Analytics*: alat peramalan bertenaga AI yang membantu pedagang mengantisipasi pergerakan harga dan pergeseran likuiditas.
- *Automated Risk Management*: analisis *real-time* terhadap eksposur perdagangan, mengoptimalkan efisiensi modal.

Tapi yang perlu digarisbawahi, AI tidak menggantikan manusia. Perusahaan yang berhasil menggunakan AI justru mereka yang bisa menyeimbangkan antara penilaian manusia dan kecerdasan buatan. Terutama untuk alur kerja kepatuhan dan regulasi, jawaban "itu

keputusan model" tidak akan diterima regulator. Perusahaan harus bisa mendokumentasikan maksud di balik setiap strategi dan menyediakan audit trail yang jelas.

Salah satu inovasi paling menarik adalah digital twin. Coupa, perusahaan teknologi *supply chain*, membangun alat yang memungkinkan klien memodelkan skenario tarif alternatif dan menilai dampaknya terhadap biaya dan risiko. Dean Bain, SVP *supply chain* Coupa, menjelaskan bahwa fokus saat ini adalah membangun ketahanan dan kelincahan dalam rantai pasok. Perusahaan melakukannya dengan membangun digital twin operasi mereka model dinamis bertenaga AI yang bisa mensimulasikan gangguan dan merekomendasikan respons secara *real-time*.

Bayangkan, perusahaan bisa bertanya, "Apa yang terjadi kalau tarif impor naik 25 persen?" dan mendapatkan jawaban dalam hitungan jam, bukan minggu. Inilah yang disebut Bain sebagai "kemampuan untuk mengidentifikasi opsi sumber alternatif dan menggunakan data untuk membuat keputusan berbasis data yang pada akhirnya melindungi profitabilitas dan posisi pasar perusahaan".

#### **Pedang Bermata Dua: Risiko di Balik Kemudahan Digital**

Tapi jangan buru-buru terpesona. Digitalisasi itu seperti pedang bermata dua. Di satu sisi memberi kemudahan, di sisi lain menyimpan risiko yang tidak kalah tajam. Sebuah artikel di antara dengan judul "Pedang bermata dua *e-commerce* untuk UMKM" mengupas tuntas sisi gelap digitalisasi. *Onboarding* digital UMKM, yang selama ini digaungkan sebagai jalan pintas naik kelas, ternyata bisa menjadi jebakan.

Ketergantungan berlebihan pada satu *platform* adalah risiko utama. Perubahan algoritma di *platform marketplace* sering membawa dampak besar bagi penjual yang bergantung pada visibilitas produk mereka. Artikel itu memberikan beberapa contoh menarik:

- Etsy pada 2019, memprioritaskan produk dengan pengiriman gratis dan peringkat tinggi. Penjual kecil dengan margin tipis yang tidak bisa menawarkan pengiriman gratis langsung kehilangan visibilitas dan penjualan.
- Amazon pada 2018, mengubah algoritmanya untuk memprioritaskan produk dengan margin keuntungan lebih tinggi untuk Amazon sendiri. Banyak penjual mandiri kehilangan posisi di halaman pertama pencarian meskipun memiliki ulasan bagus.
- eBay pada 2017, mempromosikan produk dengan harga kompetitif dan pengiriman cepat, berdampak pada penjual barang antik dan koleksi yang unik tapi mahal.

Fenomena ini menunjukkan bahwa kesuksesan instan di *platform* digital bisa berubah jadi petaka dalam semalam. Ketika algoritma berubah, pedagang kecil kehilangan visibilitas. Ketika *platform* menaikkan biaya layanan atau komisi, margin keuntungan yang sudah tipis makin tergerus. Kasus pedagang yang tiba-tiba kehilangan akun tanpa alasan jelas atau tidak memiliki akses menegosiasikan kebijakan platform semakin sering terjadi.

Yang lebih mengkhawatirkan, ketergantungan ini mengikis kemampuan UMKM membangun hubungan langsung dengan konsumen. Sebagian besar pelanggan di *platform e-commerce* adalah "milik" *platform*, bukan pedagangnya. Data konsumen, analisis perilaku, hingga strategi pemasaran terisolasi di dalam ekosistem platform, meninggalkan UMKM tanpa kendali atas aset terpenting: pelanggan.

Risiko lain yang tidak kalah penting adalah keamanan data pribadi dan transaksi keuangan. Kepala Badan Pengembangan Sumber Daya Manusia Kementerian Komunikasi dan Digital, Bonifasius Wahyu Pudjianto, mengingatkan bahwa di balik kemudahan digitalisasi, ancaman terhadap data pribadi menjadi risiko yang harus diantisipasi. Ini bukan main-main. Kebocoran data bisa menghancurkan reputasi dan kepercayaan pelanggan.

### **Membangun Ketahanan di Era Digital: Strategi untuk Semua Skala**

Lalu, bagaimana cara menghadapi semua ini? Adaptasi kerangka manajemen risiko menjadi kunci. Untuk UMKM, strateginya bisa sederhana: diversifikasi saluran distribusi. Jangan bergantung pada satu *platform*. Buka toko di beberapa *marketplace*, bangun media sosial, kalau bisa memiliki website sendiri. Dengan begitu, ketika satu *platform* berubah algoritma, masih ada yang lain. Untuk perusahaan menengah, pendekatan modular *system deployment* seperti yang dijelaskan Harrington Starr bisa jadi pilihan. Mulai dari proyek kecil misalnya, meningkatkan algoritma eksekusi atau menerapkan alat manajemen risiko baru lalu pelan-pelan memperluas. Ini mengurangi risiko gangguan operasional.

Untuk perusahaan besar, integrasi sistem menjadi keharusan. Harmonisasi data di seluruh *Order Management System* (OMS), *Execution Management System* (EMS), dan *Transaction Cost Analysis* (TCA) menciptakan alur kerja tunggal yang transparan dari pra-perdagangan hingga pasca-perdagangan. Konsistensi data di ketiga sistem adalah kunci. Data yang dilihat sebelum perdagangan harus sesuai dengan catatan pasca-perdagangan, tanpa perlu rekonsiliasi manual atau entri data berulang. Yang tidak kalah penting, bangun budaya sadar risiko digital di semua level organisasi. Setiap karyawan harus paham bahwa keamanan siber adalah tanggung jawab bersama, bukan hanya tugas tim IT. Pelatihan rutin tentang phishing, keamanan kata sandi, dan praktik digital aman menjadi investasi jangka panjang yang tidak boleh diabaikan.

## **3.2 KONSEP DASAR ARTIFICIAL INTELLIGENCE DAN MACHINE LEARNING**

Pernahkah, kita lagi asyik berdiskusi di kantin kampus, lalu tiba-tiba topiknya lari ke hal-hal yang agak berat? Misalnya, teman nanya, "kita sering mendengar istilah AI dan *Machine Learning*, tapi sebenarnya bedanya apa? Terus, kok bisa ya mesin belajar?" Pertanyaan itu, kalau dipikir-pikir, sebenarnya sederhana tapi juga dalam sangat. Karena di baliknya, ada rasa penasaran tentang bagaimana sebuah benda mati komputer, server, kode program bisa melakukan hal-hal yang dulu kita anggap hanya bisa dilakukan manusia. daripada bingung sendiri, lebih baik kita bahas pelan-pelan. Seperti diskusi santai di ruang kuliah yang tidak kaku-kaku amat, tapi tetap ngalir dengan kedalaman yang layak. Soalnya, topik ini bukan hanya soal teknologi, tapi juga soal bagaimana kita memandang kecerdasan, pembelajaran, dan masa depan pekerjaan kita sendiri.

### **Memahami "Akar" dari Segalanya: *Artificial Intelligence***

Sebelum kita masuk ke cabang-cabangnya, kita harus sepakat dulu soal akarnya. *Artificial Intelligence* (AI) atau Kecerdasan Buatan itu sebenarnya apa? Kalau kita buka buku "Kecerdasan Buatan: Teori, Algoritma, dan Aplikasi" yang diterbitkan Yayasan Tri Edukasi Ilmiah pada tahun 2024, di situ dijelaskan bahwa AI dimulai dengan konsep dasar, sejarah, dan

prinsip-prinsip yang mendasari teknologi ini. Buku ini memandu pembaca untuk memahami berbagai algoritma kunci yang menjadi fondasi AI, seperti *machine learning*, *deep learning*, dan *neural networks*.

Tapi, definisi yang lebih bumi dan mudah dicerna datang dari buku "Artificial Intelligence: Konsep, potensi masalah, hingga pertanggungjawaban pidana" karya I Gusti Kade Budhi. Dalam buku yang diterbitkan tahun 2025 ini, penulisnya dengan gamblang menyatakan bahwa AI adalah simulasi dari kecerdasan yang dimiliki oleh manusia yang dimodelkan di dalam mesin dan diprogram agar bisa berpikir seperti halnya manusia. Definisi ini penting karena menekankan dua hal: simulasi (artinya dia tiruan, bukan asli) dan berpikir seperti manusia (artinya tujuannya adalah meniru cara kerja pikiran kita).

Menariknya, buku Budhi ini tidak hanya bicara soal konsep teknis, tapi juga membahas potensi masalah dan pertanggungjawaban pidana terkait penggunaan AI. Ini memberikan kita gambaran bahwa diskusi tentang AI sudah bergeser dari "bisa apa tidak?" ke "kalau salah, siapa yang tanggung jawab?" sebuah pertanyaan yang jauh lebih rumit. Untuk melengkapi pemahaman kita, ada juga buku "*Artificial Intelligence* (Teori, Konsep, dan Implementasi di Berbagai Bidang)" yang ditulis oleh tim dosen dan peneliti, diterbitkan PT Sonpedia Publishing Indonesia tahun 2025. Buku ini membahas AI dari pengantar, komponen utama seperti penalaran, pembelajaran, dan persepsi, serta algoritma dasar yang meliputi *machine learning* dan *deep learning*. Yang menarik, buku ini juga menyentuh dimensi etis dan tantangan dalam pengembangan AI, termasuk isu privasi, bias algoritma, dan tanggung jawab sosial. Jadi, sejak awal, para ahli di Indonesia sudah mengingatkan bahwa AI bukan sekadar teknologi netral; ia memiliki konsekuensi sosial yang harus dipikirkan.

### **Cabang Paling Penting: Memahami Machine Learning**

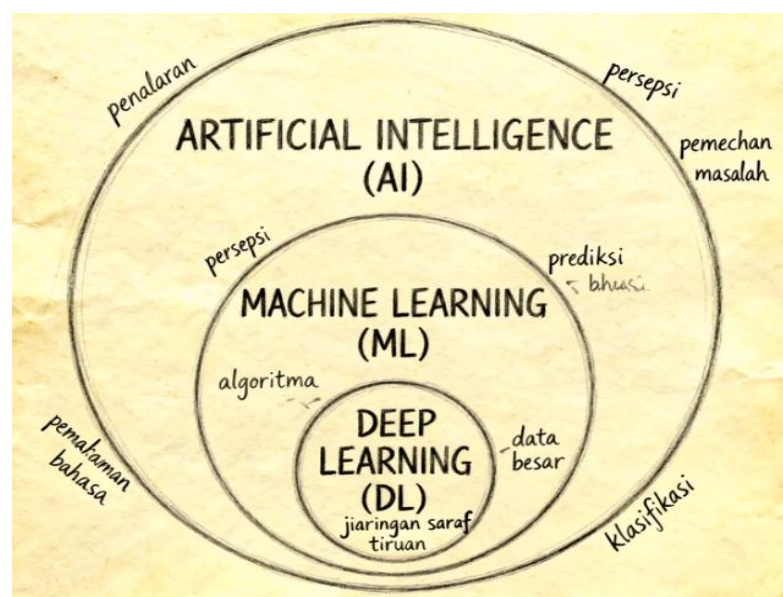
Kalau AI itu adalah "kecerdasannya", maka *Machine Learning* (ML) atau Pembelajaran Mesin adalah "cara" untuk mencapai kecerdasan itu. Ibarat kita mau jadi orang cerdas, AI-nya adalah "kepinterannya", sedangkan ML adalah "proses belajarnya". Tanpa ML, AI itu mungkin hanya bisa melakukan tugas-tugas yang sudah diprogram secara kaku. Tapi dengan ML, dia bisa belajar dari pengalaman. Buku "*Machine Learning*" karya Ade Mulyana, Yanto Hermawan, dan Isnan Mulia yang diterbitkan Kesatuan Press tahun 2025, memberikan definisi yang sangat komprehensif. Buku ini dirancang sebagai panduan bagi mahasiswa, akademisi, dan praktisi yang ingin memahami konsep dasar, algoritma, serta penerapan ML di dunia nyata.

Dalam buku itu dijelaskan, ML dimulai dengan fundamental, termasuk konsep pembelajaran terawasi (*supervised learning*), tidak terawasi (*unsupervised learning*), dan penguatan (*reinforcement learning*). Tiga paradigma ini adalah fondasi dari hampir semua yang kita kenal sebagai "kecerdasan" dalam mesin saat ini. Penjelasan detailnya nanti kita bahas, tapi yang perlu dicatat dulu, ML adalah tentang bagaimana komputer belajar dari data tanpa perlu diprogram secara eksplisit untuk setiap tugas.

Buku "*Machine Learning Untuk Big Data dan Artificial Intelligence (AI)*" yang diterbitkan PT. Surya Digital Nusantara tahun 2025, melengkapi pemahaman ini dengan menghubungkan ML dengan konteks yang lebih besar: *Big Data*. Di era digital sekarang, data melimpah ruah. Tapi data saja tidak berarti kalau tidak bisa diolah. Di sinilah ML berperan ia

mengubah data mentah menjadi pengetahuan bernilai melalui proses analisis, prediksi, dan otomatisasi cerdas. Buku ini membahas teknik klasifikasi, prediksi, *clustering*, serta penerapan algoritma populer seperti *Decision Tree*, *Naïve Bayes*, dan *Neural Network*.

ML itu bukan sekadar teori. Ada buku "Dasar-Dasar Menginterpretasikan Model *Machine Learning* dan Implementasinya Menggunakan *Python*" karya Heri, dkk., yang diterbitkan Gava Media tahun 2024, yang fokus pada bagaimana kita memahami dan menafsirkan model ML yang sudah kita buat. Ini penting sangat, karena seringkali model ML itu seperti "kotak hitam" dia memberikan jawaban, tapi kita tidak tahu kenapa dia menjawab begitu. Padahal, untuk keperluan audit, regulasi, dan kepercayaan, kita perlu bisa menjelaskan keputusan model.



**Gambar 3.3** Hierarki kecerdasan buatan yang menunjukkan bahwa *Machine Learning* adalah bagian inti dari AI, dan *Deep Learning* merupakan spesialisasi yang lebih mendalam di dalamnya.

### Tiga Pilar Machine Learning: Cara Mesin "Belajar"

sekarang kita bedah satu per satu tiga paradigma utama dalam ML. Ini seru, karena dari sini kita bisa lihat bahwa "belajar" bagi mesin itu ternyata bisa dengan berbagai cara, mirip seperti manusia.

- Pertama, *Supervised Learning* atau Pembelajaran Terawasi. Ini adalah jenis pembelajaran di mana model dilatih menggunakan data berlabel. Artinya, kita sebagai manusia sudah memberikan jawaban yang benar terlebih dahulu. Misalnya, kita memiliki ribuan foto hewan. Setiap foto sudah kita beri label: "ini kucing", "ini anjing", "ini kelinci". Model ML akan mempelajari pola-pola dari foto-foto berlabel ini bentuk telinga, warna bulu, bentuk hidung, dan sebagainya lalu ketika kita kasih foto baru yang belum pernah dilihat, model akan menebak: "ini kemungkinan besar kucing".

Dalam artikel dari Sadasa Academy, dijelaskan bahwa contoh penerapan *supervised learning* yang paling klasik adalah penyaringan email spam. Model dilatih menggunakan dataset berupa contoh-contoh email yang sudah diberi label "spam" dan "bukan spam". Setelah belajar, model bisa memprediksi apakah email baru yang masuk itu masuk ke kotak masuk atau ke folder spam.

Buku "*Machine Learning*" dari Kesatuan Press menyebutkan bahwa algoritma yang termasuk *supervised learning* antara lain regresi linier, regresi logistik, *K-Nearest Neighbors*, *Decision Tree*, dan *Neural Networks*. Masing-masing memiliki cara kerja dan cocok untuk jenis masalah yang berbeda.

- Kedua, *Unsupervised Learning* atau Pembelajaran Tidak Terawasi. Nah, kalau yang ini modelnya dilatih menggunakan data tanpa label. Kita tidak kasih tahu jawabannya. Model harus menemukan sendiri pola dan struktur tersembunyi dari data.

Contohnya, kita kasih model ribuan data transaksi nasabah kartu kredit. Data itu berisi rata-rata nilai belanja, frekuensi transaksi, waktu transaksi, dan sebagainya. Tapi kita tidak kasih label "ini nasabah royal", "ini nasabah hemat", atau "ini nasabah berisiko". Model akan mencoba mengelompokkan sendiri nasabah-nasabah ini berdasarkan kesamaan ciri-ciri yang ditemukan. Hasilnya, mungkin dia akan menemukan kelompok nasabah dengan transaksi besar dan sering, kelompok dengan transaksi kecil tapi rutin, dan kelompok dengan transaksi tidak menentu. Setelah itu, barulah kita sebagai manusia bisa memberi nama pada kelompok-kelompok itu sesuai kebutuhan bisnis.

Buku "*Machine Learning Untuk Big Data*" menyebut teknik ini sebagai *clustering* atau pengelompokan. Ini sangat berguna untuk segmentasi pasar, rekomendasi produk, atau deteksi anomali.

- Ketiga, *Reinforcement Learning* atau Pembelajaran dengan Penguatan. Ini yang paling mirip dengan cara manusia belajar dari konsekuensi. Dalam paradigma ini, ada agen (entitas yang belajar) yang berinteraksi dengan lingkungan. Agen akan mencoba berbagai tindakan, dan lingkungan akan memberi umpan balik berupa *reward* (hadiah) atau *punishment* (hukuman). Tindakan yang menghasilkan *reward* positif cenderung akan diulang, sedangkan yang menghasilkan *reward* negatif akan dikurangi.

Contoh paling populer adalah agen AI yang belajar bermain game. Dia tidak tahu aturannya secara eksplisit. Dia coba gerak ke kiri, kena musuh, mati dapat *reward* negatif. Dia coba gerak ke kanan, ambil koin, skor naik dapat *reward* positif. Lama-lama, dia belajar strategi mana yang paling menguntungkan. Contoh lain adalah *self-driving vehicle* yang belajar bernavigasi di jalanan, atau agen yang bisa mempelajari strategi lawan dalam game strategi.

### Lebih Dalam Lagi: Memahami Deep Learning dan Neural Networks

Kalau kita sudah paham ML, kita bisa masuk ke level berikutnya: *Deep Learning* atau Pembelajaran Mendalam. *Deep Learning* ini adalah sub-bagian dari ML yang menggunakan jaringan saraf tiruan (*neural networks*) dengan banyak lapisan (*deep neural networks*). Identya adalah meniru cara kerja otak manusia, di mana jutaan neuron saling terhubung dan memproses informasi secara berlapis. Buku "Pemrograman AI & *Deep Learning*" yang diterbitkan Anak Hebat Indonesia tahun 2025, memberikan pemahaman komprehensif

tentang konsep, algoritma, serta implementasi *deep learning*. Buku ini memperkenalkan dasar-dasar jaringan saraf tiruan, optimasi model, hingga arsitektur canggih seperti CNN (*Convolutional Neural Network*) untuk gambar, RNN (*Recurrent Neural Network*) untuk data berurutan seperti teks atau *time series*, dan Transformer yang menjadi dasar model-model besar seperti GPT.

Salah satu aplikasi deep learning yang paling populer dan sering kita lihat adalah Generative AI untuk gambar. Artikel dari BINUS *University School of Computer Science* mengupas tuntas model-model generatif yang sedang tren di tahun 2025. Ada beberapa arsitektur utama di sini. *Variational Autoencoder* (VAE) adalah salah satu arsitektur generatif paling awal. Ia bekerja dengan mengompres gambar ke ruang laten lalu merekonstruksinya kembali, sehingga model mempelajari "peta" kemungkinan bentuk gambar yang realistis. Kemudian ada *Generative Adversarial Network* (GAN) yang membawa lompatan besar. Arsitektur ini terdiri dari dua pemain: generator yang berusaha menciptakan gambar palsu yang meyakinkan, dan *discriminator* yang bertugas membedakan mana gambar asli dan mana yang palsu. Proses kompetitif ini membuat generator terus mengasah kemampuan hingga bisa menghasilkan gambar yang tajam dan realistis. *StyleGAN*, misalnya, sangat populer untuk menghasilkan wajah manusia yang tampak nyata.

Yang terbaru dan paling canggih 43 opula *Diffusion Models*. Alih-alih langsung membentuk gambar, model ini memulai dari noise acak, lalu secara bertahap "membersihkan" noise tersebut sampai muncul gambar yang koheren. Keunggulannya 43opula stabilitas training dan kualitas visual yang sangat tinggi, terutama untuk gambar beresolusi besar dengan detail kompleks. Model-model 43 opular seperti DALL-E, *Stable Diffusion*, dan *Midjourney* menggunakan arsitektur ini.

### **Kenapa Semua Ini Penting untuk Dipahami?**

Mungkin di antara kita ada yang bertanya, "Oke, kita jadi paham definisi dan jenis-jenisnya. Tapi sebenarnya penting buat apa?"

- Pertama, karena teknologi ini sudah ada di sekitar kita, kadang tanpa kita sadari. Rekomendasi film di Netflix, filter spam di email, asisten virtual di ponsel, bahkan fitur *face unlock* semuanya menggunakan AI dan ML. Memahami dasarnya membantu kita tidak hanya jadi pengguna pasif, tapi juga pengguna kritis.
- Kedua, karena teknologi ini akan semakin merasuk ke dunia kerja kita, apapun profesinya. Akuntan, manajer, pengusaha, guru, dokter semua akan berinteraksi dengan AI dalam berbagai bentuk. Memahami konsep dasarnya membantu kita beradaptasi dan bahkan memanfaatkannya untuk keuntungan kita.
- Ketiga, dan ini yang paling penting, karena AI memiliki risiko dan tantangan etis. Buku-buku yang kita bahas tadi semuanya menyentuh isu bias algoritma, privasi data, dan tanggung jawab sosial. Model ML belajar dari data masa lalu. Kalau data masa lalu mengandung bias misalnya, diskriminasi gender dalam rekrutmen karyawan maka model ML yang dilatih dengan data itu akan melanggengkan bahkan memperkuat bias tersebut. Ini masalah serius.

Buku "*Artificial Intelligence: Konsep, potensi masalah, hingga pertanggungjawaban pidana*" bahkan membahas aspek legalnya: kalau AI melakukan kesalahan yang merugikan, siapa yang bertanggung jawab? Pembuat kodenya? Perusahaan yang mengoperasikannya? Atau AI-nya sendiri? Ini pertanyaan yang sampai sekarang masih diperdebatkan di berbagai negara.

### 3.3 PERUBAHAN POLA IDENTIFIKASI RISIKO DENGAN TEKNOLOGI CERDAS

Pernahkah kita membayangkan, dulu orang tua kita atau mungkin kakek-nenek kita, bagaimana cara mereka berdagang? Mereka hafal pelanggan satu per satu, tahu persis siapa yang biasa ngutang dan siapa yang bayar tunai, bisa nebak kapan musim ramai dan kapan sepi. Itu semua adalah bentuk identifikasi risiko, tapi dilakukan dengan cara yang sangat sederhana mengandalkan pengalaman, ingatan, dan firasat. Coba bayangkan sekarang, dengan ribuan transaksi per hari, pelanggan dari berbagai kota, dan persaingan yang ketat, apakah cara tradisional itu masih cukup?

inilah yang menarik. Cara kita mengidentifikasi risiko dalam bisnis perdagangan mengalami perubahan yang luar biasa dalam satu dekade terakhir. Dulu kita mengandalkan lembar kerja Excel, rapat bulanan yang panjang, dan intuisi para manajer senior. Sekarang? Teknologi cerdas mengambil alih sebagian besar pekerjaan berat itu. Tapi jangan salah, ini bukan cerita tentang mesin menggantikan manusia. Justru ini cerita tentang bagaimana manusia dan teknologi bekerja sama untuk melihat hal-hal yang sebelumnya tidak terlihat.

#### Memahami Perubahan Fundamental dalam Identifikasi Risiko

Sebelum kita masuk ke dalam berbagai teknologinya, kita harus paham dulu apa sebenarnya yang dimaksud dengan perubahan pola ini. Dulu, identifikasi risiko itu sifatnya reaktif dan periodik. Kita menunggu sampai ada masalah, baru kemudian mencari tahu penyebabnya. Atau kita melakukan identifikasi setahun sekali, pas mau buat laporan tahunan. Hasilnya? Banyak risiko yang sebenarnya sudah muncul sejak lama, baru ketahuan setelah jadi masalah besar. Sekarang, dengan teknologi cerdas, identifikasi risiko berubah menjadi proaktif dan real-time. Bukan lagi menunggu masalah terjadi, tapi mendeteksi potensi masalah sebelum ia benar-benar muncul. Bukan lagi mengandalkan sampel data terbatas, tapi menganalisis seluruh populasi data secara utuh. Ini pergeseran yang fundamental.

*Proxis Consulting*, dalam artikelnya tentang *Digital Governance Revolution*, menyebut perubahan ini sebagai transformasi dari pendekatan tradisional yang reaktif menuju ekosistem digital yang menghubungkan *predictive analytics*, *artificial intelligence*, dan *automated monitoring* untuk menciptakan kemampuan deteksi dini, respons cepat, dan pencegahan risiko yang lebih efektif. Teknologi tidak lagi sekadar alat bantu, tetapi telah menjadi enabler strategis yang mengubah fungsi manajemen risiko dari sekadar *cost center* menjadi *value creator* bagi organisasi.

Kalau kita lihat dari perspektif yang lebih teknis, perubahan ini juga diakui dalam literatur akademik. Sebuah artikel di jurnal ilmiah yang terindeks Scopus misalnya, membahas tentang penerapan algoritma data mining berbasis AI untuk penilaian risiko perusahaan. Mereka menggunakan kombinasi *Support Vector Machine* dan *fuzzy-based Convolutional Neural Network* yang ditingkatkan dengan algoritma genetika untuk menciptakan model

penilaian risiko yang lebih akurat. Hasilnya menunjukkan bahwa algoritma data mining ini dapat mengevaluasi risiko perusahaan dengan sangat efektif. Ini bukti bahwa di level riset global, perubahan pola identifikasi risiko ini sudah diakui dan terus dikembangkan.

### **Teknologi-Teknologi Cerdas yang Mengubah Cara Kita Melihat Risiko**

Setelah kita paham perubahannya secara konseptual, mari kita lihat teknologi apa saja yang sebenarnya bekerja di balik 45ayer. Ini penting, karena seringkali kita mendengar istilah-istilah canggih tapi tidak benar-benar paham bagaimana mereka bekerja dalam konteks identifikasi risiko.

#### **1. Artificial Intelligence dan Machine Learning.**

Ini adalah bintang utamanya. Dalam artikel *Proxsis*, dijelaskan beberapa aplikasi spesifik AI dan ML dalam manajemen risiko. Ada *Natural Language Processing* yang digunakan untuk analisis dokumen regulasi secara real-time. Bayangkan, dulu untuk memahami perubahan regulasi, kita harus baca ratusan halaman dokumen secara manual. Sekarang, AI bisa membaca, merangkum, dan bahkan mengidentifikasi implikasi risiko dari regulasi baru itu dalam hitungan menit.

Kemudian ada predictive modeling untuk mengidentifikasi *emerging risks* risiko-risiko yang baru muncul dan belum pernah kita hadapi sebelumnya. Model ini belajar dari berbagai sumber data, mencari pola-pola halus yang mungkin mengindikasikan ancaman di masa depan. Dan ada juga *anomaly detection* dalam transaksi dan pola operasional. Ini yang sering dipakai di perbankan untuk mendeteksi transaksi mencurigakan yang mungkin indikasi fraud.

#### **2. Blockchain dan Distributed Ledger Technology.**

Mungkin kita lebih sering mendengar blockchain dalam konteks *cryptocurrency*. Tapi dalam manajemen risiko, ia memiliki peran yang sangat penting. *Smart contracts* memungkinkan otomatisasi kepatuhan kontrak yang bisa mengeksekusi dirinya sendiri ketika kondisi tertentu terpenuhi. Ini mengurangi risiko kelalaian atau manipulasi manual. Immutable audit trails menciptakan jejak audit yang tidak bisa diubah, sehingga transparansi dan akuntabilitas terjamin. Kalau ada masalah, kita bisa melacak persis apa yang terjadi, kapan, dan siapa yang terlibat.

#### **3. Internet of Things (IoT) dan Sensor Networks.**

Ini mungkin yang paling membumi dan nyata dampaknya. Dengan IoT, kita bisa melakukan *real-time* monitoring terhadap risiko operasional. Bayangkan sensor-sensor yang dipasang di gudang penyimpanan, terus-menerus memantau suhu, kelembaban, getaran, dan berbagai parameter lainnya. Kalau ada penyimpangan misalnya suhu naik di atas batas aman untuk produk tertentu sistem bisa langsung memberi peringatan sebelum barang rusak. Ini adalah bentuk identifikasi risiko yang tidak mungkin dilakukan dengan inspeksi manual. Selain itu, ada juga *predictive maintenance* untuk mencegah kegagalan peralatan. Sensor pada mesin-mesin produksi bisa mendeteksi getaran tidak normal atau peningkatan suhu yang mengindikasikan mesin akan rusak. Sebelum mesin benar-benar mati dan mengganggu produksi, kita sudah bisa melakukan perawatan.

#### 4. **Robotic Process Automation (RPA).**

Teknologi ini mungkin kurang glamor dibanding AI, tapi dampaknya terhadap identifikasi risiko sangat signifikan. RPA digunakan untuk *automated data collection* dan pelaporan, serta *streamlined compliance workflows*. Tugas-tugas repetitif yang dulu dilakukan manual dan rawan kesalahan manusia, sekarang bisa diotomatisasi. Ini secara langsung mengurangi risiko operasional yang berasal dari *human error*.

#### **Implementasi Nyata: Dari Quarantin AI hingga AI-See-U**

Teori dan teknologi tadi akan lebih masuk akal kalau kita lihat contoh-contoh nyata implementasinya di Indonesia. Ternyata, perubahan pola identifikasi risiko dengan teknologi cerdas ini sudah terjadi di berbagai sektor, dan beberapa contohnya cukup mencengangkan.

##### 1. Contoh pertama datang dari Badan Karantina Indonesia (Barantin).

Mereka mengembangkan sistem bernama Quarantin AI untuk memperkuat ketahanan dan keamanan pangan melalui layanan digital yang lebih efisien, akurat, dan berkelanjutan. Kepala PDSI Barantin, Ichwandi, menjelaskan bahwa AI ini digunakan untuk kegiatan operasional seperti pengambilan keputusan, analisis data dalam jumlah besar, otomasi pada proses verifikasi, peringatan dini (*early warning*), identifikasi risiko, serta pelaporan kejadian anomali.

Yang menarik, mereka mengintegrasikan AI ini dengan sistem digital *Best Trust* yang sudah ada, dan menghubungkannya dengan sistem pertukaran data kementerian dan lembaga terkait, bahkan dengan karantina negara lain. Ini contoh bagus tentang bagaimana identifikasi risiko tidak lagi dilakukan sendiri-sendiri, tapi dalam ekosistem yang terhubung. Dengan *Quarantin AI*, proses yang tadinya mengandalkan keterlibatan petugas bisa diminimalisir, sehingga terhindar dari potensi kelalaian atau kealpaan, dan akurasi pengambilan keputusan serta efisiensi menjadi lebih optimal.

##### 2. Contoh kedua, dan ini menurut saya paling menarik, datang dari Pertamina Drilling.

Mereka meluncurkan teknologi bernama *AI-See-U*, sebuah sistem kecerdasan buatan yang terintegrasi dengan CCTV untuk mencegah kecelakaan kerja secara *real-time*. Latar belakangnya cukup mengkhawatirkan: data BPJS Ketenagakerjaan menunjukkan bahwa pada tahun 2023 tercatat 370.747 kasus kecelakaan kerja, melonjak dibandingkan 297.725 kasus pada tahun sebelumnya.

*AI-See-U* dirancang untuk mendeteksi *unsafe act & condition*, seperti pelanggaran penggunaan Alat Pelindung Diri mulai dari tidak memakai helm, sepatu pelindung, hingga sarung tangan dan kacamata keselamatan. Sistem ini secara otomatis mengirimkan peringatan ke penanggung jawab lapangan melalui WhatsApp atau email, dan mencatat data untuk analisis lebih lanjut. Bahkan, mereka merencanakan pengembangan lanjutan agar sistem bisa mengenali skenario tambahan seperti personel tidak sadarkan diri, deteksi asap dan api, ledakan, hingga isyarat permintaan bantuan dengan gerakan khusus. Ini adalah contoh sempurna tentang bagaimana identifikasi risiko berubah dari manual menjadi otomatis, dari reaktif menjadi proaktif, dan dari periodik menjadi *real-time*.

3. Contoh ketiga, masih dari grup Pertamina, yaitu PT Kilang Pertamina Internasional (KPI) Unit Balikpapan.

Mereka mengembangkan teknologi bernama RUVision yang mengintegrasikan sistem CCTV dengan analitik berbasis AI untuk mendeteksi kondisi berbahaya di lingkungan kilang. Sistem ini mampu melakukan deteksi dini terhadap aktivitas berisiko tinggi, termasuk perilaku tidak aman, kecepatan kendaraan, hingga indikasi kebocoran bahan berbahaya. Yang menarik, sistem ini dikembangkan tanpa harus mengganti seluruh perangkat CCTV yang ada, sehingga tetap efisien dari sisi anggaran.

Komisaris Independen PT KPI, *Prabunindya Revta Revolusi*, menyatakan bahwa lebih baik mengetahui potensi bahaya sejak dini agar bisa langsung ditangani, dan teknologi seperti ini bukan hanya mendukung keselamatan kerja, tapi juga mempercepat pengambilan keputusan. Dari ketiga contoh ini, kita bisa melihat pola yang sama: identifikasi risiko bergeser dari mengandalkan manusia dengan segala keterbatasannya, menuju kolaborasi antara manusia dan teknologi yang saling memperkuat.

#### **Risk Scoring dengan AI: Menyederhanakan Kompleksitas**

Selain contoh-contoh di atas, ada satu lagi perubahan pola yang sangat signifikan, yaitu dalam hal risk scoring. CRMS Indonesia, dalam publikasinya, menjelaskan bagaimana AI mengoptimalkan proses pemberian skor risiko. Risk scoring adalah proses pemberian skor terhadap suatu risiko berdasarkan berbagai parameter yang telah ditentukan. Skor ini membantu dalam mengkategorikan risiko dari tingkat rendah hingga tinggi, memungkinkan pengambil keputusan untuk menentukan strategi mitigasi yang tepat. Dalam metode tradisional, risk scoring sering kali mengandalkan analisis manual dan subjektif. Tapi dengan AI, proses ini menjadi lebih sistematis dan objektif.

#### **Ada beberapa cara AI mengoptimalkan risk scoring:**

- Pertama, analisis data yang lebih cepat dan akurat.  
AI dapat menganalisis data dalam jumlah besar dengan kecepatan tinggi, memungkinkan perusahaan mengidentifikasi pola risiko yang mungkin tidak terlihat dalam analisis manual.
- Kedua, reduksi bias dalam penilaian risiko.  
Risk assessment tradisional sering kali dipengaruhi oleh subjektivitas manusia. AI mengurangi bias ini dengan menilai risiko berdasarkan data historis dan algoritma yang telah dikembangkan.
- Ketiga, prediksi risiko dengan *machine learning*.  
Model *machine learning* dapat mempelajari pola dari kejadian masa lalu dan membuat prediksi risiko di masa depan, membantu organisasi dalam mengambil langkah pencegahan lebih awal.
- Keempat, automasi dalam proses *risk assessment*.  
Dengan AI, banyak tugas yang sebelumnya dilakukan secara manual dapat diotomatisasi, menghemat waktu dan sumber daya perusahaan.

Penerapan AI dalam *risk scoring* ini sudah terjadi di berbagai industri. Di sektor keuangan, AI digunakan untuk mendeteksi risiko kredit, mendukung penilaian kelayakan pinjaman, dan

mendeteksi aktivitas penipuan. Di keamanan siber, AI membantu mendeteksi ancaman dengan menganalisis pola serangan dan aktivitas mencurigakan secara *real-time*. Di rantai pasok, AI meningkatkan ketahanan dengan mengidentifikasi risiko operasional dan logistik sebelum berdampak pada bisnis. Di kesehatan, AI membantu menilai risiko pasien berdasarkan data medis.

Tentu saja, implementasi ini tidak tanpa tantangan. Kualitas data menjadi isu krusial AI sangat bergantung pada data berkualitas tinggi. Data yang tidak akurat atau tidak lengkap dapat menyebabkan hasil yang kurang tepat. Ada juga persoalan regulasi dan kepatuhan, di mana penggunaan AI harus memastikan transparansi dan keadilan dalam pengambilan keputusan. Dan yang tak kalah penting, keamanan dan privasi data menjadi aspek kritis, terutama ketika menangani informasi sensitif.

### **Evolusi Menuju GRC 4.0 dan Masa Depan Identifikasi Risiko**

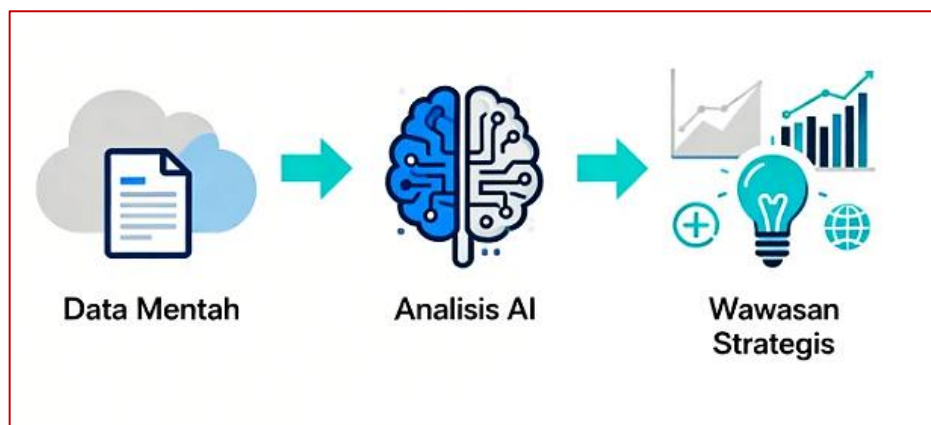
Semua perubahan yang kita bahas ini penggunaan AI, ML, blockchain, IoT, RPA, dan *risk scoring* cerdas sebenarnya adalah bagian dari evolusi yang lebih besar, yang oleh para ahli disebut sebagai GRC 4.0 atau Digitalisasi GRC. *Proxsis Consulting* mendefinisikan digitalisasi GRC sebagai transformasi fundamental dalam pendekatan *Governance, Risk, and Compliance* melalui integrasi teknologi digital mutakhir yang mengubah proses manual dan terfragmentasi menjadi sistem otomatis, terintegrasi, dan berbasis data. Ini merupakan evolusi dari GRC tradisional menuju ekosistem digital yang memanfaatkan kecerdasan buatan untuk menciptakan kemampuan prediktif dalam mengidentifikasi risiko, mengotomasi kepatuhan, dan mengoptimalkan tata kelola.

Poin pentingnya adalah, digitalisasi GRC tidak sekadar mengotomasi proses yang sudah ada, tetapi mentransformasi model operasional GRC dari reaktif menjadi proaktif, dari berbasis sampel menjadi berbasis populasi data penuh, dan dari terisolasi menjadi terintegrasi penuh dengan operasi bisnis. Ke depan, tren digitalisasi GRC akan semakin menarik. Kita akan melihat *autonomous compliance systems* sistem yang dapat secara otomatis beradaptasi dengan perubahan regulasi tanpa intervensi manusia. Ada juga *quantum computing for risk modeling* yang memungkinkan pemrosesan data dalam skala masif untuk pemodelan risiko yang lebih kompleks dan akurat. Dan yang tak kalah penting, akan ada *ethical AI governance frameworks* untuk memastikan penggunaan AI yang etis dan accountable dalam manajemen Risiko

### **3.4 MANFAAT AI DALAM PENGAMBILAN KEPUTUSAN BERBASIS DATA**

Mari kita duduk sejenak, bayangkan kita berada di sebuah ruang kerja yang penuh dengan tumpukan berkas data yang tingginya hampir menyentuh langit-langit. Dulu, seorang manajer mungkin butuh waktu berminggu-minggu, atau bahkan berbulan-bulan, hanya untuk memilah mana informasi yang relevan dan mana yang sekadar gangguan atau noise. Namun sekarang, kita berada di ambang era di mana mesin tidak hanya membantu kita menghitung, tapi juga membantu kita "melihat" apa yang tidak kasatmata di balik ribuan baris angka tersebut. Inilah inti dari bagaimana kecerdasan buatan atau AI mengubah fundamental pengambilan keputusan berbasis data.

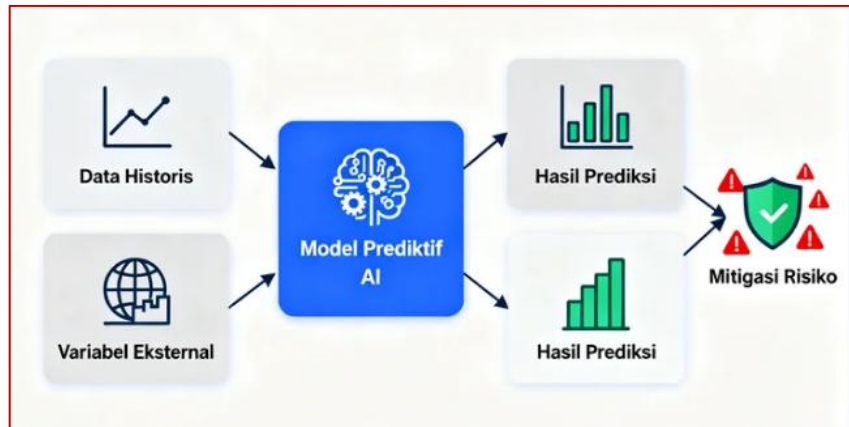
Keputusan yang diambil manusia, betapapun hebatnya pengalaman mereka, sering kali terjepit oleh batasan biologis yang disebut sebagai *bounded rationality*. Kita memiliki keterbatasan dalam memproses informasi yang terlalu masif dalam satu waktu. Di sinilah AI masuk sebagai asisten yang luar biasa tangguh. AI bukan sekadar alat otomatisasi, tapi sebuah mesin inferensi. Jika kita merujuk pada pemikiran Davenport dan Mittal (2020) dalam karya mereka mengenai *Augmented Intelligence*, manfaat utama AI bukanlah menggantikan peran manusia, melainkan memperluas jangkauan kognitif kita. AI mampu mendeteksi pola yang terlalu halus untuk ditangkap indra manusia, memprediksi tren masa depan dengan akurasi yang menakutkan, dan memberikan rekomendasi tindakan secara *real-time*.



**Gambar 3.4** Alur kerja pengambilan keputusan berbasis AI yang mentransformasi data mentah melalui pemrosesan algoritmik menjadi wawasan strategis yang dapat dieksekusi oleh manajemen.

Manfaat yang paling terasa dalam dunia bisnis, terutama perdagangan, adalah kemampuan AI dalam melakukan analisis prediktif yang sangat tajam. Bayangkan sebuah perusahaan retail yang harus memutuskan berapa banyak stok barang yang harus dibeli untuk musim depan. Dulu, ini mungkin lebih banyak mengandalkan "firasat" atau data penjualan tahun lalu yang sudah usang. Sekarang, AI bisa menarik data dari cuaca, tren media sosial, kondisi ekonomi makro, hingga perilaku pencarian di internet untuk memberikan angka yang jauh lebih presisi. Manfaatnya nyata: efisiensi biaya karena tidak ada stok yang mengendap terlalu lama, dan peningkatan kepuasan pelanggan karena barang selalu tersedia saat dibutuhkan.

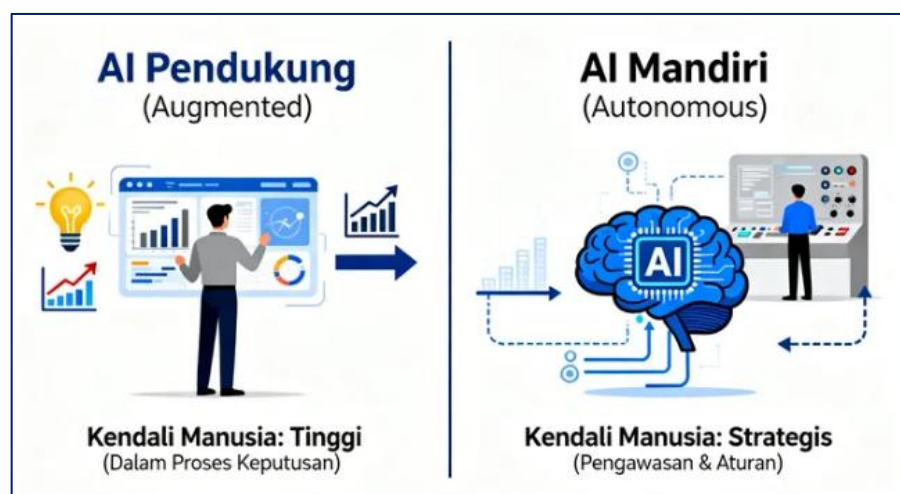
Namun, mari kita bicarakan sisi humanisnya. Ada semacam keresahan yang muncul; apakah kita menjadi terlalu bergantung pada mesin? Rasanya memang ada risiko di sana. Tapi sebenarnya, AI justru membebaskan kita dari tugas-tugas administratif yang membosankan dan repetitif. Saat AI menangani analisis data mentah, manusia kembali ke peran sejatinya: menjadi pemikir strategis dan penilai etis. Provost dan Fawcett (2013) dalam bukunya *Data Science for Business* menekankan bahwa keputusan berbasis data yang sukses memerlukan sinergi antara kemampuan teknis mesin dan intuisi kontekstual manusia. Mesin tahu "apa" yang terjadi dalam data, tapi manusia tahu "mengapa" hal itu penting bagi masyarakat atau pelanggan mereka.



**Gambar 3.5** Model analisis prediktif yang menunjukkan hubungan antara data historis, variabel eksternal, dan hasil prediksi yang membantu pemimpin bisnis memitigasi risiko di masa depan.

Selain itu, manfaat AI dalam pengambilan keputusan juga mencakup aspek kecepatan. Di pasar yang berubah secepat kilat, keputusan yang terlambat satu jam bisa berarti kehilangan peluang jutaan dolar. AI memungkinkan apa yang disebut sebagai *automated decision making* untuk hal-hal yang sifatnya rutin, sehingga manajemen puncak bisa fokus pada isu-isu besar yang membutuhkan kebijaksanaan. Namun, ada catatan kecil di sini keputusan otomatis ini tetap harus berada di bawah pengawasan tata kelola yang ketat. Kita tidak ingin algoritma berjalan sendiri tanpa ada kompas moral yang menjaganya.

Hal yang sama berlaku di dunia bisnis. AI memberikan data, AI memberikan probabilitas, tapi tanggung jawab akhir tetaplah milik manusia. Inilah yang membuat pengambilan keputusan berbasis AI menjadi sangat kuat; ia menggabungkan kekuatan komputasi yang dingin dengan nurani manusia yang hangat.



**Gambar 3.6** Perbandingan antara AI sebagai pendukung keputusan (*Augmented*) dan AI sebagai pengambil keputusan mandiri (*Autonomous*), menyoroti peran penting kendali manusia di setiap level.

Tantangan berikutnya dalam meraih manfaat ini adalah soal "kepercayaan". Bagaimana kita bisa percaya pada keputusan yang dihasilkan oleh sebuah kotak hitam atau *black box*? Itulah mengapa sekarang berkembang konsep *Explainable AI* (XAI). Manfaat AI akan maksimal jika para pemimpin bisnis bisa memahami alasan di balik sebuah rekomendasi. Kita tidak bisa hanya mengikuti instruksi mesin secara buta. Kita butuh transparansi agar setiap keputusan yang diambil bisa dipertanggungjawabkan secara moral dan hukum.

Pada akhirnya, perjalanan menuju digitalisasi dan adopsi AI dalam pengambilan keputusan adalah sebuah proses pendewasaan bagi organisasi. Ini bukan hanya soal membeli teknologi, tapi soal merombak cara kita berpikir. Kita belajar untuk lebih rendah hati di hadapan data, namun tetap tegas dalam memegang nilai-nilai kemanusiaan. AI adalah kompas yang sangat akurat, tapi kita tetaplah nahkodanya. Tanpa tujuan yang jelas dari manusia, kompas secanggih apa pun hanya akan menunjukkan arah tanpa tahu ke mana kita ingin berlabuh.

### 3.5 TANTANGAN IMPLEMENTASI AI DI SEKTOR PERDAGANGAN

Pernahkah, kita duduk santai sambil ngopi, lalu memikirkan sesuatu yang agak absurd: "bagaimana rasanya kalau tiba-tiba semua pedagang di pasar tradisional diganti jadi robot?" Atau, "Kira-kira kalau toko langganan kita pakai AI buat nentuin harga, apa yang bakal terjadi?" Pertanyaan-pertanyaan ini, yang awalnya mungkin hanya iseng, sebenarnya menyentuh inti dari transformasi besar yang sedang terjadi di dunia perdagangan saat ini. Sekarang, coba bayangkan sebuah skenario yang lebih realistis. Sebuah perusahaan dagang menengah, sebut saja PT Niaga Sejahtera, memutuskan untuk mengadopsi AI. Mereka beli *software* mahal, rekrut data *scientist*, pasang server canggih. Dua tahun kemudian, mereka evaluasi. Ternyata, yang berhasil diimplementasikan hanya chatbot untuk layanan pelanggan. Sisanya? Gagal total. Data *scientist*-nya resign karena frustrasi, *software*-nya jarang dipakai, dan manajemen mulai bertanya-tanya, "sudah habis miliaran, hasilnya mana?"

Cerita seperti ini bukan fiksi. Ini adalah kenyataan yang dihadapi banyak perusahaan saat ini. Survei global oleh *Tata Consultancy Services* (TCS) pada awal tahun 2026 mengungkapkan fakta yang cukup mencengangkan. Di tengah hiruk-pikuk pemberitaan tentang AI yang serba canggih, ternyata 85% peritel belum mulai mengimplementasikan atau bahkan merencanakan sistem multi-agen AI. Lebih dari separuhnya tepatnya 51% masih terjebak di teknologi dasar seperti chatbots dan asisten virtual, yang notabene sudah ada sejak bertahun-tahun lalu. Ini menunjukkan bahwa adopsi AI di sektor perdagangan, khususnya ritel, masih berada di permukaan. Ia seperti buih di lautan kelihatan banyak, tapi kedalamannya belum terjelajahi.

Pertanyaannya kemudian, kenapa? Kenapa teknologi yang dijanjikan bisa merevolusi segalanya ini, nyatanya sulit sangat diimplementasikan, terutama di sektor perdagangan yang notabene adalah tulang punggung ekonomi? Jawabannya tidak sederhana. Ada jalinan rumit antara masalah teknis, kesiapan manusia, hambatan regulasi, dan yang paling mendasar: kesenjangan antara harapan dan kenyataan di lapangan. Mari kita bedah satu per satu, pelan-pelan, seperti sedang membedah kasus di ruang kuliah. Bukan untuk mencari siapa yang salah,

tapi untuk memahami kompleksitas yang ada, agar kita tidak jatuh ke lubang yang sama ketika kelak berkecimpung di dunia nyata.

### **Benteng Pertama: Problem Teknis dan Kesiapan Infrastruktur**

Kalau kita berdiskusi sama para praktisi IT atau konsultan teknologi, keluhan pertama yang sering muncul soal adopsi AI hampir selalu berkaitan dengan data. Data adalah makanan pokoknya AI. Tanpa data yang berkualitas, AI itu seperti mesin balap tanpa bahan bakar canggih tapi tidak bisa jalan. Tapi masalah data ini tidak sesederhana "memiliki data atau tidak". Lapisannya banyak.

1. **Akses ke data berkualitas.** Survei gabungan WTO dan *International Chamber of Commerce* (ICC) yang dirilis Desember 2025 menemukan bahwa 14% perusahaan mengaku kesulitan mendapatkan data berkualitas tinggi untuk melatih sistem AI mereka. Bayangkan, dari sekian banyak perusahaan yang sudah memutuskan untuk berinvestasi di AI, satu dari tujuh di antaranya langsung mentok di masalah paling mendasar ini. Data yang dimiliki mungkin tidak lengkap, tidak terstruktur, atau terlalu kotor untuk dipakai. Di perusahaan dagang, data bisa tersebar di berbagai tempat: catatan transaksi di toko, logistik di gudang, interaksi pelanggan di media sosial, dan semuanya seringkali dalam format yang tidak kompatibel satu sama lain.
2. **Keterpisahan bahan bakar.** Istilah ini mungkin terdengar asing, tapi saya kutip dari analisis yang sangat menarik dari Huatai Securities, salah satu perusahaan sekuritas terkemuka. Dalam forum teknologi bursa efek akhir tahun 2025, *Chief Information Officer* mereka, Han Zhencong, memaparkan konsep ini dengan gamblang. Intinya, perusahaan teknologi (*big tech*) mungkin jago dalam algoritma, tapi mereka tidak memiliki akses ke data internal perusahaan yang paling berharga data transaksi riil, data loyalitas pelanggan, data rantai pasok. Data-data ini sangat sensitif dan dilindungi regulasi privasi, sehingga tidak bisa begitu saja diberikan ke pihak ketiga untuk melatih model AI.

Sebaliknya, perusahaan dagang yang memiliki data, seringkali tidak memiliki keahlian untuk mengolahnya. Survei TCS menunjukkan bahwa kesenjangan keterampilan tenaga kerja (*workforce skills gaps*) adalah tantangan terbesar kedua setelah tekanan finansial. Artinya, memiliki data saja tidak cukup. Perusahaan butuh orang-orang yang bisa "memasak" data mentah itu menjadi sesuatu yang berguna. Dan orang-orang dengan keahlian ini data scientist, *machine learning engineer* harganya mahal dan rebutan.

3. **Kompleksitas teknis dan biaya.** Implementasi AI itu tidak seperti beli software biasa yang tinggal instal lalu jalan. Ada proses panjang yang harus dilalui: survei kebutuhan, pembersihan data, pemilihan model, pelatihan model, pengujian, integrasi dengan sistem lama (*legacy systems*), dan pemeliharaan berkelanjutan. Survei WTO-ICC juga mencatat bahwa 14% perusahaan menyebut kurangnya keahlian atau pengetahuan AI sebagai tantangan utama. Ini bukan hanya soal biaya membeli teknologi, tapi juga biaya merekrut dan mempertahankan talenta, biaya

infrastruktur komputasi (terutama untuk melatih model besar), dan biaya konsultasi.

Masalah integrasi dengan sistem lama juga tidak kalah pelik. Banyak perusahaan dagang, terutama yang sudah berdiri puluhan tahun, memiliki sistem warisan yang dibangun dengan teknologi usang. Menyambungkan AI modern ke sistem tua ini seperti memasang mesin jet ke mobil klasik secara teknis mungkin, tapi butuh adaptasi dan biaya yang tidak sedikit.

### **Benteng Kedua: Problem Manusia dan Budaya Organisasi**

Ini yang paling menarik, sekaligus paling sulit. Karena teknologi bisa dibeli, tapi manusia tidak bisa diprogram ulang semudah itu. Respon manusia terhadap adopsi AI sangat kompleks, dan kalau tidak dikelola dengan baik, bisa jadi bumerang.

1. **Resistensi dari karyawan.** Sebuah studi yang sangat mendalam dari jurnal *Journal of Retailing and Consumer Services* pada akhir 2025 menginvestigasi "sisi gelap" adopsi AI di sektor ritel waralaba. Penelitian ini dilakukan di Taiwan, melibatkan 366 karyawan toko serba ada (*convenience store*) yang dipaksa menggunakan sistem pemesanan berbasis AI. Hasilnya? Meskipun adopsi teknologi ini bersifat wajib (karyawan tidak memiliki pilihan), hambatan yang dirasakan secara signifikan berdampak langsung pada ketidakpuasan kerja. Hambatan ini mencakup:

- Hambatan nilai: Karyawan merasa AI tidak memberikan nilai tambah bagi pekerjaan mereka. Sistem sering salah prediksi, menyebabkan kelebihan stok (yang akhirnya busuk) atau kekurangan stok (kehilangan penjualan).
- Hambatan risiko: Karyawan khawatir pekerjaan mereka terancam atau mereka tidak mampu menguasai teknologi baru.
- Hambatan tradisi: Perubahan ini mengganggu kebiasaan dan rutinitas kerja yang sudah mapan.
- Hambatan citra: Pengalaman negatif dengan AI membuat karyawan merasa tertekan dan tidak nyaman.

Yang lebih penting, ketidakpuasan kerja ini kemudian termanifestasi dalam berbagai bentuk keluhan (*complaints*). Ada keluhan yang sifatnya produktif (memberi masukan untuk perbaikan sistem), ada yang sekadar pelampiasan (curhat ke rekan kerja), dan ada yang bersifat maladaptif atau bahkan merusak. Ini menunjukkan bahwa mengabaikan aspek manusia dalam adopsi AI bisa memicu dinamika organisasi yang tidak sehat.

2. **Kesenjangan antara ekspektasi manajemen dan realitas lapangan.** Manajemen puncak sering melihat AI dari perspektif strategis: efisiensi, pengurangan biaya, peningkatan akurasi. Tapi di lapangan, ceritanya bisa berbeda. Kasus *AI-See-U* dari Pertamina Drilling yang saya singgung di bab sebelumnya memang sukses, tapi itu di lingkungan yang sangat terkontrol (rig pengeboran). Di ritel, lingkungannya jauh lebih dinamis dan tidak terduga. Studi yang sama menunjukkan bahwa karena seringnya produk baru dan variabel yang tak terduga (cuaca, hari libur, acara lokal), efektivitas "pembelajaran" AI seringkali tidak bisa mengimbangi perubahan cepat. Alhasil, sistem yang diandalkan malah jadi sumber masalah baru.

3. **Resistensi terhadap perubahan dan manajemen perubahan.** Banyak perusahaan terlalu fokus pada aspek teknis implementasi, tapi lupa bahwa adopsi AI adalah perubahan sosial. Pekerja mungkin takut kehilangan pekerjaan, takut tidak mampu beradaptasi, atau sekadar tidak suka dengan perubahan rutinitas. Mengabaikan aspek ini bisa menyebabkan kegagalan total. Seperti disebutkan dalam sebuah artikel praktis, "menerapkan AI bukanlah perubahan mekanis ini adalah perubahan sosial". Perusahaan perlu mengkomunikasikan manfaat, menawarkan pelatihan komprehensif, dan membina budaya yang menghargai pembelajaran berkelanjutan.

#### **Benteng Ketiga: Problem Etika, Regulasi, dan Tata Kelola**

Ini mungkin benteng yang paling rumit, karena menyangkut hal-hal yang tidak kasat mata: kepercayaan, keadilan, dan tanggung jawab. Jurnal dari *Future Business Journal* pada tahun 2025 melakukan studi komprehensif tentang implikasi etis adopsi AI dalam bisnis. Mereka mengidentifikasi setidaknya tujuh area kerisauan etis utama:

1. **Privasi dan Perlindungan Data:** Ini yang paling sering dibicarakan. Sistem AI, terutama yang digunakan untuk personalisasi pemasaran atau analisis perilaku konsumen, membutuhkan data pribadi dalam jumlah besar. Survei WTO-ICC menunjukkan bahwa dua pertiga perusahaan yang menggunakan AI memperkirakan biaya kepatuhan mereka akan meningkat setidaknya 5% karena perbedaan regulasi perlindungan data di berbagai negara. Untuk perusahaan dagang yang berekspansi lintas negara, ini beban yang tidak ringan.
2. **Bias dan Keadilan:** AI belajar dari data masa lalu. Kalau data masa lalu mengandung bias misalnya, preferensi terhadap kelompok tertentu maka AI akan melanggengkan bahkan memperkuat bias itu. Dalam konteks perdagangan, ini bisa berarti diskriminasi harga atau promosi yang tidak adil.
3. **Transparansi dan Explainability:** Banyak model AI, terutama *deep learning*, bekerja seperti "kotak hitam". Mereka bisa memberi hasil yang akurat, tapi tidak bisa menjelaskan mengapa hasil itu bisa keluar. Dalam konteks pengambilan keputusan bisnis yang kritis misalnya, menentukan limit kredit pelanggan atau memutuskan harga dinamis kurangnya transparansi ini menjadi masalah serius.
4. **Akuntabilitas dan Tanggung Jawab:** Kalau AI membuat kesalahan misalnya, sistem pemesanan otomatis salah order sehingga perusahaan rugi miliaran siapa yang bertanggung jawab? Vendor pembuat software? Manajer yang mengoperasikannya? Atau AI-nya sendiri? Pertanyaan ini masih jauh dari jawaban.
5. **Pergeseran Pekerjaan:** Otomatisasi yang dibawa AI memang bisa meningkatkan efisiensi, tapi juga bisa menghilangkan pekerjaan. Di sektor perdagangan, ini adalah isu sensitif karena sektor ini menyerap banyak tenaga kerja.
6. **Pengaruh Algoritmik dan Manipulasi:** Kemampuan AI untuk mempersonalisasi konten dan rekomendasi bisa disalahgunakan untuk memanipulasi pilihan konsumen.

**7. Pengambilan Keputusan Etis:** Mampukah AI membuat keputusan etis dalam situasi yang kompleks dan ambigu? Sejauh ini, jawabannya tidak.

Survei WTO-ICC menegaskan bahwa regulasi yang terfragmentasi dan ketidakpastian regulasi adalah tantangan inti. Hampir seperlima (19%) responden menyebut ketidakpastian regulasi sebagai perhatian utama mereka, dan 12% lainnya menyebut tantangan terkait regulasi atau kepatuhan sebagai hambatan utama adopsi AI. Ketika setiap negara memiliki aturan main sendiri tentang data, privasi, dan AI, perusahaan dagang global berada dalam posisi yang sangat sulit. Mereka harus mematuhi semua aturan yang berbeda-beda ini, yang secara signifikan meningkatkan kompleksitas dan biaya.

MIT Sloan Management Review, dalam artikelnya tentang "Tiga Hambatan yang Memperlambat AI yang Bertanggung Jawab", mengidentifikasi adanya kesenjangan akuntabilitas, kesenjangan budaya, dan kesenjangan komitmen. Banyak perusahaan dengan lantang mendeklarasikan prinsip-prinsip AI yang etis, tapi gagal mengimplementasikannya dalam praktik sehari-hari. Mereka tidak memiliki struktur kepemilikan yang jelas di tingkat proyek, tidak mengintegrasikan etika ke dalam prosedur rutin, dan tidak memberi insentif bagi perilaku yang bertanggung jawab.

**Benteng Keempat: Kesenjangan Digital Global dan Fragmentasi Pasar**

Ini adalah tantangan makro yang sering luput dari perhatian, tapi dampaknya sangat nyata. Adopsi AI tidak terjadi di ruang hampa. Ia terjadi di dunia yang timpang secara ekonomi dan teknologi. Kesenjangan antara negara maju dan berkembang sangat mencolok. Data WTO-ICC menunjukkan bahwa di negara berpenghasilan tinggi, 66% perusahaan sudah mengadopsi AI. Di negara berpenghasilan rendah dan menengah ke bawah, angkanya hanya 27%. Ini bukan sekadar angka statistik. Ini adalah gambaran tentang bagaimana AI, yang seharusnya bisa menjadi alat untuk meratakan lapangan bermain (*levelling the playing field*), justru berisiko memperdalam jurang pemisah yang sudah ada.

Perusahaan di negara berkembang menghadapi hambatan berlapis: infrastruktur digital yang kurang memadai, akses terbatas ke data berkualitas, lebih sedikit talenta AI, dan ketidakpastian regulasi yang lebih tinggi. Akibatnya, mereka tertinggal dalam perlombaan ini, dan kesenjangan terus melebar. Kesenjangan antara perusahaan besar dan kecil (UMKM) juga tidak kalah tajam. Survei yang sama menunjukkan bahwa perusahaan besar lebih maju dalam adopsi AI untuk kepatuhan perdagangan, sementara UMKM lebih banyak menggunakan AI untuk pengumpulan intelijen pasar dan komunikasi. Perusahaan besar memiliki sumber daya untuk membangun tim AI internal atau menyewa konsultan mahal. UMKM harus puas dengan solusi siap pakai yang mungkin tidak sepenuhnya sesuai dengan kebutuhan mereka.

Fragmentasi regulasi yang sudah disebutkan sebelumnya memperparah keadaan. Ketika setiap negara memiliki aturan sendiri tentang data dan AI, perusahaan kecil yang ingin berekspansi ke luar negeri akan kewalahan menghadapi kompleksitas ini. Biaya kepatuhan yang membengkak bisa menjadi penghalang yang tidak bisa diatasi.

**Benteng Kelima: Masalah Spesifik Domain Kinerja AI di Sektor Keuangan dan Perdagangan**

Terakhir, ada tantangan yang sangat spesifik terkait dengan domain perdagangan itu sendiri, terutama di area yang melibatkan "uang beneran" seperti transaksi finansial, perdagangan saham, atau penentuan harga.

Pertama, masalah "halusinasi" (*hallucination*) pada model bahasa besar (LLM). Ini adalah istilah teknis untuk kondisi di mana AI dengan percaya diri memberikan informasi yang salah atau mengada-ada. Dalam konteks percakapan santai, mungkin ini hanya jadi bahan ketawa. Tapi dalam konteks perdagangan, halusinasi bisa berakibat fatal. Sebuah studi yang sangat teliti di jurnal *Frontiers of Information Technology & Electronic Engineering* pada akhir 2025 menguji kemampuan LLM untuk memproses dan mengeksekusi instruksi perdagangan finansial. Hasilnya? Mengejutkan sekaligus mengecewakan.

Memang, model-model ini cukup bagus dalam menghasilkan format data yang benar (sekitar 80-99% berhasil) dan cukup pintar untuk mengajukan pertanyaan klarifikasi ketika instruksi tidak lengkap (90-100%). Tapi, di situlah berhentinya kabar baik.

Akurasi *end-to-end* sangat rendah, hanya sekitar 6% sampai 14%. Artinya, dari seratus instruksi perdagangan yang diberikan, hanya 6 sampai 14 yang benar-benar diproses dengan tepat dari awal hingga akhir.

Informasi yang hilang cukup besar, antara 12% sampai 66%. Model sering kehilangan detail penting dalam instruksi. Yang paling parah, 70% sampai 80% pertanyaan lanjutan yang diajukan model sebenarnya tidak perlu. Mereka terlalu banyak bertanya, yang tidak hanya membuat proses jadi lambat, tapi juga berpotensi mengekspos informasi sensitif yang seharusnya tidak perlu. Studi ini dengan tegas menunjukkan bahwa meskipun LLM memiliki potensi besar, mereka belum siap untuk diandalkan di area yang membutuhkan presisi tinggi dan toleransi kesalahan nol, seperti eksekusi perdagangan.

Kedua, masalah "harga halusinasi" di sektor keuangan. Open AI sendiri, pencipta ChatGPT, secara eksplisit melarang penggunaan model mereka untuk memberikan nasihat keuangan. Kenapa? Karena risikonya terlalu besar. Kesalahan interpretasi sekecil apa pun bisa menyebabkan kerugian finansial yang masif. Ini menunjukkan bahwa bahkan pencipta teknologi ini pun sadar akan keterbatasannya.

Ketiga, risiko sistemik. Penggunaan AI secara masif di sektor perdagangan dan keuangan bisa menciptakan risiko baru yang sebelumnya tidak ada. FTI Consulting, dalam analisisnya, menyoroti beberapa risiko kunci:

- Ketidakstabilan pasar: Adopsi AI secara kolektif dapat mengakibatkan aksi bersama dan risiko konsentrasi yang lebih tinggi, sehingga memperkuat guncangan pasar. Bank of England bahkan berencana untuk secara ketat memantau penggunaan AI oleh hedge fund dan bank karena kekhawatiran ini.
- Risiko sistemik: Ketergantungan pada sejumlah kecil penyedia layanan AI dapat membuat perusahaan rentan terhadap pengambilan keputusan perdagangan yang berisiko tinggi atau suboptimal secara seragam.

- Latensi: Beberapa sistem AI generatif mungkin tidak cocok untuk perdagangan frekuensi tinggi karena latensi inferensi mereka relatif terhadap algoritma perdagangan konvensional.

### 3.6 PERBEDAAN AI, BIG DATA, DAN AUTOMATION

Perkembangan teknologi digital telah mengubah cara organisasi mengelola data, mengambil keputusan, dan menjalankan proses bisnis. Tiga teknologi yang memiliki peranan penting dalam perubahan tersebut adalah *Artificial Intelligence (AI)*, *Big Data*, dan *Automation*. Ketiga konsep tersebut sering digunakan secara bersamaan sehingga terkadang dianggap sebagai teknologi yang sama. Padahal, masing-masing memiliki tujuan, karakteristik, mekanisme kerja, dan keluaran yang berbeda.

*Big Data* berfokus pada pengelolaan dan analisis data dalam jumlah besar serta kompleks. *Artificial Intelligence* berfokus pada kemampuan sistem komputer untuk mempelajari data, mengenali pola, melakukan prediksi, dan menghasilkan keputusan atau rekomendasi. Sementara itu, *Automation* berfokus pada pelaksanaan suatu pekerjaan atau proses secara otomatis dengan mengurangi kebutuhan intervensi manusia.

Perbedaan tersebut tidak berarti bahwa ketiganya berdiri sendiri. Dalam praktiknya, *Big Data* dapat menyediakan sumber data bagi AI, AI dapat menghasilkan prediksi atau keputusan berdasarkan data tersebut, sedangkan *Automation* dapat menjalankan tindakan berdasarkan hasil analisis AI. Penelitian terbaru bahkan menunjukkan adanya kecenderungan integrasi antara automation, Big Data Analytics, AI, dan Machine Learning dalam berbagai sektor industri.

#### Artificial Intelligence

*Artificial Intelligence (AI)* atau kecerdasan buatan merupakan teknologi yang memungkinkan sistem komputer melakukan tugas yang sebelumnya membutuhkan kemampuan kognitif manusia. Kemampuan tersebut antara lain mengenali pola, melakukan klasifikasi, memahami bahasa, melakukan prediksi, memberikan rekomendasi, dan membantu pengambilan keputusan. Dalam lingkungan Industry 4.0, AI menjadi salah satu teknologi utama karena dapat memanfaatkan data yang dihasilkan oleh sensor, Internet of Things (IoT), sistem informasi, dan berbagai sumber digital lainnya. Jan et al. (2023) menunjukkan bahwa implementasi AI dalam Industry 4.0 berkaitan erat dengan ketersediaan data dalam jumlah besar, machine learning, jaringan sensor, IoT, cloud computing, serta teknologi digital lainnya. Dengan demikian, AI tidak hanya dapat dipahami sebagai sebuah aplikasi seperti chatbot atau virtual assistant. AI merupakan sebuah pendekatan komputasional yang memungkinkan sistem melakukan proses yang bersifat **intelligent**, seperti belajar dari data dan menghasilkan prediksi.

#### BIG DATA

*Big Data* mengacu pada data yang memiliki skala, kompleksitas, dan kecepatan pertumbuhan yang membuatnya sulit dikelola menggunakan metode pengolahan data konvensional. Big Data tidak hanya berkaitan dengan ukuran data yang besar. Data dapat berasal dari berbagai sumber, memiliki format yang berbeda, dihasilkan dengan kecepatan

tinggi, dan memiliki tingkat kualitas yang berbeda. Dalam konteks analitik, Big Data memungkinkan organisasi memperoleh informasi dan pola yang sebelumnya sulit ditemukan melalui metode pengolahan data tradisional. Big Data akan menjadi lebih bernilai ketika diproses menggunakan teknik analitik. *Big Data Analytics* merupakan proses mengolah dan menganalisis data dalam skala besar untuk memperoleh informasi, pola, hubungan, atau prediksi. Jamarani et al. (2024), melalui systematic literature review terhadap 109 penelitian, menunjukkan bahwa Big Data Predictive Analytics digunakan pada berbagai bidang, termasuk industri, e-commerce, smart healthcare, smart agriculture, smart city, ICT, dan weather forecasting.

### **Automation**

*Automation* atau otomatisasi adalah penggunaan teknologi untuk menjalankan suatu proses atau pekerjaan secara otomatis dengan sedikit intervensi manusia. Automation sebenarnya bukan konsep yang sepenuhnya baru. Sistem otomatis telah digunakan dalam industri sejak lama. Namun, perkembangan AI, Big Data, IoT, cloud computing, dan machine learning telah melahirkan bentuk baru yang sering disebut sebagai *Intelligent Automation*.

### **Contoh Penerapan AI dalam Manajemen Risiko**

Artificial Intelligence (AI) dapat diterapkan dalam manajemen risiko untuk membantu perusahaan mengidentifikasi, menganalisis, dan mengendalikan berbagai risiko secara lebih cepat dan akurat. Salah satu contohnya adalah dalam mendeteksi penipuan atau fraud, yaitu dengan menganalisis pola transaksi dan mengenali aktivitas yang tidak biasa. AI juga dapat digunakan dalam penilaian risiko kredit dengan menganalisis data calon debitur, seperti riwayat pembayaran dan kondisi keuangan, untuk memperkirakan kemungkinan terjadinya gagal bayar. Selain itu, AI dapat membantu memprediksi risiko operasional, misalnya dengan menganalisis kondisi mesin dan data produksi untuk mengetahui kemungkinan terjadinya kerusakan atau gangguan sebelum terjadi.

Dalam bidang keamanan, AI dapat digunakan untuk mengelola risiko siber dengan mendeteksi aktivitas mencurigakan, seperti akses tidak sah atau serangan terhadap jaringan perusahaan. AI juga dapat membantu perusahaan dalam menghadapi risiko pasar dengan menganalisis data historis dan kondisi pasar untuk memperkirakan perubahan harga saham, nilai tukar, atau komoditas. Dengan kemampuan tersebut, AI dapat membantu perusahaan melakukan pemantauan risiko secara real-time dan memberikan peringatan apabila terdapat potensi masalah. Oleh karena itu, penerapan AI dalam manajemen risiko dapat membuat proses pengelolaan risiko menjadi lebih efektif, cepat, dan berbasis data. Namun, penggunaan AI tetap perlu disertai pengawasan manusia agar hasil analisis dapat dievaluasi dan keputusan yang diambil tetap tepat.

### **KESIMPULAN**

Dari seluruh pembahasan yang sudah kita telusuri bersama, ada beberapa benang merah yang bisa ditarik sebagai kesimpulan. Pertama, digitalisasi telah mengubah wajah perdagangan secara fundamental. Dari transaksi tatap muka di pasar tradisional, kita bergerak menuju ekosistem digital yang kompleks dengan jangkauan global. Pemerintah Indonesia

sendiri telah mendorong digitalisasi ribuan pasar dan ratusan ribu pedagang, membuktikan bahwa transformasi ini bukan lagi pilihan, melainkan keharusan.

Kedua, *Artificial Intelligence* dan *Machine Learning* adalah inti dari kecerdasan digital. AI adalah simulasi kecerdasan manusia dalam mesin, sementara ML adalah cara mesin belajar dari data baik dengan pengawasan, tanpa pengawasan, maupun penguatan. *Deep learning* dengan jaringan saraf tiruan membawa kemampuan ini ke level berikutnya, memungkinkan mesin mengenali pola yang tidak kasat mata. Tapi yang perlu diingat, AI bukan magic; ia sangat bergantung pada kualitas data yang kita berikan.

Ketiga, teknologi cerdas mengubah pola identifikasi risiko secara radikal. Dulu identifikasi risiko bersifat reaktif dan periodic menunggu masalah datang baru bereaksi. Sekarang, dengan IoT, AI, dan analitik prediktif, ia menjadi proaktif dan *real-time*. Sensor di gudang mendeteksi potensi kerusakan sebelum terjadi. CCTV dengan AI mengenali perilaku tidak aman dan memberi peringatan langsung. Sistem analitik memprediksi risiko kredit sebelum pelanggan macet. Quarantin AI, AI-See-U, dan RUVision adalah bukti nyata bahwa perubahan ini sudah berjalan di Indonesia.

Keempat, manfaat AI dalam pengambilan keputusan berbasis data sangat nyata. AI mampu menganalisis data dalam volume besar dengan kecepatan tinggi, mengurangi bias subjektivitas manusia, memprediksi risiko masa depan dengan machine learning, mengotomatisasi tugas-tugas repetitif, dan memberikan rekomendasi yang lebih akurat. Dalam risk scoring, misalnya, AI mengubah proses manual dan subjektif menjadi sistematis dan objektif. Hasilnya, keputusan bisnis bisa diambil lebih cepat, lebih tepat, dan lebih terinformasi.

Kelima, tantangan implementasi AI di sektor perdagangan masih sangat berat. Survei global menunjukkan 85% peritel bahkan belum mulai merencanakan sistem AI multi-agen. Hambatan datang dari berbagai sisi: kualitas data yang buruk, kesenjangan keterampilan tenaga kerja, resistensi karyawan, fragmentasi regulasi lintas negara, masalah etika dan bias algoritma, hingga kesenjangan digital antara negara maju dan berkembang. Yang paling mengkhawatirkan, studi menunjukkan akurasi AI dalam eksekusi instruksi perdagangan hanya 6-14%—jauh dari kata layak untuk diandalkan di area yang membutuhkan presisi tinggi.

*Pada Akhirnya...*

Transformasi digital dan AI dalam manajemen risiko adalah pedang bermata dua. Di satu sisi, ia membuka peluang luar biasa untuk efisiensi, akurasi, dan kecepatan yang tidak mungkin dicapai manusia sendiri. Di sisi lain, ia membawa risiko baru yang tidak kalah kompleks risiko data, risiko etika, risiko regulasi, dan risiko manusia.

Yang paling penting untuk diingat: AI bukan pengganti manusia, melainkan alat untuk memperkuat manusia. Teknologi secanggih apa pun, pada akhirnya keputusan strategis, pertimbangan etis, dan akuntabilitas tetap berada di tangan manusia. Perusahaan yang berhasil bukanlah yang paling canggih teknologinya, tapi yang paling bijak mengelola keseimbangan antara kecanggihan mesin dan kebijaksanaan manusia. Masa depan manajemen risiko bukan tentang mesin yang mengambil alih, tapi tentang kolaborasi yang

harmonis antara kecerdasan buatan dan kecerdasan alami. Dan untuk mencapai itu, perjalanannya masih panjang.

### **LATIHAN SOAL**

Dalam pembahasan mengenai risk scoring dengan AI, dijelaskan bahwa AI dapat mengurangi bias dalam penilaian risiko dan melakukan analisis data dalam jumlah besar dengan kecepatan tinggi.

- Perbandingan: Jelaskan perbedaan mendasar antara identifikasi risiko secara tradisional (manual) dan identifikasi risiko dengan bantuan teknologi cerdas (AI) dari sisi kecepatan, akurasi, dan objektivitas.
- Batas Kemampuan AI: Meskipun AI sangat canggih, disebutkan bahwa teknologi tidak dapat memutuskan mana risiko yang harus diprioritaskan berdasarkan nilai-nilai perusahaan. Mengapa faktor manusia tetap menjadi pusat dalam pengambilan keputusan strategis meskipun AI sudah diimplementasikan?
- Etika: Salah satu tantangan etis AI adalah masalah "kotak hitam" (black box) atau kurangnya transparansi dalam pengambilan keputusan. Dalam konteks perdagangan, mengapa hal ini bisa menjadi masalah serius, terutama jika dikaitkan dengan akuntabilitas?

# BAB 4

## IDENTIFIKASI RISIKO PERUSAHAAN DAGANG BERBASIS AI

---

Bagaimana data dan algoritma memperluas kemampuan deteksi tanpa menghilangkan peran manusia?

### CAPAIAN PEMBELAJARAN

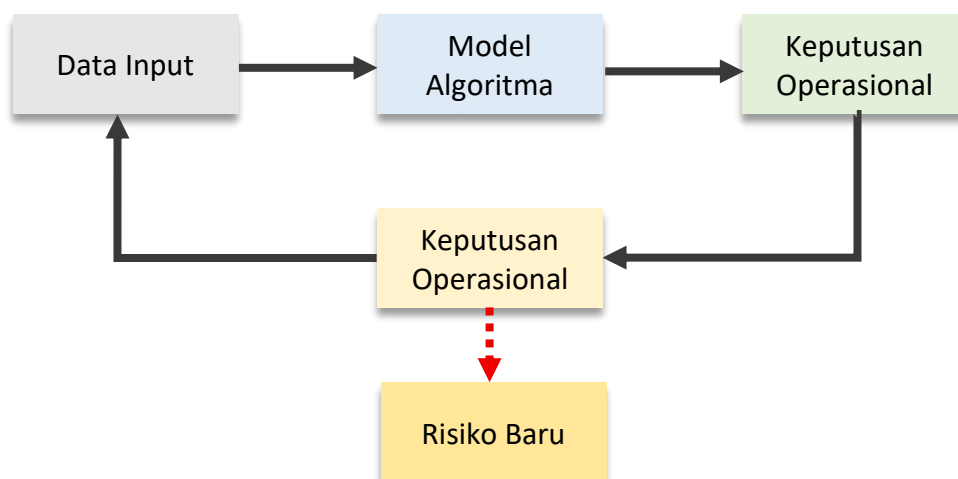
- Membandingkan identifikasi tradisional dan berbasis data.
- Menggunakan AI untuk memetakan risiko operasional dan pasar.
- Menjelaskan deteksi anomali transaksi.
- Menilai kelebihan dan keterbatasan pendekatan hibrida.
- Menyusun daftar risiko yang dapat ditindaklanjuti.

#### 4.1 PENGANTAR BAB

Mari kita duduk sejenak dan coba renungkan ini secara lebih mendalam. Bayangkan sebuah gudang besar atau pusat distribusi ritel yang sangat sibuk di pinggiran kota, di mana ribuan jenis barang mengalir masuk dan keluar setiap detiknya tanpa henti. Di sudut ruangan yang sunyi, ada sebuah server atau mungkin hanya laptop tipis yang bekerja dalam diam, mencoba membedah pola perilaku jutaan manusia untuk memprediksi apa yang akan mereka beli besok pagi. Itulah realitas kita saat ini sebuah peradaban dagang yang sudah menyerahkan sebagian besar "otak" operasionalnya kepada Kecerdasan Buatan atau AI.

Namun, sering kali dalam obrolan hangat di koridor kampus atau saat diskusi serius di ruang rapat, orang-orang bicara tentang AI seolah-olah itu adalah entitas dewa yang tidak bisa salah dan serba tahu. Padahal, memasukkan AI ke dalam jantung perusahaan dagang itu ibarat mengundang seorang tamu jenius yang sangat asing; dia memang luar biasa pintar, tapi kalau tidak diawasi dengan teliti, dia bisa mengacaukan seluruh tatanan rumah karena dia tidak memahami konteks lokal, emosi manusia, atau etika yang selama ini menjadi perekat hubungan jual beli.

Identifikasi risiko di era keemasan AI ini bukan lagi sekadar perkara mencatat barang yang hilang di rak atau mengeluh soal harga bensin yang naik-turun secara manual di buku besar. Ini jauh lebih dalam dari itu ini soal memahami "kotak hitam" atau black box yang kita sebut algoritma. Risiko dalam perusahaan dagang berbasis AI itu berlapis-lapis dan sering kali tidak kasatmata sampai semuanya meledak menjadi kerugian nyata. Ada risiko teknis yang rumit, risiko bias data yang sangat halus, hingga risiko etika yang kalau dibiarkan bisa meruntuhkan reputasi yang sudah dibangun dengan keringat selama puluhan tahun hanya dalam hitungan detik.



**Gambar 4.1** Alur identifikasi risiko dalam ekosistem perdagangan digital yang menunjukkan interaksi dinamis antara input data, model algoritma, dan keputusan operasional yang berpotensi melahirkan risiko baru yang bersifat sistemik.

Jika kita menilik kembali perspektif klasik dari Vaughan dan Vaughan (2007), risiko secara mendasar didefinisikan sebagai suatu kondisi di mana terdapat kemungkinan munculnya

penyimpangan dari hasil yang semula diharapkan. Nah, dalam konteks teknologi masa kini, penyimpangan ini sering kali bukan terjadi karena mesinnya rusak atau kabelnya putus, tapi justru karena mesinnya belajar dari pola yang salah, data yang sudah "basi", atau variabel yang tidak relevan dengan kondisi lapangan yang sebenarnya.

Mari kita bedah satu per satu sumber "kericuhan" potensial ini dengan cara yang lebih membumi, seolah kita sedang berdiskusi di depan segelas kopi. Pertama, ada yang namanya risiko ketergantungan pada integritas data. Perusahaan dagang sekarang sangat bergantung pada data historis untuk memprediksi berapa banyak stok yang harus disediakan di gudang.

Masalahnya, AI itu sangat haus akan data, tapi ia tidak bisa membedakan mana data yang "bergizi" dan mana data yang "beracun". Kalau data yang dimasukkan itu "kotor" atau bias misalnya data penjualan dari masa pandemi dua tahun lalu yang sangat anomali dan tidak normal maka prediksi AI untuk masa depan akan menjadi sangat kacau balau. James Lam (2014) dalam bukunya yang sangat tajam mengingatkan bahwa manajemen risiko yang efektif harus mampu menghubungkan sinyal-sinyal risiko ini ke dalam strategi bisnis secara utuh. Jika seorang manajer atau pemilik toko hanya percaya mentah-mentah pada apa yang dikatakan angka di layar monitor tanpa melakukan verifikasi manual atau sekadar pengecekan logika dasar, perusahaan tersebut bisa terjebak dengan jutaan stok barang yang sebenarnya sama sekali tidak diinginkan oleh pasar saat ini.

Jeda sejenak, coba kita pikirkan soal risiko dari sisi algoritma itu sendiri. AI terkadang melakukan apa yang oleh para ahli disebut sebagai "halusinasi". Di dunia perdagangan, ini bisa berarti sistem secara otomatis memberikan diskon yang luar biasa besar karena ia mendeteksi pola musiman yang sebenarnya tidak ada atau hanya kebetulan sesaat. Atau yang jauh lebih parah lagi adalah risiko bias sosial yang tersembunyi. Algoritma mungkin saja secara tidak sadar membatasi akses produk premium kepada kelompok masyarakat tertentu hanya karena data masa lalu menunjukkan profil risiko yang tinggi secara tidak adil. Ini bukan hanya soal kehilangan potensi keuntungan, tapi soal masalah keadilan dan etika bisnis yang sangat sensitif. Di sinilah aspek humanis atau sentuhan manusia harus masuk dengan sangat kuat. Kita butuh mata manusia yang jeli untuk mengaudit algoritma tersebut secara berkala. Identifikasi risiko tidak bisa lagi dilakukan setahun sekali seperti sebuah ritual audit tradisional yang membosankan; ia harus dilakukan secara terus-menerus, lincah, dan penuh kewaspadaan.

#### **4.2 TEKNIK IDENTIFIKASI RISIKO TRADISIONAL VS BERBASIS DATA**

Pernahkah kita merenung sejenak, betapa berbedanya dunia sekarang dengan dua puluh tahun lalu? Dulu, kalau ada manajer risiko mau tahu potensi masalah di perusahaannya, caranya sederhana: berdiskusi sama orang-orang, turun ke lapangan lihat langsung, atau baca laporan setebal bantal. Sekarang? Seorang analis data bisa duduk di satu tempat, membuka dashboard, dan dalam hitungan detik tahu persis di mana letak keanehan transaksi mencurigakan dari pelanggan A, pola pembelian aneh dari cabang B, atau potensi kebocoran data dari server C.

Dua pendekatan ini yang satu mengandalkan pengamatan manusia dan pengalaman, yang satu lagi mengandalkan hitungan mesin dan algoritma sering disebut sebagai teknik identifikasi risiko tradisional dan teknik identifikasi risiko berbasis data. Keduanya memiliki tempat masing-masing. Tapi kalau kita pahami lebih dalam, sebenarnya bukan soal mana yang lebih baik, melainkan bagaimana keduanya bisa saling melengkapi di tengah dunia yang makin kompleks. Mari kita berdiskusi ini, pelan-pelan, seperti diskusi di ruang kuliah yang tidak kaku-kaku amat. Sambil sesekali ngopi, kalau perlu. Karena topik ini penting sangat buat kita pahami, terutama kalau kelak berkecimpung di dunia bisnis yang makin digital.

Memahami Dulu: Apa Itu Identifikasi Risiko?

Sebelum kita masuk ke perbandingan tekniknya, kita harus sepakat dulu soal apa itu identifikasi risiko. Dalam literatur manajemen risiko, identifikasi risiko adalah langkah pertama dan paling fundamental dalam seluruh proses manajemen risiko. Ini adalah proses menemukan, mengenali, dan mencatat risiko-risiko yang mungkin mempengaruhi pencapaian tujuan organisasi. Buku "Manajemen Risiko" yang ditulis oleh Gatot Ahmad dan koleganya, diterbitkan CV Widina Media Utama tahun 2025, menjelaskan bahwa konsep risiko melibatkan pemahaman tentang kemungkinan terjadinya peristiwa atau situasi yang dapat menyebabkan kerugian atau dampak negatif terhadap sebuah tujuan, baik secara individu maupun organisasi. Risiko timbul karena ketidakpastian dan kemungkinan hal negatif yang akan timbul dan terjadi. Secara sederhana, risiko mengacu pada kemungkinan ketidaksesuaian antara hasil aktual dan harapan, serta adanya ancaman atau peluang yang perlu diidentifikasi, diukur, dan dikelola dengan bijaksana. identifikasi risiko inilah yang menjadi pintu masuk. Kalau kita salah mengidentifikasi, maka langkah-langkah selanjutnya analisis, evaluasi, mitigasi akan berjalan di tempat yang salah. Ibarat mau berobat, kalau diagnosis keliru, obat semahal apa pun tidak akan menyembuhin.

#### **Teknik Identifikasi Risiko Tradisional: Akar yang Kokoh**

Mari kita bedah lebih dalam tentang teknik identifikasi risiko tradisional. Ini adalah metode-metode yang sudah digunakan puluhan tahun, bahkan ada yang sejak awal abad ke-20. Mereka disebut "tradisional" bukan karena usang atau tidak berguna, tapi karena pendekatannya yang lebih manual, lebih mengandalkan keahlian manusia, dan biasanya bersifat kualitatif.

- **Identifikasi berbasis wawancara dan observasi.** Ini adalah metode paling sederhana dan paling tua. Penelitian di industri batik yang dipublikasikan di Jurnal Dinamika Kerajinan dan Batik menggunakan pendekatan ini. Para peneliti turun langsung ke lapangan, berdiskusi dengan para perajin, melihat proses produksi, dan mencatat apa saja yang bisa salah. Mereka menggunakan pendekatan ISO 31000 dan model House of Risk untuk mengidentifikasi 25 kejadian risiko dari 20 agen risiko. Dari identifikasi ini, mereka kemudian merumuskan 8 strategi mitigasi, mulai dari pengarahan untuk memotivasi pekerja, menerapkan sistem reward and punishment, hingga merekrut karyawan administrasi yang paham IT.
- **Metode pohon kejadian (*event tree*) dan analisis probabilistik.** Ini adalah metode yang lebih maju dari sekadar wawancara. Studi tentang Bendungan Saguling yang

dipublikasikan di Jurnal Wahana Teknik Sipil Polines menggunakan tiga metode berbeda: metode tradisional, metode pohon kejadian, dan metode modifikasi ICOLD. Hasilnya sangat menarik: metode tradisional menunjukkan bahwa risiko Bendungan Saguling "tidak dapat diterima" (*unacceptable*) karena metode ini tidak menggambarkan setiap kemungkinan secara detail. Sementara metode pohon kejadian menunjukkan hasil sebaliknya risikonya dapat diterima. Metode modifikasi ICOLD menunjukkan bahwa bendungan ini masuk dalam kategori risiko sedang.

- **Matriks risiko atau risk matrix.** Ini mungkin alat yang paling populer dan paling banyak digunakan di berbagai organisasi. Matriks risiko menggabungkan estimasi kemungkinan terjadinya (*probabilitas*) dan tingkat keparahan dampak (*severity*) ke dalam satu visualisasi sederhana biasanya kotak-kotak berwarna merah, kuning, hijau. Metode ini dijelaskan dalam berbagai literatur, termasuk artikel dari Universitas Medan Area tentang langkah-langkah manajemen risiko IT. Dalam matriks risiko, setelah melakukan analisis kemungkinan dan dampak, kita menentukan tingkat keparahan dan memprioritaskan risiko berdasarkan tingkat keparahannya.
- **Job Safety Analysis (JSA) untuk identifikasi bahaya di tempat kerja.** Metode ini banyak digunakan di sektor industri dan pertambangan. Meskipun tidak disebutkan secara eksplisit dalam sumber yang kita memiliki, JSA adalah contoh klasik identifikasi risiko tradisional yang mengandalkan observasi langsung dan pengalaman pekerja. Tim keselamatan kerja akan mengamati setiap langkah pekerjaan, mengidentifikasi potensi bahaya di setiap langkah, dan menentukan tindakan pengendalian yang diperlukan.
- **Delphi method dan expert judgment.** Metode ini mengandalkan konsensus para ahli melalui serangkaian kuesioner dan diskusi terstruktur. Para ahli diminta memberikan penilaian mereka tentang berbagai risiko, kemudian hasilnya dirangkum dan dikembalikan ke para ahli untuk penilaian putaran berikutnya. Proses ini diulang sampai tercapai konsensus. Metode ini sangat berguna ketika data kuantitatif tidak tersedia atau tidak memadai.

#### Keterbatasan Metode Tradisional: Ketika Dunia Bergerak Terlalu Cepat

Setelah kita memahami berbagai teknik tradisional, kita harus jujur mengakui bahwa metode-metode ini memiliki keterbatasan yang semakin terasa di era digital sekarang.

1. Sifatnya yang reaktif dan periodik. Metode tradisional biasanya dilakukan secara berkala setahun sekali, atau paling sering sebulan sekali. Identifikasi risiko di industri batik dilakukan melalui wawancara di satu titik waktu. Penilaian risiko bendungan dilakukan berdasarkan data dan inspeksi periodik. Masalahnya, risiko tidak pernah statis. Mereka berubah setiap hari, bahkan setiap jam. Seperti diungkapkan dalam artikel Raconteur, perusahaan yang menggunakan pendekatan tradisional dengan siklus penilaian risiko tahunan atau periodik akan kesulitan mengikuti perubahan.
2. Kedua, ketidakmampuan menangani volume data besar. Metode tradisional dirancang untuk dunia di mana data terbatas. Wawancara puluhan orang, observasi beberapa lokasi, diskusi kelompok terfokus semua itu bekerja baik ketika data yang perlu dianalisis masih sedikit. Tapi bagaimana kalau perusahaan memiliki ribuan transaksi

per hari, jutaan data pelanggan, dan ratusan sensor di gudang? Metode tradisional akan kewalahan. Artikel *Raconteur* menyebutkan bahwa perusahaan multinasional dengan puluhan ribu karyawan di banyak negara bisa menghabiskan waktu hingga tiga bulan hanya untuk "menatap dan membandingkan" data akses pengguna. Itu pun hanya untuk satu area risiko.

3. Subjektivitas yang tinggi. Wawancara, observasi, dan *expert judgment* sangat bergantung pada siapa yang melakukan penilaian. Dua orang ahli bisa memberikan penilaian yang sangat berbeda untuk risiko yang sama. Studi tentang Bendungan Saguling membuktikan bahwa metode yang berbeda bisa menghasilkan kesimpulan yang berlawanan. Ini bukan berarti para ahli tidak kompeten, tapi lebih pada keterbatasan metode itu sendiri.
4. Tidak mampu menangkap pola kompleks dan tersembunyi. Manusia memiliki keterbatasan dalam memproses informasi. Kita hanya bisa fokus pada beberapa hal dalam satu waktu. Pola-pola yang tersebar di ribuan transaksi atau yang muncul dalam interaksi yang sangat halus seringkali luput dari pengamatan manusia. Padahal, pola-pola inilah yang sering menjadi indikator awal risiko besar.

#### **Revolusi Berbasis Data: Ketika Mesin Ikut Membaca Risiko**

di sinilah titik baliknya. Teknik identifikasi risiko berbasis data hadir untuk menjawab keterbatasan-keterbatasan itu. Ini bukan berarti metode tradisional ditinggalkan sama sekali, tapi diperkuat dan diperluas dengan kemampuan komputasi dan kecerdasan buatan.

- Pertama, apa itu identifikasi risiko berbasis data? Secara sederhana, ini adalah pendekatan yang menggunakan data dalam volume besar, algoritma canggih, dan komputasi cepat untuk menemukan, mengenali, dan mendeskripsikan risiko secara otomatis dan *real-time*. Data bisa berasal dari berbagai sumber: transaksi internal, media sosial, sensor IoT, laporan eksternal, dan ribuan sumber lainnya.
- Kedua, machine learning untuk deteksi pola dan anomali. Ini adalah jantung dari identifikasi risiko berbasis data. Machine learning memungkinkan sistem belajar dari data historis, mengenali pola-pola normal, dan secara otomatis mendeteksi ketika ada penyimpangan.

Artikel ini menguraikan tujuh model ML utama *Linear Regression*, *Logistic Regression*, *Gradient Boosting*, *Random Forest*, *Neural Network*, *Support Vector Machine*, dan *k-NN* serta bagaimana masing-masing model dapat diterapkan untuk keamanan data. Misalnya:

- *Logistic Regression* digunakan untuk klasifikasi akses berbahaya atau tidak berbahaya, deteksi anomali event pada *log server*, dan deteksi data *exfiltration*.
- *Random Forest* digunakan untuk deteksi data leak dari akun user, penilaian risiko akses ke data sensitif, dan model early-warning untuk serangan DDoS.
- *Neural Network*, terutama dengan arsitektur *autoencoder*, unggul untuk deteksi anomali *exfiltration* dan *malware data theft detection*.

- *Gradient Boosting* sangat kuat untuk mendeteksi data breach berbasis pola aktivitas, termasuk slow exfiltration yang dilakukan sedikit demi sedikit tapi konsisten.
- *Support Vector Machine* baik untuk mengklasifikasi *traffic* berisiko dari metadata dan membedakan user legitimate vs malicious.
- *k-NN (k-Nearest Neighbor)* digunakan untuk mendeteksi penyimpangan akses berdasarkan kemiripan pola user dianggap anomali jika perilakunya jauh berbeda dari kelompoknya.

Yang menarik, artikel ini juga membahas pentingnya teknik regularisasi (*L1/LASSO*, *L2/Ridge*, *Elastic Net*) untuk menjaga ketahanan model terhadap data yang berisik dan dinamis. Ini adalah aspek teknis yang sering luput dari diskusi awam bahwa model ML tidak bisa begitu saja dipakai; mereka perlu dikalibrasi dan disesuaikan dengan karakteristik data.

- Ketiga, studi kasus nyata dari Indonesia: inspeksi pipa minyak dan gas dengan AI. Contoh paling menarik datang dari penelitian disertasi Taufik Aditiyawarman, mahasiswa program doktor Teknik Metalurgi dan Material Universitas Indonesia. Dalam disertasinya yang berjudul "*Screening dan Asesmen RBI (Risk Based Inspection) pada Sistem Perpipaan Minyak dan Gas di Indonesia untuk Menunjang Keamanan Produksi Menggunakan Machine Learning dan Deep Learning*", ia menggunakan sampel *ex-spool* pipa berdiameter 16 inci yang diuji melalui berbagai metode metalurgi.

Untuk menganalisis data yang kompleks, ia menerapkan algoritma *machine learning* seperti *AdaBoost*, *Random Forests*, dan *Gradient Boosting*. Teknik *K-Means Clustering* dan *Gaussian Mixture Model* digunakan untuk mengklasifikasikan risiko kegagalan pipa ke dalam tiga kelompok berdasarkan tingkat risikonya rendah, sedang, dan tinggi. Hasilnya, model machine learning yang dikembangkan mampu memprediksi tingkat korosi dan lokasi kerusakan pada pipa dengan cepat dan akurat, memungkinkan tim pemeliharaan mengambil tindakan pencegahan sebelum kegagalan terjadi.

Ini contoh sempurna bagaimana identifikasi risiko berbasis data tidak hanya lebih cepat, tapi juga lebih akurat. Taufik, yang juga menjabat sebagai Direktur Utama PT Kilang Pertamina Internasional, menyatakan bahwa metode ini tidak hanya meningkatkan keselamatan operasional, tetapi juga memberikan keuntungan ekonomi yang signifikan dengan mengurangi biaya pemeliharaan dan risiko kegagalan pipa yang mengakibatkan kerugian besar.

- Keempat, perubahan paradigma: dari menghindari risiko ke meramal peluang. Yang menarik, identifikasi risiko berbasis data juga membuka pintu ke arah yang lebih positif. Artikel dari Telkom University Surabaya membahas bagaimana data kini digunakan bukan hanya untuk menghindari kerugian, tetapi untuk meramalkan peluang pertumbuhan secara proaktif.

Disiplin yang disebut *decision intelligence* kombinasi antara data analytics, AI, dan ilmu perilaku memungkinkan organisasi mengambil keputusan strategis berbasis wawasan

prediktif. Contohnya, Amazon dan Alibaba menggunakan machine learning untuk memprediksi tren pembelian berdasarkan perilaku pengguna secara real-time, sehingga bisa meluncurkan produk baru sebelum tren mencapai puncaknya. Netflix juga menggunakan analisis preferensi tontonan jutaan pengguna untuk memutuskan memproduksi serial seperti *House of Cards*, sebuah langkah yang bukan didasarkan pada intuisi semata, melainkan prediksi data.

Studi dari Provost dan Fawcett (2013) yang dikutip dalam artikel tersebut menyatakan bahwa predictive analytics mampu meningkatkan ROI hingga 300% dibanding metode analisis tradisional ketika diterapkan untuk inovasi produk dan pemasaran. Ini membuktikan bahwa identifikasi risiko berbasis data tidak hanya tentang menghindari hal buruk, tapi juga tentang menangkap hal baik.

### **Perbandingan Langsung: Tradisional vs Berbasis Data**

Sekarang, mari kita coba bandingkan secara langsung kedua pendekatan ini dalam beberapa dimensi.

- **Dimensi Waktu dan Frekuensi:**

Tradisional: Periodik. Dilakukan setahun sekali, triwulan, atau paling cepat sebulan sekali. Siklusnya kaku dan lambat merespons perubahan. Berbasis Data: Kontinu atau real-time. Sistem bekerja 24/7, mendeteksi risiko begitu muncul. Perusahaan farmasi dalam artikel *Raconteur* beralih dari audit triwulan ke analitik *real-time*, dan hasilnya dramatis.

- **Dimensi Cakupan Data:**

Tradisional: Berbasis sampel. Karena keterbatasan manusia dan waktu, hanya sebagian data yang diperiksa. Artikel *Raconteur* menyebutkan bahwa perusahaan kadang menggunakan pendekatan sampling dalam penilaian risiko. Berbasis Data: Berbasis populasi. Seluruh data dianalisis, tidak ada yang terlewat. Dalam deteksi anomali akses, misalnya, sistem bisa memeriksa akses semua karyawan, bukan sampelnya saja.

- **Dimensi Metode:**

Tradisional: Wawancara, observasi, brainstorming, matriks risiko, pohon kejadian, *expert judgment*. Sangat mengandalkan keahlian dan pengalaman manusia. Berbasis Data: *Machine learning*, *deep learning*, analitik prediktif, deteksi anomali, clustering. Sangat mengandalkan algoritma dan komputasi.

- **Dimensi Kecepatan:**

Tradisional: Lambat. Butuh waktu berminggu-minggu atau berbulan-bulan untuk menghasilkan laporan. Perusahaan farmasi butuh tiga bulan untuk mendeteksi anomali akses. Berbasis Data: Cepat. Dalam hitungan detik atau menit, sistem sudah memberi peringatan.

- **Dimensi Akurasi:**

Tradisional: Subjektif, sangat tergantung pada kualitas dan pengalaman penilai. Bisa inkonsisten antar penilai. Studi Bendungan Saguling membuktikan metode berbeda

bisa menghasilkan kesimpulan berlawanan. Berbasis Data: Objektif, konsisten, berdasarkan data. Akurasi meningkat seiring waktu karena model terus belajar.

- **Dimensi Biaya:**

Tradisional: Biaya operasional tinggi untuk tenaga kerja, tapi investasi awal rendah. Cocok untuk organisasi kecil dengan sumber daya terbatas. Berbasis Data: Investasi awal tinggi untuk teknologi dan SDM ahli, tapi biaya operasional jangka panjang bisa lebih rendah karena otomatisasi.

- **Dimensi Kemampuan Deteksi:**

Tradisional: Hanya bisa mendeteksi risiko yang sudah dikenal atau yang bisa dilihat langsung. Sulit mendeteksi pola kompleks dan tersembunyi. Berbasis Data: Mampu mendeteksi pola-pola halus yang tidak kasat mata, termasuk slow exfiltration yang dilakukan sedikit demi sedikit, atau anomali yang tersebar di ribuan transaksi.

- **Dimensi Orientasi:**

Tradisional: Lebih berorientasi ke belakang (*backward-looking*), melihat data historis dan pengalaman masa lalu. Berbasis Data: Bisa berorientasi ke depan (*forward-looking*) dengan predictive analytics, meramalkan risiko dan peluang sebelum terjadi.

#### **Bukan Saling Menggantikan, Tapi Saling Melengkapi**

Setelah semua perbandingan ini, penting untuk dicatat bahwa identifikasi risiko berbasis data bukan untuk menggantikan metode tradisional, melainkan melengkapi. Ada beberapa alasan. Pertama, metode tradisional tetap relevan untuk risiko-risiko yang sulit diukur secara kuantitatif. Risiko reputasi, risiko budaya organisasi, risiko perubahan regulasi yang belum memiliki data historis semua ini lebih cocok didekati dengan wawancara, diskusi, dan expert judgment. Data saja tidak cukup untuk memahami nuansa dan konteks.

Kedua, metode tradisional memberikan pemahaman kontekstual yang tidak bisa diberikan data. Wawancara dengan karyawan bisa mengungkapkan dinamika internal yang tidak tercermin dalam angka. Observasi langsung bisa menangkap hal-hal yang tidak terekam dalam sensor. Kombinasi antara data dan pemahaman kontekstual inilah yang paling kuat. Ketiga, metode berbasis data membutuhkan data berkualitas. Kalau data yang dimiliki kotor, tidak lengkap, atau bias, maka hasil analisisnya juga akan bias. Di sinilah peran manusia untuk memastikan kualitas data dan menginterpretasi hasil dengan bijak.

Keempat, metode berbasis data tetap butuh validasi dan pengawasan manusia. Model ML bisa salah, bisa bias, bisa belajar hal yang salah dari data. Manusia harus terus memantau, mengevaluasi, dan mengkalibrasi ulang model. Pendekatan hibrida ini yang dijalankan oleh perusahaan-perusahaan maju. Mereka tidak membuang metode tradisional, tapi memperkuatnya dengan kecerdasan buatan. Hasilnya, identifikasi risiko menjadi lebih cepat, lebih akurat, lebih komprehensif, dan yang paling penting lebih proaktif.

### **4.3 PEMANFAATAN AI UNTUK MEMETAKAN RISIKO OPERASIONAL DAN PASAR**

Mari kita duduk sejenak dan coba kita renungkan bersama, bagaimana sebenarnya wajah dunia perdagangan kita hari ini? Kalau kita perhatikan, di balik layar monitor para pedagang besar atau di sela-sela rak gudang yang menjulang tinggi, ada kekuatan yang bekerja

dalam diam, sesuatu yang kita sebut sebagai Kecerdasan Buatan atau AI. Sering kali, dalam obrolan hangat di selasar kampus atau saat diskusi serius di ruang rapat, orang-orang bicara tentang AI seolah itu adalah tongkat sihir yang bisa menebak masa depan dengan sempurna. Padahal, kalau mau jujur, memanfaatkan AI untuk memetakan risiko operasional dan pasar itu ibarat kita sedang belajar membaca bahasa alam yang sangat rumit; ia butuh ketelitian, butuh data yang jujur, dan yang paling penting, ia butuh sentuhan kebijaksanaan manusia agar tidak tersesat dalam angka-angka.

Dalam dunia bisnis dagang, risiko itu seperti dua sisi mata uang yang tidak bisa dipisahkan. Ada risiko operasional yang bicara soal "jeroan" Perusahaan mulai dari gangguan rantai pasok, kerusakan mesin, sampai kesalahan manusia dan ada risiko pasar yang bicara soal keganasan dunia luar, seperti fluktuasi harga komoditas atau perubahan selera konsumen yang secepat kilat. Secara mendasar, jika kita menilik perspektif dari Vaughan dan Vaughan (2007), risiko dipandang sebagai suatu kondisi di mana terdapat kemungkinan terjadinya penyimpangan dari hasil yang kita harapkan. Nah, peran AI di sini adalah menjadi "radar" yang jauh lebih sensitif dibandingkan cara-cara tradisional yang sering kali telat menyadari datangnya badai.



**Gambar 4.2** Visualisasi sistem pemantauan risiko operasional berbasis AI yang mengintegrasikan data dari sensor logistik dan kinerja internal untuk mendeteksi anomali secara real-time.

Mari kita bedah pelan-pelan soal risiko operasional terlebih dahulu. Bayangkan sebuah perusahaan distribusi besar yang memiliki ribuan armada. Dengan AI, kita tidak lagi menunggu truk mogok untuk melakukan perbaikan. Algoritma *Machine Learning* bisa memprediksi kapan sebuah komponen akan rusak hanya dari getaran atau suhu yang terekam oleh sensor IoT. Ini yang disebut sebagai *predictive maintenance*. James Lam (2014) dalam bukunya yang menjadi rujukan banyak praktisi menekankan bahwa manajemen risiko harus menjadi bagian dari desain strategi, bukan sekadar pemadam kebakaran saat krisis terjadi. AI membantu kita

mengidentifikasi celah-celah kecil di gudang atau jalur distribusi sebelum celah itu menjadi lubang besar yang menelan modal kita. Rasanya memang sedikit ajaib, tapi ini adalah hasil dari pengolahan data yang sangat tekun.

Namun, yang jauh lebih menantang adalah memetakan risiko pasar. Pasar itu ibarat samudra yang cuacanya bisa berubah dalam hitungan menit. AI masuk ke sana dengan kemampuan mengolah *Big Data* yang luar biasa masif. Ia memantau berita global, kebijakan politik di negara produsen, hingga tren tagar di media sosial untuk memetakan risiko harga. Jika harga bahan baku di tingkat global diprediksi melonjak karena konflik geopolitik, AI akan memberikan sinyal peringatan dini. Manfaatnya nyata; perusahaan bisa melakukan lindung nilai (*hedging*) atau mencari pemasok alternatif lebih awal. Tanpa AI, kita mungkin baru menyadari kenaikan harga saat tagihan sudah sampai di meja akuntansi. Kan sudah terlambat kalau begitu?

Jeda sejenak, mari kita pikirkan sisi manusianya. Ada ketakutan bahwa AI akan mengambil alih keputusan sepenuhnya. Tapi coba renungkan ini: AI mungkin jago melihat pola, tapi ia tidak memiliki "firasat" atau konteks moral. Ia tidak tahu kalau sebuah kebijakan pasar mungkin akan memukul pedagang kecil secara tidak adil. Di sinilah tugas kita sebagai manusia. AI memetakan risikonya, memberikan kita peta yang sangat detail, tapi kitalah yang memegang kemudi untuk memutuskan ke mana kapal akan berlayar. Hopkin (2018) mengingatkan bahwa identifikasi risiko yang proaktif harus tetap sejalan dengan nilai-nilai organisasi. Jangan sampai karena terlalu mengejar efisiensi dari data AI, kita melupakan aspek etika dan keberlanjutan.

Ada juga risiko yang lahir dari AI itu sendiri, yang sering disebut sebagai risiko model. Bagaimana kalau data yang dipelajari AI itu bias? Atau bagaimana kalau AI mengalami "halusinasi" karena ada gangguan pada sinyal data? Ini adalah tantangan baru yang sangat manusiawi untuk dikelola. Kita tidak bisa menyerahkan nasib perusahaan pada kotak hitam (*black box*) tanpa pengawasan. Kita butuh apa yang disebut sebagai *Explainable AI* (XAI), di mana sistem bisa menjelaskan mengapa ia menganggap sebuah transaksi itu berisiko tinggi. Transparansi ini penting agar kita tidak mengambil keputusan yang salah hanya karena "kata komputer begitu".



**Gambar 4.3** Model kolaborasi antara analis manusia dan kecerdasan buatan dalam memvalidasi sinyal risiko pasar, memastikan keputusan tetap memiliki dasar konteks sosial dan ekonomi.

Satu hal yang sering luput dari diskusi adalah soal kecepatan adaptasi. Perusahaan dagang yang masih menggunakan metode manual untuk memetakan risiko pasar akan sangat tertinggal dibandingkan mereka yang sudah menggunakan AI. Namun, teknologi ini juga bukan tanpa biaya. Investasi pada infrastruktur data dan pelatihan staf itu mahal dan melelahkan. Sering kali terjadi gesekan di internal perusahaan antara orang-orang lama yang percaya pada pengalaman dan anak-anak muda yang mendewakan data. Kuncinya adalah jembatan komunikasi. Pengalaman para senior sangat dibutuhkan untuk memvalidasi apakah hasil pemetaan AI itu masuk akal atau tidak di dunia nyata.

Pada akhirnya, memanfaatkan AI untuk memetakan risiko operasional dan pasar adalah perjalanan panjang untuk menjadi lebih rendah hati di hadapan data, namun tetap berdaulat sebagai manusia. Kita menggunakan teknologi ini bukan untuk menghilangkan risiko karena itu mustahil tapi untuk mengenali wajah risiko tersebut dengan lebih jelas. Dengan begitu, kita bisa mengambil langkah yang lebih berani dan terukur. Bisnis dagang adalah tentang kepercayaan, dan AI membantu kita membangun kepercayaan itu di atas fondasi data yang kokoh, bukan sekadar tebakan yang penuh keraguan.

Ingatlah, seberapa pun canggihnya algoritma yang kita miliki, jantung dari perdagangan tetaplah pemenuhan kebutuhan hidup sesama manusia. Jika AI membantu kita memitigasi risiko sehingga barang sampai ke tangan konsumen dengan lebih cepat dan harga yang lebih adil, maka kita sudah menjalankan peran teknologi dengan benar. Manajemen risiko berbasis AI bukan hanya soal menyelamatkan margin keuntungan, tapi soal menjaga keberlangsungan ekosistem perdagangan agar tetap sehat dan tangguh di tengah dunia yang makin tidak menentu ini.

#### 4.4 ANALISIS DATA TRANSAKSI UNTUK MENDETEKSI POLA RISIKO

Data transaksi merupakan jejak perilaku operasional yang paling dekat dengan aktivitas perdagangan. Setiap pembelian, penerimaan barang, perpindahan stok, penjualan, retur, diskon, perubahan harga, dan pembayaran menyimpan sinyal yang dapat digunakan untuk mengenali risiko. Analisis tidak dimulai dengan mencari kesalahan semata, melainkan dengan menetapkan pola normal, lalu menguji penyimpangan yang relevan terhadap sasaran perusahaan.

Proses analisis yang baik mencakup lima langkah. Pertama, tentukan tujuan kontrol, misalnya mencegah kehilangan persediaan atau mendeteksi transaksi tidak wajar. Kedua, pilih atribut data yang dapat diamati, seperti waktu transaksi, nominal, pengguna, lokasi, produk, metode pembayaran, dan riwayat pembatalan. Ketiga, bangun baseline berdasarkan pola historis dan aturan bisnis. Keempat, beri skor pada penyimpangan. Kelima, lakukan verifikasi manusia sebelum menetapkan kesimpulan atau tindakan korektif.

| Sinyal data                             | Pola yang diamati                            | Risiko yang mungkin                        | Tindak lanjut awal                            |
|-----------------------------------------|----------------------------------------------|--------------------------------------------|-----------------------------------------------|
| Penjualan di luar jam normal            | Lonjakan frekuensi atau nominal              | Penyalahgunaan akun/fraud                  | Verifikasi pengguna, perangkat, dan otorisasi |
| Diskon berulang oleh pengguna yang sama | Diskon mendekati batas kewenangan            | Kebocoran margin/konflik kepentingan       | Uji sampel transaksi dan persetujuan          |
| Retur tinggi pada produk tertentu       | Rasio retur menyimpang dari kelompok sejenis | Kualitas produk atau manipulasi penjualan  | Telusuri batch, pemasok, dan alasan retur     |
| Selisih stok sistem dan fisik           | Pola berulang pada lokasi/SKU tertentu       | Kehilangan, salah catat, atau proses lemah | Stock opname terarah dan review akses         |
| Pembayaran gagal atau terlambat         | Perubahan pola pelanggan                     | Risiko kredit dan likuiditas               | Tinjau limit, aging, dan kebijakan penagihan  |

##### PRINSIP INTERPRETASI ANOMALI

Anomali adalah sinyal untuk diperiksa, bukan bukti otomatis bahwa telah terjadi kecurangan. Konteks proses, kualitas data, perubahan musiman, promosi, gangguan sistem, dan penjelasan pemilik proses harus dipertimbangkan sebelum keputusan diambil.

Dalam praktik pembelajaran, mahasiswa dapat menggunakan data transaksi sederhana untuk menghitung frekuensi, nilai rata-rata, deviasi, rasio retur, umur piutang, dan perputaran persediaan. Teknik tersebut kemudian dapat diperluas dengan clustering, isolation forest, atau model klasifikasi. Namun, hasil model tetap harus diterjemahkan ke dalam pernyataan risiko yang jelas: penyebab, peristiwa, dampak, pemilik risiko, kontrol yang ada, dan bukti yang diperlukan.

**KESIMPULAN**

Identifikasi risiko berbasis AI memperluas kemampuan organisasi untuk menganalisis populasi data, mendeteksi anomali, dan mengenali sinyal lebih cepat. Keunggulan tersebut harus dipadukan dengan wawancara, observasi, expert judgment, dan pemahaman konteks. Risiko yang teridentifikasi perlu dirumuskan secara jelas sebagai hubungan antara penyebab, peristiwa, dan dampak agar dapat dilanjutkan ke analisis serta penilaian.

**LATIHAN SOAL**

1. Bandingkan identifikasi risiko tradisional dan berbasis AI dari sisi cakupan, kecepatan, dan bias.
2. Susun lima sinyal data untuk mendeteksi risiko persediaan.
3. Jelaskan mengapa anomali tidak selalu berarti fraud.
4. Rancang proses validasi manusia atas alert risiko pasar.
5. Buat daftar risiko baru yang muncul akibat penggunaan AI dalam identifikasi.

# BAB 5

## ANALISIS DAN PENILAIAN RISIKO BERBASIS DATA DAN AI

---

Bagaimana risiko diukur, dibandingkan, dan diprioritaskan secara konsisten?

### CAPAIAN PEMBELAJARAN

- Menetapkan konteks, kriteria, dan unit analisis.
- Menilai kualitas data dan ketidakpastian.
- Memilih teknik analisis yang sesuai.
- Menyusun model skoring dan validasi.

DIKO • Mengevaluasi residual dan portofolio risiko.

### 5.1 ORIENTASI ANALISIS DAN PENILAIAN RISIKO

Identifikasi risiko menjawab pertanyaan tentang apa yang dapat terjadi, sedangkan analisis risiko menjelaskan seberapa besar kemungkinan peristiwa tersebut terjadi, seberapa berat dampaknya, dan seberapa tinggi tingkat ketidakpastian yang menyertai penilaian. Dalam perusahaan dagang, analisis yang baik membantu manajemen membedakan gangguan kecil yang dapat ditangani oleh prosedur rutin dari risiko yang dapat mengancam arus kas, reputasi, kepatuhan, atau kelangsungan usaha. Ketika AI digunakan, kemampuan analisis meningkat karena data transaksi, persediaan, perilaku pelanggan, logistik, dan pasar dapat diproses dalam skala yang jauh lebih besar. Namun, kualitas kesimpulan tetap bergantung pada tujuan analisis, mutu data, metode pengukuran, dan kemampuan manusia memahami konteks bisnis.

Penilaian risiko tidak seharusnya dipahami sebagai kegiatan memberi warna pada matriks. Nilai rendah, sedang, tinggi, atau ekstrem hanya bermanfaat apabila terkait dengan keputusan yang jelas. Setiap tingkat risiko perlu dihubungkan dengan pemilik risiko, batas toleransi, tenggat penanganan, kebutuhan eskalasi, dan indikator pemantauan. Dalam praktik yang matang, angka tidak berdiri sendiri. Skor harus disertai penjelasan mengenai asumsi, sumber data, rentang kesalahan, kondisi yang dapat mengubah hasil, dan konsekuensi apabila manajemen tidak bertindak.

AI dapat membantu menghitung pola kemungkinan berdasarkan data historis, memprediksi besaran kerugian, mengelompokkan risiko yang serupa, dan mengenali anomali yang tidak terlihat oleh analisis manual. Meskipun demikian, model tidak dapat menentukan sendiri risiko mana yang pantas diterima secara etis atau strategis. Keputusan tersebut memerlukan penilaian manusia mengenai kepentingan pelanggan, kewajiban hukum, nilai organisasi, dan dampak jangka panjang. Karena itu, analisis berbasis AI sebaiknya diposisikan sebagai *augmented risk assessment*: mesin memperluas daya lihat, sedangkan manusia menetapkan makna dan tindakan.

#### PRINSIP KUNCI

Analisis risiko yang andal harus dapat ditelusuri, dapat dijelaskan, dapat diuji ulang, dan relevan dengan keputusan. Ketepatan matematis tidak cukup apabila data, asumsi, atau tujuan penggunaannya tidak tepat.



**Catatan:** pengukuran kuantitatif tidak menggantikan penilaian konteks, tetapi memperkuat konsistensi keputusan

**Gambar 5.1** Alur analisis dan penilaian risiko berbasis AI dari data hingga respons.

*Sumber: diolah untuk diktat ini.*

### Menetapkan Konteks, Kriteria, dan Unit Analisis

Sebelum model atau matriks digunakan, organisasi harus menetapkan konteks. Konteks mencakup sasaran bisnis, proses yang dianalisis, pihak yang terdampak, horizon waktu, wilayah operasi, peraturan yang berlaku, serta kondisi internal dan eksternal. Risiko kekurangan stok pada toko harian memiliki horizon waktu yang berbeda dengan risiko salah memilih platform teknologi untuk lima tahun. Tanpa konteks yang jelas, data yang benar dapat menghasilkan keputusan yang salah karena dianalisis untuk pertanyaan yang keliru.

Unit analisis juga harus ditentukan. Organisasi dapat menilai risiko pada tingkat transaksi, produk, pelanggan, pemasok, cabang, proses, model AI, atau portofolio perusahaan. Satu risiko pada tingkat transaksi mungkin kecil, tetapi menjadi material ketika terjadi berulang dalam jutaan transaksi. Sebaliknya, peristiwa yang jarang terjadi dapat tetap menjadi prioritas apabila dampaknya menyangkut keselamatan, pelanggaran hak, kebocoran data sensitif, atau kegagalan operasional luas. Pemilihan unit analisis memengaruhi data yang dikumpulkan, model yang digunakan, dan cara hasil dilaporkan.

Kriteria risiko merupakan aturan untuk menilai signifikansi risiko. Kriteria biasanya mencakup skala kemungkinan, skala dampak, kecepatan terjadinya dampak, durasi pemulihan, tingkat keterdeteksian, dan kekuatan kontrol yang telah ada. Perusahaan dagang dapat menambahkan dimensi yang spesifik, misalnya dampak terhadap ketersediaan barang, ketepatan pengiriman, margin, pengalaman pelanggan, kualitas produk, kepatuhan perlindungan data, atau hubungan dengan pemasok. Kriteria harus disepakati sebelum penilaian agar hasil tidak dimanipulasi untuk membenarkan keputusan yang telah diambil sebelumnya.

*Risk appetite* menjelaskan jumlah dan jenis risiko yang bersedia diambil organisasi untuk mencapai tujuan, sedangkan *risk tolerance* menerjemahkannya menjadi batas yang lebih operasional. Contohnya, perusahaan dapat menerima eksperimen rekomendasi produk dengan dampak finansial terbatas, tetapi menetapkan toleransi sangat rendah terhadap AI yang secara otomatis memblokir pelanggan tanpa mekanisme banding. Batas ini perlu dinyatakan secara terukur, misalnya maksimum persentase kesalahan, nilai kerugian, waktu henti, jumlah keluhan, atau tingkat penyimpangan antar kelompok pelanggan.

**Tabel 5.1** Contoh kriteria penilaian risiko perusahaan dagang

| Dimensi                 | Skala rendah                          | Skala sedang                     | Skala tinggi                                         | Bukti utama                                        |
|-------------------------|---------------------------------------|----------------------------------|------------------------------------------------------|----------------------------------------------------|
| <b>Kemungkinan</b>      | Kurang dari sekali dalam tiga tahun   | Satu sampai empat kali per tahun | Terjadi bulanan atau lebih sering                    | Log kejadian, tren, dan <i>expert judgment</i>     |
| <b>Dampak finansial</b> | Dapat diserap unit kerja              | Memerlukan realokasi anggaran    | Mengganggu arus kas atau target strategis            | Nilai transaksi, margin, dan skenario kerugian     |
| <b>Dampak pelanggan</b> | Keluhan terbatas dan mudah dipulihkan | Keluhan lintas segmen atau kanal | Kerugian luas, hak terganggu, atau kepercayaan turun | Keluhan, <i>refund</i> , <i>churn</i> , dan survei |

|                     |                                     |                                      |                                       |                                                     |
|---------------------|-------------------------------------|--------------------------------------|---------------------------------------|-----------------------------------------------------|
| <b>Kecepatan</b>    | Dampak muncul lebih dari satu bulan | Dampak muncul dalam hari atau minggu | Dampak menyebar dalam menit atau jam  | Waktu deteksi, respons, dan pemulihan               |
| <b>Keterbalikan</b> | Keputusan mudah dibatalkan          | Membutuhkan biaya dan koordinasi     | Sulit atau tidak mungkin dipulihkan   | <i>Rollback</i> , mekanisme banding, dan kompensasi |
| <b>Kepatuhan</b>    | Tidak menyentuh kewajiban material  | Memerlukan review fungsi hukum       | Potensi pelanggaran hukum atau sanksi | Register regulasi dan <i>legal opinion</i>          |

## 5.2 DATA SEBAGAI FONDASI PENILAIAN RISIKO

Model penilaian risiko bekerja seperti cermin terhadap data yang digunakan. Jika data tidak lengkap, terlambat, tidak konsisten, atau bias, hasil model akan memantulkan kelemahan tersebut. Karena itu, pemeriksaan kualitas data harus dilakukan sebelum pemodelan. Dimensi yang umum diperiksa meliputi kelengkapan, akurasi, konsistensi, ketepatan waktu, keunikan, validitas, representativitas, dan keterlacakan. Dalam perusahaan dagang, masalah sederhana seperti kode produk yang berbeda antar cabang dapat mengacaukan prediksi permintaan dan membuat risiko persediaan terlihat lebih kecil atau lebih besar dari kondisi sebenarnya.

Data historis tidak selalu mewakili masa depan. Perubahan pola konsumen, inflasi, promosi pesaing, gangguan cuaca, kebijakan platform, atau perubahan regulasi dapat menyebabkan *concept drift*. Model yang akurat pada tahun sebelumnya mungkin gagal ketika kondisi pasar berubah. Oleh sebab itu, analisis perlu memisahkan pola yang stabil dari pola yang sensitif terhadap perubahan. Organisasi juga perlu menilai apakah periode data mencakup kejadian ekstrem. Data penjualan pada kondisi normal tidak cukup untuk menilai risiko ketika terjadi gangguan rantai pasok atau lonjakan permintaan mendadak.

Ketika data pribadi digunakan, kebutuhan analisis harus diseimbangkan dengan prinsip minimisasi data. Tidak semua atribut yang tersedia harus dipakai. Model risiko kredit pelanggan, misalnya, harus menggunakan variabel yang relevan dan dapat dipertanggungjawabkan, bukan sekadar variabel yang secara statistik berkorelasi. Variabel proksi dapat menyebabkan diskriminasi tidak langsung. Alamat tempat tinggal, jenis perangkat, atau pola waktu belanja mungkin berkorelasi dengan kelompok sosial tertentu dan menghasilkan perlakuan yang tidak adil apabila digunakan tanpa kajian dampak.

Data eksternal dapat memperkaya analisis, tetapi sumbernya harus dinilai. Organisasi perlu memeriksa legalitas akses, lisensi, metode pengumpulan, tingkat pembaruan, definisi variabel, dan potensi manipulasi. Data media sosial dapat memberikan sinyal tren, tetapi juga mengandung akun palsu, kampanye terkoordinasi, dan bias demografis. Data cuaca dapat membantu perencanaan distribusi, tetapi harus dipadankan dengan lokasi dan waktu yang tepat. Setiap sumber data perlu memiliki pemilik, dokumentasi, dan aturan retensi yang jelas.

**Tabel 5.2** Dimensi kualitas data untuk penilaian risiko

| Dimensi                  | Pertanyaan pengujian                           | Contoh indikator                                | Tindakan bila gagal                                          |
|--------------------------|------------------------------------------------|-------------------------------------------------|--------------------------------------------------------------|
| <b>Kelengkapan</b>       | Apakah kolom dan periode penting tersedia?     | Persentase nilai kosong per variabel            | Lengkapi sumber, imputasi terkontrol, atau batasi penggunaan |
| <b>Akurasi</b>           | Apakah data sesuai kondisi nyata?              | Hasil rekonsiliasi dengan dokumen sumber        | Perbaiki master data dan kontrol input                       |
| <b>Konsistensi</b>       | Apakah definisi sama antar sistem dan cabang?  | Selisih kode, satuan, dan format                | Standardisasi definisi dan mapping                           |
| <b>Ketepatan waktu</b>   | Apakah data cukup baru untuk keputusan?        | Usia data dan keterlambatan feed                | Terapkan <i>freshness check</i> dan <i>fallback</i>          |
| <b>Representativitas</b> | Apakah kelompok penting terwakili?             | Distribusi per wilayah, produk, dan segmen      | Tambah sampel atau batasi generalisasi                       |
| <b>Lineage</b>           | Dapatkah data ditelusuri dari sumber ke model? | Persentase elemen dengan owner dan transformasi | Bangun katalog, log transformasi, dan <i>versioning</i>      |

### Pengukuran Kemungkinan, Dampak, dan Ketidakpastian

Kemungkinan dapat dinilai secara kualitatif, semi-kuantitatif, atau kuantitatif. Pendekatan kualitatif menggunakan kategori seperti jarang, mungkin, atau hampir pasti. Pendekatan semi-kuantitatif memberi skor numerik pada kategori untuk memudahkan pemeringkatan. Pendekatan kuantitatif menggunakan frekuensi, probabilitas, distribusi statistik, atau simulasi. Pilihan metode harus disesuaikan dengan kualitas data dan materialitas keputusan. Menggunakan angka dengan banyak desimal tidak otomatis membuat analisis lebih akurat apabila datanya lemah.

Dampak sebaiknya dipandang secara multidimensi. Kerugian finansial sering menjadi fokus utama, tetapi dampak dapat mencakup operasi, pelanggan, reputasi, hukum, keselamatan, lingkungan, dan strategi. Satu kegagalan *chatbot* mungkin tidak menimbulkan kerugian langsung, tetapi dapat menyebarkan informasi yang salah kepada ribuan pelanggan. Penilaian perlu mempertimbangkan dampak langsung dan tidak langsung, dampak jangka pendek dan jangka panjang, serta pihak yang menanggung dampak. Dalam kasus AI, pihak yang dirugikan mungkin berbeda dari pihak yang menikmati manfaat efisiensi.

Kecepatan risiko atau *risk velocity* menunjukkan seberapa cepat dampak muncul setelah peristiwa terjadi. Kebocoran data dan harga otomatis yang salah dapat menyebar dalam hitungan menit, sedangkan bias model mungkin baru terlihat setelah berbulan-bulan. Risiko dengan kecepatan tinggi memerlukan indikator *real-time*, tombol penghentian, dan jalur eskalasi yang lebih singkat. Durasi dampak dan waktu pemulihan juga penting. Gangguan sistem selama dua jam mungkin pulih cepat, tetapi kehilangan kepercayaan pelanggan dapat berlangsung jauh lebih lama.

Ketidakpastian harus dinyatakan, bukan disembunyikan. Model dapat menghasilkan rentang prediksi, interval kepercayaan, atau beberapa skenario. Manajemen perlu memahami bahwa estimasi kerugian bukan angka pasti. Untuk keputusan penting, organisasi dapat

menggunakan skenario optimistis, dasar, dan stres; analisis sensitivitas; atau simulasi Monte Carlo. Tujuannya bukan meramalkan masa depan secara sempurna, melainkan memahami faktor mana yang paling memengaruhi hasil dan kapan keputusan harus ditinjau ulang.



**Gambar 5.2** Contoh matriks risiko 5 x 5 dan cara membaca tingkat prioritas.

*Sumber: diolah untuk diktat ini.*

**Tabel 5.3** Perbandingan metode pengukuran risiko

| Metode                  | Kondisi penggunaan                          | Kelebihan                                  | Keterbatasan                                     |
|-------------------------|---------------------------------------------|--------------------------------------------|--------------------------------------------------|
| <b>Kualitatif</b>       | Data terbatas atau risiko baru              | Cepat dan mudah dipahami                   | Subjektif dan sulit dibandingkan lintas penilai  |
| <b>Semi-kuantitatif</b> | Prioritisasi portofolio                     | Konsisten dan mudah divisualkan            | Skor ordinal sering diperlakukan terlalu presisi |
| <b>Kuantitatif</b>      | Data cukup dan keputusan material           | Dapat menghitung distribusi dan skenario   | Membutuhkan data, asumsi, dan keahlian           |
| <b>Skenario</b>         | Peristiwa ekstrem atau perubahan struktural | Menguji kesiapan dan efek domino           | Hasil bergantung pada kualitas skenario          |
| <b>Simulasi</b>         | Banyak variabel tidak pasti                 | Menampilkan rentang hasil dan sensitivitas | Kompleks dan dapat memberi rasa pasti palsu      |

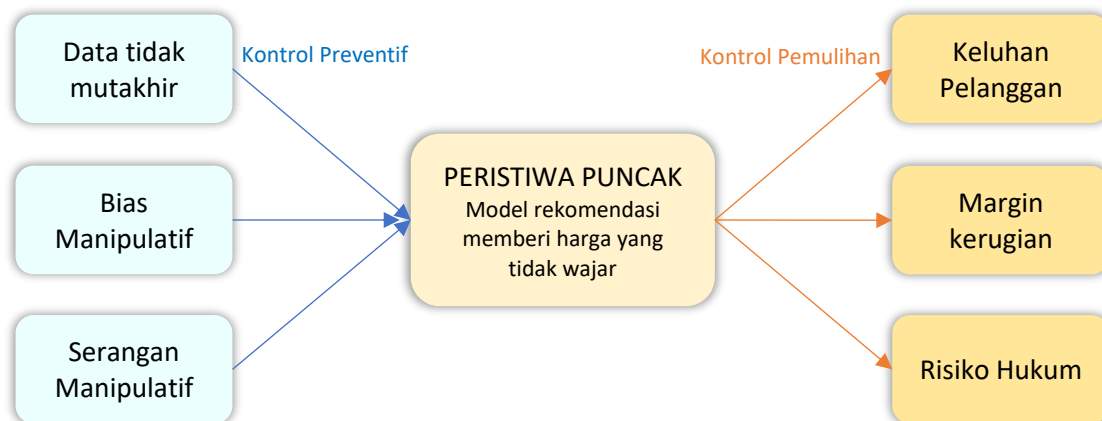
### 5.3 TEKNIK ANALISIS YANG RELEVAN BAGI PERUSAHAAN DAGANG

Analisis deskriptif menjelaskan apa yang telah terjadi melalui tren, frekuensi, distribusi, dan perbandingan. Teknik ini cocok untuk memetakan retur, selisih stok, keterlambatan pemasok, atau pola keluhan. Analisis diagnostik menjelaskan mengapa kejadian terjadi, misalnya melalui *drill-down*, korelasi, diagram sebab-akibat, atau *root cause analysis*. Kedua pendekatan ini menjadi dasar sebelum organisasi beralih ke prediksi. Model yang canggih tidak akan banyak membantu apabila definisi masalah dan penyebab dasarnya belum dipahami.

Analisis prediktif memperkirakan apa yang mungkin terjadi. Regresi dapat digunakan untuk mengestimasi nilai kerugian atau permintaan, klasifikasi untuk menilai kemungkinan *fraud* atau gagal bayar, dan *time-series* untuk memprediksi penjualan serta kebutuhan stok. *Clustering* membantu mengenali kelompok pelanggan, produk, atau pemasok dengan karakteristik risiko serupa. Deteksi anomali berguna ketika kejadian berisiko jarang dan label historis terbatas. Pemilihan teknik harus didasarkan pada tujuan, ketersediaan label, interpretabilitas, dan biaya kesalahan.

Analisis skenario sangat penting ketika data historis tidak cukup. Tim dapat merancang skenario gangguan pelabuhan, pemadaman pusat data, perubahan komisi *marketplace*, serangan *ransomware*, atau larangan regulasi. AI dapat membantu mensimulasikan dampak pada persediaan, arus kas, dan pelayanan. Namun, skenario tetap harus divalidasi oleh orang yang memahami operasi. Skenario yang tampak teknis tetapi mengabaikan kapasitas gudang, pola kontrak, atau perilaku pelanggan dapat menyesatkan.

*Bow-tie analysis* menghubungkan penyebab, peristiwa puncak, konsekuensi, kontrol preventif, dan kontrol pemulihan. Teknik ini berguna karena memaksa organisasi melihat kontrol sebelum dan sesudah kejadian. Dalam penggunaan AI untuk penetapan harga, penyebab dapat berupa data tidak mutakhir, manipulasi input, atau konfigurasi promosi yang salah. Peristiwa puncaknya adalah harga yang tidak wajar, sedangkan konsekuensinya dapat berupa kerugian margin, keluhan, dan pelanggaran perlindungan konsumen.



**Gambar 5.3** Contoh analisis bow-tie untuk risiko penetapan harga berbasis AI.

Sumber: diolah untuk diktat ini.

**Tabel 5.4** Teknik analisis risiko dan contoh penerapannya

| Teknik            | Pertanyaan utama          | Contoh perusahaan dagang                 | Output                               |
|-------------------|---------------------------|------------------------------------------|--------------------------------------|
| <b>Deskriptif</b> | Apa yang telah terjadi?   | Tren retur dan selisih stok              | Distribusi, frekuensi, dan tren      |
| <b>Diagnostik</b> | Mengapa terjadi?          | Akar keterlambatan pengiriman            | Penyebab utama dan faktor kontribusi |
| <b>Prediktif</b>  | Apa yang mungkin terjadi? | Prediksi <i>stockout</i> dan gagal bayar | Probabilitas atau nilai perkiraan    |

| Preskriptif     | Tindakan apa yang optimal?                       | Rekomendasi alokasi stok               | Alternatif dan trade-off        |
|-----------------|--------------------------------------------------|----------------------------------------|---------------------------------|
| Deteksi anomali | Apa yang menyimpang dari normal?                 | Transaksi fraud atau akses tidak biasa | Alert dan skor anomali          |
| Bow-tie         | Bagaimana penyebab dan konsekuensi dikendalikan? | Harga otomatis tidak wajar             | Kontrol preventif dan pemulihan |

#### 5.4 MODEL SKORING RISIKO BERBASIS AI

*Risk scoring* mengubah sejumlah indikator menjadi nilai yang membantu prioritas. Skor dapat dibangun dengan aturan sederhana, model statistik, machine learning, atau kombinasi ketiganya. Dalam penilaian pemasok, indikator dapat mencakup ketepatan pengiriman, kualitas barang, stabilitas finansial, konsentrasi sumber, keamanan siber, dan kepatuhan. Dalam penilaian transaksi, indikator dapat mencakup nilai, frekuensi, lokasi, perangkat, pola pembayaran, dan perbedaan dari perilaku normal.

Organisasi harus membedakan skor sebagai alat keputusan dari keputusan itu sendiri. Skor 85 tidak memiliki makna tanpa definisi, rentang, ambang, dan tindakan. Apakah 85 berarti berisiko tinggi, perlu pemeriksaan tambahan, atau harus ditolak? Ambang yang terlalu ketat dapat menimbulkan banyak *false positive*, menghambat pelanggan sah, dan menambah beban verifikasi. Ambang yang terlalu longgar dapat meloloskan *fraud*. Karena itu, pemilihan ambang harus mempertimbangkan biaya dua jenis kesalahan dan kapasitas tim tindak lanjut. Model skoring perlu dikalibrasi. Jika model menyatakan peluang gagal bayar 20 persen, dalam kelompok kasus serupa seharusnya sekitar 20 persen benar-benar gagal. Model dapat memiliki akurasi klasifikasi yang baik tetapi kalibrasi buruk. Untuk penggunaan operasional, organisasi perlu menilai diskriminasi model, kalibrasi, stabilitas, fairness, dan ketahanan terhadap perubahan. Pengujian harus dilakukan pada data yang tidak digunakan untuk pelatihan dan, bila memungkinkan, pada periode waktu yang berbeda.

*Explainability* diperlukan agar pengguna memahami faktor yang mendorong skor. Penjelasan global menunjukkan variabel yang berpengaruh secara umum, sedangkan penjelasan lokal menjelaskan satu keputusan. Penjelasan harus disesuaikan dengan audiens. Analis mungkin membutuhkan kontribusi fitur, manajer membutuhkan alasan bisnis, pelanggan membutuhkan penjelasan yang sederhana dan mekanisme koreksi. Organisasi harus berhati-hati agar penjelasan tidak membocorkan detail yang memudahkan pelaku mengakali sistem.

**Tabel 5.5** Kontrol minimum model *risk scoring*

| Area   | Kontrol minimum                                     | Bukti                                               |
|--------|-----------------------------------------------------|-----------------------------------------------------|
| Tujuan | Definisi keputusan, pengguna, dan konsekuensi       | <i>Use-case charter</i> dan <i>approval</i>         |
| Data   | Kualitas, representativitas, legalitas, dan lineage | <i>Dataset sheet</i> dan hasil <i>quality check</i> |

|                   |                                                              |                                               |
|-------------------|--------------------------------------------------------------|-----------------------------------------------|
| <b>Model</b>      | <i>Baseline</i> , performa, kalibrasi, dan interpretabilitas | Model card dan laporan pengujian              |
| <b>Ambang</b>     | <i>Trade-off false positive</i> dan <i>false negative</i>    | Analisis biaya kesalahan dan keputusan komite |
| <b>Operasi</b>    | Human review, override, fallback, dan eskalasi               | SOP, log, dan rekaman pelatihan               |
| <b>Pemantauan</b> | Drift, fairness, insiden, dan perubahan                      | Dashboard, alert, dan change log              |

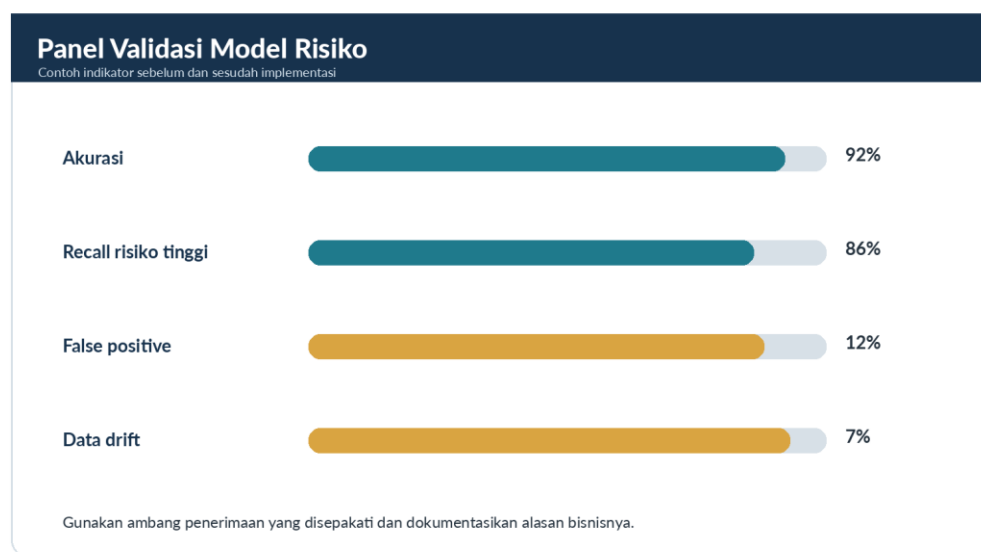
### Validasi Model dan Pengujian Sebelum Penggunaan

Validasi adalah proses independen untuk menilai apakah model sesuai dengan tujuan, data, dan konteks penggunaan. Validasi tidak hanya memeriksa performa teknis, tetapi juga desain, asumsi, sumber data, keterbatasan, *fairness*, keamanan, dan kesiapan operasional. Model yang sangat akurat di laboratorium dapat gagal di lapangan apabila integrasi data terlambat, pengguna salah menafsirkan *output*, atau proses tindak lanjut tidak tersedia.

Pengujian performa harus memilih metrik yang sesuai. Untuk risiko yang jarang tetapi berat, akurasi keseluruhan dapat menipu. Model yang selalu memprediksi transaksi normal mungkin terlihat 99 persen akurat jika *fraud* hanya 1 persen, tetapi tidak berguna. *Precision*, *recall*, *F1-score*, *area under curve*, *false positive rate*, dan *false negative rate* perlu dibaca bersama. Untuk model regresi, organisasi dapat menggunakan MAE, RMSE, dan analisis kesalahan pada segmen penting.

Pengujian *fairness* membandingkan hasil antar kelompok yang relevan dan menilai apakah perbedaan memiliki dasar yang sah. Tidak ada satu metrik *fairness* yang cocok untuk semua kondisi. Kesetaraan peluang, paritas kesalahan, dan kesetaraan kalibrasi dapat menghasilkan *trade-off*. Karena itu, pilihan metrik harus didokumentasikan dan melibatkan fungsi hukum, risiko, serta pihak yang memahami dampak sosial. Fokusnya bukan sekadar memenuhi angka, tetapi mencegah kerugian yang tidak adil.

*Stress testing* menilai perilaku model pada kondisi ekstrem atau tidak biasa. Data dapat dimodifikasi untuk meniru lonjakan permintaan, perubahan *kurs*, gangguan pemasok, pola *fraud* baru, atau serangan terhadap input. Organisasi juga dapat melakukan *adversarial testing* dan *red teaming* untuk mencari cara sistem disalahgunakan. Temuan harus diterjemahkan menjadi batas penggunaan, *guardrail*, rencana *fallback*, dan keputusan apakah model layak dirilis.



**Gambar 5.4** Contoh panel indikator validasi model risiko.

Sumber: diolah untuk diktat ini.

**Tabel 5.6** Program validasi model risiko

| Aspek                       | Prosedur                                                             | Kriteria penerimaan                                     |
|-----------------------------|----------------------------------------------------------------------|---------------------------------------------------------|
| <b>Conceptual soundness</b> | Review teori, tujuan, fitur, dan asumsi                              | Logis, relevan, dan terdokumentasi                      |
| <b>Data</b>                 | Uji kualitas, leakage, dan representativitas                         | Memenuhi ambang dan keterbatasan dinyatakan             |
| <b>Kinerja</b>              | <i>Reperformance</i> metrik pada holdout dan periode berbeda         | Melebihi <i>baseline</i> dan stabil pada segmen penting |
| <b>Fairness</b>             | Bandingkan hasil dan kesalahan antar kelompok                        | Perbedaan dijelaskan dan risiko dikelola                |
| <b>Robustness</b>           | <i>Stress test</i> , <i>outlier</i> , dan perubahan distribusi       | Tidak gagal secara tidak terkendali                     |
| <b>Implementasi</b>         | Uji <i>pipeline</i> , akses, <i>monitoring</i> , dan <i>fallback</i> | Hasil produksi konsisten dengan validasi                |
| <b>Governance</b>           | Peran, <i>approval</i> , perubahan, dan dokumentasi                  | Pemilik jelas dan <i>residual risk</i> disetujui        |

## 5.5 EVALUASI RISIKO RESIDUAL DAN PORTOFOLIO RISIKO

Risiko *inheren* adalah tingkat risiko sebelum kontrol diperhitungkan, sedangkan risiko residual adalah tingkat risiko setelah kontrol yang ada dinilai. Perbedaan keduanya menunjukkan nilai kontrol. Penilaian residual harus didasarkan pada bukti efektivitas, bukan hanya keberadaan kebijakan. Kebijakan yang tidak dipahami, log yang tidak ditinjau, atau persetujuan yang selalu diberikan secara otomatis tidak boleh dianggap sebagai kontrol yang kuat.

Dalam sistem AI, kontrol dapat bersifat preventif, detektif, korektif, dan kompensatif. Kontrol preventif mencakup pembatasan data, validasi input, dan segregasi akses. Kontrol detektif mencakup monitoring drift, alarm anomali, dan review sampel. Kontrol korektif mencakup rollback, retraining, koreksi keputusan, dan pemulihan data. Kontrol kompensatif digunakan ketika kontrol ideal belum tersedia, misalnya review manual sementara pada transaksi tertentu.

Manajemen perlu melihat portofolio risiko, bukan hanya daftar individual. Beberapa risiko dapat berkorelasi dan terjadi bersamaan. Gangguan *vendor cloud* dapat memengaruhi rekomendasi, persediaan, pembayaran, dan layanan pelanggan sekaligus. Model yang menggunakan sumber data yang sama dapat gagal karena satu masalah kualitas data. Analisis konsentrasi membantu mengidentifikasi ketergantungan pada vendor, teknologi, dataset, atau personel kunci.

Agregasi risiko membutuhkan kehati-hatian. Menjumlahkan skor ordinal dari matriks dapat memberi kesan presisi yang tidak ada. Organisasi dapat menggunakan peta keterkaitan, skenario gabungan, atau simulasi untuk memahami efek domino. Dewan dan direksi membutuhkan ringkasan portofolio yang menunjukkan risiko utama, tren, konsentrasi, keterkaitan, tindakan, serta keputusan yang diminta. Informasi teknis yang terlalu rinci dapat disimpan sebagai lampiran, tetapi asumsi material tidak boleh disembunyikan.

**Tabel 5.7** Contoh penilaian risiko inheren dan residual

| Risiko                        | Inheren | Kontrol utama                                                          | Residual | Keputusan                                  |
|-------------------------------|---------|------------------------------------------------------------------------|----------|--------------------------------------------|
| <b>Salah harga otomatis</b>   | Ekstrem | Batas margin, <i>approval</i> , <i>anomaly alert</i> , <i>rollback</i> | Sedang   | Pilot terbatas dan <i>review</i> mingguan  |
| <b>Prediksi stok meleset</b>  | Tinggi  | <i>Fallback</i> , <i>override</i> , <i>freshness check</i>             | Sedang   | Diterima dengan KRI <i>stockout</i>        |
| <b>Kebocoran data chatbot</b> | Ekstrem | RAG berizin, <i>masking</i> , <i>least privilege</i> , <i>red team</i> | Tinggi   | Rilis ditunda sampai temuan kritis selesai |
| <b>Bias model kredit</b>      | Tinggi  | <i>Fairness test</i> , <i>banding</i> , <i>review</i> manusia          | Sedang   | Diterima dengan monitoring per segmen      |
| <b>Vendor tidak tersedia</b>  | Tinggi  | SLA, <i>cache</i> , model alternatif, prosedur manual                  | Rendah   | Diterima dan diuji semesteran              |

#### Studi Kasus Terpadu: Prediksi Permintaan pada CV Sumber Pangan

CV Sumber Pangan adalah distributor bahan makanan dengan enam gudang dan ratusan pelanggan ritel. Perusahaan sering mengalami dua masalah: produk tertentu habis

pada saat permintaan tinggi, sementara produk lain kedaluwarsa karena kelebihan stok. Manajemen mengembangkan model prediksi permintaan yang menggunakan data penjualan, promosi, kalender, cuaca, dan riwayat pengiriman. Tujuan model adalah memberi rekomendasi jumlah pemesanan mingguan untuk setiap gudang.

Tim memulai dengan mendefinisikan sasaran dan batas. Model hanya memberi rekomendasi; manajer persediaan tetap menyetujui pesanan. Produk dengan umur simpan pendek diperlakukan sebagai kategori risiko tinggi karena kesalahan prediksi cepat berubah menjadi limbah. Data diperiksa dan ditemukan bahwa beberapa cabang menggunakan kode produk yang berbeda, sedangkan data promosi tidak selalu dicatat. Sebelum model dibangun, perusahaan menyelaraskan master data dan membuat aturan wajib pencatatan promosi.

Model *time-series* meningkatkan ketepatan prediksi rata-rata, tetapi hasil validasi menunjukkan kesalahan besar pada produk musiman. Tim kemudian menambahkan skenario dan fitur kalender lokal. Metrik tidak hanya berupa akurasi, tetapi juga *stockout rate*, nilai kedaluwarsa, *service level*, dan jumlah *override* oleh manusia. Setiap *override* harus disertai alasan sehingga dapat digunakan sebagai umpan balik. Model tidak digunakan ketika data harian terlambat lebih dari batas tertentu; sistem otomatis beralih ke metode perencanaan konservatif.

Setelah tiga bulan, *stockout* menurun, tetapi satu gudang menunjukkan pola *override* yang sangat tinggi. Investigasi menemukan bahwa pemasok lokal sering mengubah jadwal tanpa pembaruan sistem. Masalah tersebut bukan kegagalan algoritma, melainkan masalah integrasi proses. Perusahaan memperbaiki kontrak dan pertukaran data dengan pemasok. Kasus ini menunjukkan bahwa penilaian risiko model harus mencakup lingkungan operasional, bukan hanya kode dan metrik teknis.

**Tabel 5.8** Ringkasan keputusan pada kasus CV Sumber Pangan

| Tahap             | Temuan                                              | Keputusan                                              |
|-------------------|-----------------------------------------------------|--------------------------------------------------------|
| <b>Konteks</b>    | Produk berumur simpan pendek memiliki dampak tinggi | Pisahkan kategori dan <i>target service level</i>      |
| <b>Data</b>       | Kode produk dan promosi tidak konsisten             | Perbaiki master data sebelum pemodelan                 |
| <b>Validasi</b>   | Error tinggi pada produk musiman                    | Tambah fitur kalender lokal dan skenario               |
| <b>Operasi</b>    | <i>Override</i> tinggi pada satu gudang             | Investigasi proses pemasok, bukan langsung retraining  |
| <b>Monitoring</b> | <i>Stockout</i> turun tetapi data pemasok terlambat | Tambahkan KRI <i>freshness</i> dan kewajiban integrasi |

### Praktikum Penyusunan Penilaian Risiko

Praktikum dilakukan dengan memilih satu proses perdagangan, misalnya pembelian, penerimaan barang, pengelolaan stok, penetapan harga, penjualan kredit, layanan pelanggan, atau distribusi. Peserta menyusun sasaran proses, pihak yang terdampak, batas waktu, data yang tersedia, dan daftar kejadian risiko. Setelah itu peserta menetapkan skala kemungkinan

dan dampak, lalu memilih minimal satu teknik analisis tradisional dan satu teknik berbasis data.

Peserta diminta menyusun dua penilaian: penilaian inheren dan residual. Setiap kontrol harus disertai bukti yang dapat diperiksa. Jika model AI digunakan, peserta menjelaskan variabel, sumber data, metrik, ambang, batas penggunaan, dan proses review manusia. Hasil akhir disajikan dalam risk register dan satu halaman executive summary. Penilaian tidak hanya dinilai dari kerapian skor, tetapi juga dari logika, transparansi asumsi, kualitas bukti, dan keterhubungan dengan keputusan.

**Tabel 5.9** Rubrik praktikum penilaian risiko

| Komponen                  | Bobot | Indikator kualitas                                       |
|---------------------------|-------|----------------------------------------------------------|
| Konteks dan sasaran       | 15%   | Batas proses, pihak terdampak, dan horizon waktu jelas   |
| Data dan asumsi           | 20%   | Sumber, kualitas, keterbatasan, dan legalitas dijelaskan |
| Metode analisis           | 20%   | Metode sesuai masalah dan dapat direplikasi              |
| Kontrol dan residual risk | 20%   | Kontrol terkait penyebab dan didukung bukti              |
| Keputusan dan komunikasi  | 15%   | Prioritas, pemilik, tenggat, dan eskalasi jelas          |
| Refleksi etis             | 10%   | Trade-off dan dampak pada pemangku kepentingan dibahas   |

## KESIMPULAN

Analisis dan penilaian risiko mengubah daftar ketidakpastian menjadi informasi yang dapat digunakan untuk menentukan prioritas. Proses dimulai dari konteks, kriteria, dan unit analisis; dilanjutkan dengan pemeriksaan data; pengukuran kemungkinan, dampak, kecepatan, dan ketidakpastian; pemilihan teknik; validasi model; serta evaluasi risiko residual dan portofolio. AI meningkatkan kapasitas analisis, tetapi tidak menghilangkan kebutuhan akan penilaian manusia, dokumentasi asumsi, dan pengujian independen.

Organisasi yang matang tidak menggunakan skor sebagai tujuan akhir. Skor menjadi awal percakapan mengenai siapa yang harus bertindak, kapan tindakan dilakukan, bukti apa yang dibutuhkan, dan bagaimana perubahan dipantau. Model yang baik adalah model yang sesuai dengan tujuan, adil, aman, stabil, dapat dijelaskan, dan terintegrasi dengan proses operasional. Ketika kondisi berubah, penilaian harus diperbarui.

## LATIHAN SOAL

1. Jelaskan perbedaan risiko inheren dan risiko residual serta berikan satu contoh pada sistem rekomendasi produk?
2. Mengapa akurasi tidak cukup untuk menilai model deteksi fraud? Sebutkan minimal tiga metrik tambahan?
3. Susun contoh risk appetite dan risk tolerance untuk penggunaan chatbot layanan pelanggan?

4. Jelaskan dua kondisi ketika analisis skenario lebih tepat daripada model prediktif berbasis data historis?
5. Bagaimana organisasi membuktikan bahwa kontrol manusia benar-benar efektif dan bukan sekadar formalitas?
6. Buat matriks 5 x 5 untuk risiko kehabisan stok, kebocoran data, dan salah harga. Jelaskan alasan penilaian?
7. Uraikan risiko penggunaan variabel proksi pada penilaian kredit pelanggan?
8. Rancang satu stress test untuk model prediksi permintaan pada masa gangguan rantai pasok?

#### **PILIHAN GANDA**

1. Tujuan utama analisis risiko adalah ...
  - A. menghilangkan seluruh risiko
  - B. menilai signifikansi dan mendukung keputusan
  - C. mengganti tanggung jawab manajemen
  - D. membuat skor setinggi mungkin
2. Metrik yang penting ketika kasus risiko jarang tetapi kritis adalah ...
  - A. ukuran file
  - B. recall
  - C. jumlah pengguna
  - D. warna dashboard
3. Risiko setelah kontrol disebut ...
  - A. inheren
  - B. residual
  - C. strategis
  - D. eksternal
4. Data drift berarti ...
  - A. perubahan distribusi input
  - B. perubahan struktur organisasi
  - C. hapus data
  - D. pelanggaran kontrak
5. Metode bow-tie menghubungkan ...
  - A. anggaran dan laba
  - B. penyebab, peristiwa, konsekuensi, dan kontrol
  - C. vendor dan pelanggan
  - D. kode dan lisensi
6. Model terkalibrasi berarti ...
  - A. selalu akurat 100%
  - B. probabilitas sesuai frekuensi outcome
  - C. tidak pernah berubah
  - D. tidak perlu monitoring

7. Risk velocity adalah ...
  - A. nilai aset
  - B. kecepatan dampak muncul
  - C. jumlah model
  - D. umur data
8. Penggunaan variabel proksi dapat memicu ...
  - A. bias tidak langsung
  - B. kompresi file
  - C. latensi jaringan
  - D. duplikasi kontrak
9. Stress test bertujuan ...
  - A. mempercantik laporan
  - B. menguji kondisi ekstrem
  - C. menghapus semua error
  - D. mengganti pengguna
10. Skor risiko seharusnya selalu disertai ...
  - A. pemilik, asumsi, dan tindakan
  - B. logo perusahaan
  - C. warna merah
  - D. nama vendor saja

# BAB 6

## ETIKA, PRIVASI, KEAMANAN, DAN KEPATUHAN AI

---

Bagaimana inovasi dijalankan tanpa mengorbankan hak, keamanan, dan kepercayaan?

### CAPAIAN PEMBELAJARAN

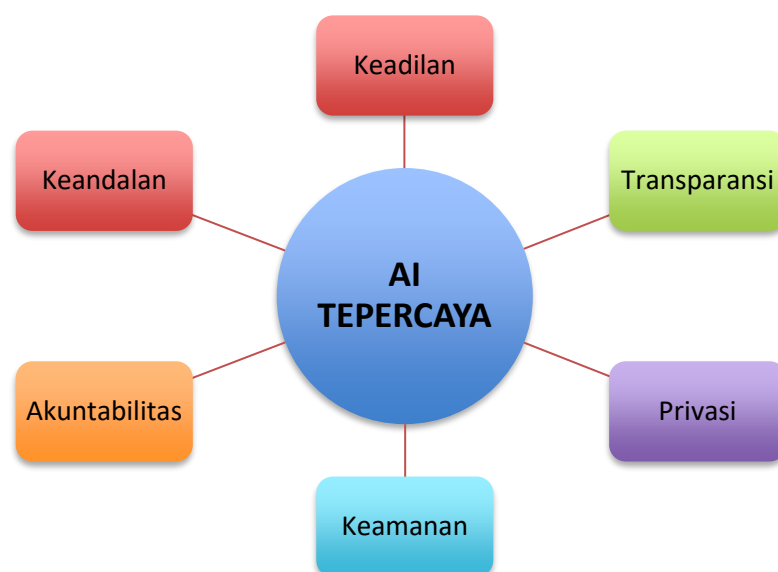
- Menganalisis bias, fairness, dan dampak.
- Merancang transparansi dan akuntabilitas.
- Menerapkan privacy by design.
- Memetakan ancaman keamanan AI.
- Menyusun AI Impact Assessment dan peta kepatuhan

### 6.1 MENGAPA ETIKA, PRIVASI, KEAMANAN, DAN KEPATUHAN HARUS TERINTEGRASI

Penggunaan AI pada perusahaan dagang tidak hanya menimbulkan pertanyaan teknis, tetapi juga pertanyaan tentang hak, kepentingan, dan tanggung jawab. Sistem rekomendasi dapat memengaruhi pilihan konsumen, model kredit dapat menentukan akses terhadap fasilitas pembayaran, sistem harga dapat menghasilkan perlakuan berbeda, dan chatbot dapat menyampaikan informasi yang dipercaya pelanggan. Ketika keputusan atau komunikasi tersebut keliru, dampaknya tidak selalu dapat dipulihkan hanya dengan memperbaiki kode. Kepercayaan, reputasi, dan rasa adil dapat rusak dalam waktu singkat.

Etika memberi arah tentang apa yang seharusnya dilakukan, privasi mengatur penghormatan terhadap data dan kendali individu, keamanan melindungi sistem dari gangguan dan penyalahgunaan, sedangkan kepatuhan memastikan praktik selaras dengan kewajiban hukum dan standar. Keempatnya saling bergantung. Sistem yang aman belum tentu adil; sistem yang transparan belum tentu melindungi data; sistem yang patuh secara formal belum tentu digunakan secara bertanggung jawab. Karena itu, perusahaan memerlukan pendekatan terintegrasi yang menghubungkan prinsip, kontrol, bukti, dan pengawasan.

NIST AI RMF menempatkan karakteristik seperti valid dan andal, aman, *secure* dan *resilient*, *accountable* dan *transparent*, *explainable* dan *interpretable*, *privacy-enhanced*, serta *fair* dengan bias berbahaya yang dikelola sebagai unsur AI tepercaya. ISO/IEC 42001 menyediakan kerangka sistem manajemen AI, sedangkan ISO/IEC 23894 memberi panduan pengelolaan risiko AI. Prinsip OECD dan rekomendasi UNESCO memperluas perhatian pada manusia, hak, nilai demokratis, keberlanjutan, dan akuntabilitas. Organisasi dapat menggunakan rujukan tersebut sebagai kompas, kemudian menyesuaikannya dengan konteks, ukuran, dan risiko usaha.



**Gambar 6.1** Pilar AI yang bertanggung jawab dan dapat dipercaya.

*Sumber: diolah untuk diktat ini.*

**PRINSIP KUNCI**

Etika bukan slogan, dan kepatuhan bukan sekadar dokumen. Keduanya harus terlihat pada desain data, pembatasan penggunaan, pengujian, keputusan manusia, penanganan keluhan, dan bukti audit.

**6.2 KEADILAN, BIAS, DAN DAMPAK TERHADAP PEMANGKU KEPENTINGAN**

Bias dapat muncul dari data, definisi target, pemilihan fitur, desain sampel, label manusia, algoritma, ambang keputusan, atau cara sistem digunakan. Data historis sering memuat pola ketidakadilan masa lalu. Jika model mempelajari pola tersebut tanpa koreksi, AI dapat mempertahankan atau memperbesar ketimpangan. Bias juga dapat muncul karena kelompok tertentu kurang terwakili, sehingga kinerja model untuk kelompok tersebut lebih buruk meskipun rata-rata terlihat baik.

Dalam perdagangan, risiko bias dapat terlihat pada promosi yang hanya ditampilkan kepada kelompok tertentu, sistem *fraud* yang terlalu sering menandai transaksi dari wilayah tertentu, model kredit yang menggunakan variabel proksi, atau chatbot yang memberi layanan berbeda berdasarkan bahasa. Evaluasi *fairness* harus dimulai dengan pemetaan pihak yang terdampak dan jenis kerugian yang mungkin terjadi. Tidak semua perbedaan adalah diskriminasi, tetapi setiap perbedaan material perlu memiliki alasan yang sah, proporsional, dan dapat dijelaskan.

*Fairness* tidak memiliki satu rumus tunggal. Organisasi dapat membandingkan tingkat penerimaan, peluang benar, tingkat kesalahan, atau kalibrasi antar kelompok. Metrik dapat saling bertentangan, sehingga pilihan harus didasarkan pada tujuan dan dampak. Untuk keputusan berisiko tinggi, evaluasi sebaiknya melibatkan tim lintas fungsi dan, bila relevan, perwakilan pengguna. Hasil pengujian perlu disertai keterbatasan, ukuran sampel, dan rencana pemantauan setelah penerapan.

Mekanisme banding dan koreksi merupakan kontrol penting. Pelanggan yang dirugikan oleh keputusan otomatis harus memiliki jalur untuk meminta penjelasan, memperbaiki data, dan memperoleh peninjauan manusia. Mekanisme tersebut tidak boleh dibuat terlalu rumit atau lambat. Data keluhan dan banding juga dapat menjadi indikator *fairness* yang bernilai, karena masalah yang tidak terlihat pada metrik laboratorium sering muncul dalam pengalaman pengguna.

**Tabel 6.1** Sumber bias dan kontrol *fairness*

| Sumber bias   | Contoh                                        | Kontrol                                                |
|---------------|-----------------------------------------------|--------------------------------------------------------|
| Data historis | Pola kredit lama merugikan kelompok tertentu  | Kajian sejarah, <i>reweighting</i> , dan data tambahan |
| Sampling      | Pelanggan daerah tertentu kurang terwakili    | <i>Stratified sampling</i> dan uji per segmen          |
| Label         | Penilai manusia memberi label tidak konsisten | Pedoman label, double review, dan audit agreement      |

|                     |                                                  |                                                        |
|---------------------|--------------------------------------------------|--------------------------------------------------------|
| <b>Fitur proksi</b> | Alamat menjadi proksi status sosial              | <i>Review</i> fitur, uji sensitivitas, dan pembatasan  |
| <b>Ambang</b>       | Satu <i>threshold</i> menghasilkan error berbeda | Analisis <i>trade-off</i> dan persetujuan kebijakan    |
| <b>Operasi</b>      | Petugas hanya mereview sebagian kelompok         | <i>Monitoring override</i> dan audit keputusan manusia |

### 6.3 TRANSPARANSI, EXPLAINABILITY, DAN AKUNTABILITAS

Transparansi berarti organisasi memberi informasi yang cukup mengenai penggunaan AI, tujuan, batasan, dan pihak yang bertanggung jawab. Transparansi tidak sama dengan membuka seluruh kode sumber. Tingkat informasi perlu disesuaikan dengan audiens dan risiko. Pelanggan perlu mengetahui ketika berinteraksi dengan chatbot; pengguna internal perlu memahami cara membaca *output*; manajemen memerlukan informasi tentang asumsi dan risiko; auditor memerlukan dokumentasi, log, dan bukti pengendalian.

*Explainability* membantu memahami mengapa model menghasilkan *output* tertentu. Model yang kompleks dapat dijelaskan melalui fitur penting, contoh pembandingan, aturan lokal, atau visualisasi. Namun, penjelasan harus jujur dan tidak dibuat sekadar untuk memberi kesan dapat dipahami. Penjelasan yang terlalu sederhana dapat menyesatkan, sedangkan penjelasan terlalu teknis tidak membantu pengguna. Organisasi perlu menetapkan standar minimum penjelasan untuk setiap use case berdasarkan dampaknya.

Akuntabilitas berarti ada orang atau unit yang dapat dimintai pertanggungjawaban. Menyatakan bahwa keputusan dibuat oleh algoritma tidak menghapus tanggung jawab organisasi. Pemilik bisnis bertanggung jawab atas tujuan dan penggunaan, pemilik data atas kualitas dan legalitas, tim teknis atas desain dan pengujian, fungsi risiko atas *challenge*, serta direksi atas pengawasan. Pembagian peran perlu dituangkan dalam RACI dan keputusan penting harus memiliki jejak persetujuan.

Dokumentasi menjadi jembatan antara transparansi dan akuntabilitas. Model card, dataset *sheet*, catatan perubahan, hasil validasi, *risk register*, dan log insiden membantu organisasi menjelaskan apa yang dilakukan. Dokumentasi harus diperbarui ketika model, data, atau konteks berubah. Dokumen yang dibuat hanya untuk audit dan tidak digunakan dalam operasi cenderung cepat usang.

**Tabel 6.2** Tingkat transparansi berdasarkan audiens

| <b>Audiens</b>           | <b>Informasi minimum</b>                              | <b>Media</b>                                             |
|--------------------------|-------------------------------------------------------|----------------------------------------------------------|
| <b>Pelanggan</b>         | Fakta penggunaan AI, tujuan, batas, dan jalur bantuan | Notifikasi, FAQ, dan mekanisme banding                   |
| <b>Pengguna internal</b> | Cara membaca <i>output</i> , larangan, dan eskalasi   | Panduan kerja dan pelatihan                              |
| <b>Manajemen</b>         | Manfaat, risiko, metrik, insiden, dan residual risk   | <i>Dashboard</i> dan laporan komite                      |
| <b>Validator/auditor</b> | Data, model, kode, log, hasil uji, dan keputusan      | <i>Model card</i> , <i>repository</i> , dan kertas kerja |

|                        |                                          |                                             |
|------------------------|------------------------------------------|---------------------------------------------|
| <b>Regulator/mitra</b> | Dokumentasi sesuai kewajiban dan kontrak | <i>Technical file</i> dan laporan kepatuhan |
|------------------------|------------------------------------------|---------------------------------------------|

#### 6.4 PERLINDUNGAN DATA PRIBADI DAN PRIVACY BY DESIGN

Perusahaan dagang mengelola data pelanggan, karyawan, pemasok, dan mitra. AI meningkatkan nilai data sekaligus memperbesar risiko karena data dapat digabungkan untuk menghasilkan inferensi baru. Informasi yang tampak tidak sensitif dapat menjadi sensitif ketika dikombinasikan. Pola belanja, lokasi, waktu transaksi, dan perangkat dapat digunakan untuk menebak kebiasaan, kondisi, atau preferensi. Karena itu, perlindungan data harus mencakup data mentah maupun inferensi yang dihasilkan model.

*Privacy by design* berarti perlindungan dirancang sejak awal. Tim harus menetapkan tujuan pemrosesan, dasar yang sah, jenis data minimum, periode retensi, pihak yang dapat mengakses, dan cara data dihapus. Data uji dan data produksi perlu dipisahkan. Pengembang tidak seharusnya menyalin data pelanggan ke lingkungan eksperimen tanpa kontrol. Teknik seperti pseudonimisasi, agregasi, *masking*, enkripsi, *differential privacy*, atau *synthetic data* dapat dipertimbangkan sesuai konteks.

Hak subjek data perlu diterjemahkan ke proses operasional. Organisasi harus mampu menemukan data yang terkait individu, mengoreksi kesalahan, menanggapi permintaan, dan menghentikan pemrosesan ketika diwajibkan. Pada sistem AI, penghapusan tidak selalu sederhana karena data mungkin telah digunakan untuk pelatihan. Oleh sebab itu, data *lineage* dan keputusan retensi harus dirancang sebelum model dibangun. Untuk penggunaan berisiko, organisasi dapat melakukan *data protection impact assessment* atau penilaian dampak yang setara.

UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi menjadi rujukan utama di Indonesia. Selain kewajiban hukum, praktik privasi yang baik merupakan bagian dari kepercayaan pelanggan. Organisasi sebaiknya tidak hanya bertanya apakah data boleh digunakan, tetapi juga apakah penggunaannya wajar, proporsional, dan sesuai harapan individu. Penggunaan yang sah secara formal dapat tetap menimbulkan risiko reputasi apabila mengejutkan atau merugikan pelanggan.



**Gambar 6.2** *Privacy by design* dalam siklus hidup sistem AI.

Sumber: diolah untuk diktat ini.

**Tabel 6.3** Checklist *privacy by design*

| Pertanyaan                            | Ya/Tidak | Bukti yang diharapkan                   |
|---------------------------------------|----------|-----------------------------------------|
| Tujuan pemrosesan dinyatakan dan sah? |          | <i>Use-case charter</i> dan legal basis |

|                                                    |  |                                              |
|----------------------------------------------------|--|----------------------------------------------|
| Data dibatasi pada kebutuhan minimum?              |  | Data map dan justifikasi fitur               |
| Data sensitif dipisah dan dilindungi?              |  | Kontrol akses, masking, dan enkripsi         |
| Retensi dan penghapusan dapat dijalankan?          |  | Jadwal retensi dan <i>log deletion</i>       |
| Hak subjek data didukung?                          |  | Prosedur akses, koreksi, dan keberatan       |
| Vendor dilarang menggunakan ulang data tanpa izin? |  | Klausul kontrak dan konfigurasi layanan      |
| Log tidak menyimpan informasi berlebihan?          |  | <i>Log schema</i> dan <i>review sampling</i> |

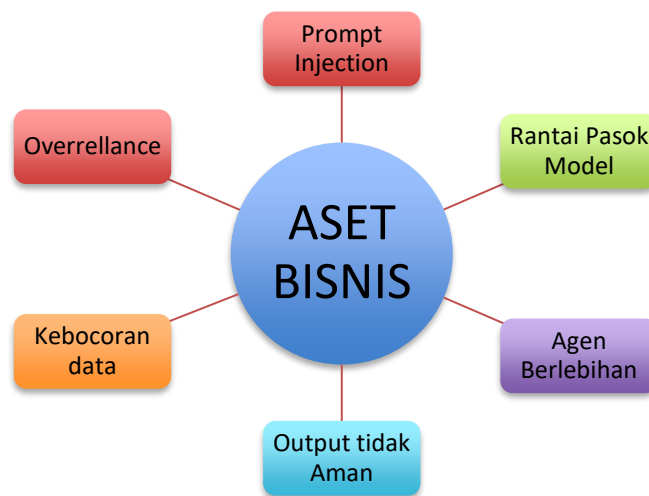
### 6.5 KEAMANAN SIBER DAN ANCAMAN KHUSUS AI

Sistem *AI* memperluas permukaan serangan. Selain *server*, aplikasi, jaringan, dan identitas, organisasi perlu melindungi data pelatihan, model, *prompt*, *knowledge base*, *plugin*, API, serta komponen pihak ketiga. Ancaman dapat terjadi pada seluruh rantai nilai. Penyerang dapat meracuni data, mencuri model, memanipulasi input, memaksa sistem mengungkapkan informasi, atau memanfaatkan output yang tidak divalidasi untuk menyerang sistem lain.

Pada aplikasi *generative AI*, *prompt injection* menjadi perhatian karena instruksi berbahaya dapat disisipkan melalui input pengguna atau dokumen yang dibaca model. Sistem dapat diarahkan mengabaikan aturan, membocorkan data, atau menjalankan tindakan yang tidak dimaksudkan. Kontrol tidak boleh hanya mengandalkan *prompt* sistem. Organisasi perlu membatasi akses alat, memvalidasi *input* dan *output*, menerapkan *least privilege*, memisahkan konteks sensitif, dan menggunakan persetujuan manusia untuk tindakan penting.

Ancaman lain adalah *excessive agency*, yaitu pemberian kewenangan terlalu luas kepada agen *AI*. Agen yang dapat mengirim email, mengubah harga, membuat pesanan, atau mengakses basis data tanpa batas dapat menimbulkan kerugian besar ketika salah atau dimanipulasi. Setiap alat harus memiliki daftar izin, batas jumlah dan nilai transaksi, segregasi tugas, log, dan kill switch. Kewenangan sebaiknya bertambah secara bertahap setelah bukti keandalan tersedia.

*Supply chain risk* muncul karena sistem *AI* bergantung pada model dasar, *library*, *dataset*, layanan *cloud*, dan *plugin*. Kerentanan atau perubahan pada satu komponen dapat memengaruhi seluruh sistem. Organisasi perlu melakukan inventarisasi komponen, menilai vendor, memantau pembaruan, memverifikasi sumber, dan memiliki rencana alternatif. Kontrak perlu mengatur notifikasi insiden, lokasi data, penggunaan data untuk pelatihan, hak audit, subprosesor, pemulihan, dan penghapusan data.



**Gambar 6.3** Peta ancaman utama pada aplikasi AI generatif.

*Sumber: diolah untuk diktat ini.*

**Tabel 6.4** Ancaman keamanan AI dan mitigasi

| Ancaman                            | Skenario                                                 | Mitigasi utama                                                                                 |
|------------------------------------|----------------------------------------------------------|------------------------------------------------------------------------------------------------|
| <b><i>Prompt injection</i></b>     | Instruksi berbahaya menubah perilaku model               | Isolasi konteks, <i>allowlist tools</i> , <i>output validation</i> , dan <i>human approval</i> |
| <b><i>Sensitive disclosure</i></b> | Model mengungkapkan data pelanggan atau rahasia          | <i>Least privilege</i> , <i>filtering</i> , <i>masking</i> , dan <i>testing</i>                |
| <b><i>Data poisoning</i></b>       | Data pelatihan dimanipulasi                              | <i>Provenance</i> , <i>integrity check</i> , <i>approval</i> , dan <i>anomaly detection</i>    |
| <b><i>Excessive agency</i></b>     | Agen melakukan transaksi tanpa kontrol                   | Batas kewenangan, <i>value limit</i> , <i>approval</i> , dan <i>kill switch</i>                |
| <b><i>Supply chain</i></b>         | <i>Library</i> , model, atau <i>plugin</i> dikompromikan | SBOM/AI-BOM, <i>vendor due diligence</i> , <i>pinning</i> , dan <i>patching</i>                |
| <b><i>Model theft</i></b>          | Model atau <i>prompt proprietary</i> dicuri              | <i>Access control</i> , <i>rate limit</i> , <i>monitoring</i> , dan <i>encryption</i>          |
| <b><i>Unsafe output</i></b>        | <i>Output</i> dieksekusi oleh sistem lain                | <i>Schema validation</i> , <i>sandbox</i> , <i>escaping</i> , dan <i>policy enforcement</i>    |

## 6.6 KEPATUHAN NASIONAL DAN KERANGKA INTERNASIONAL

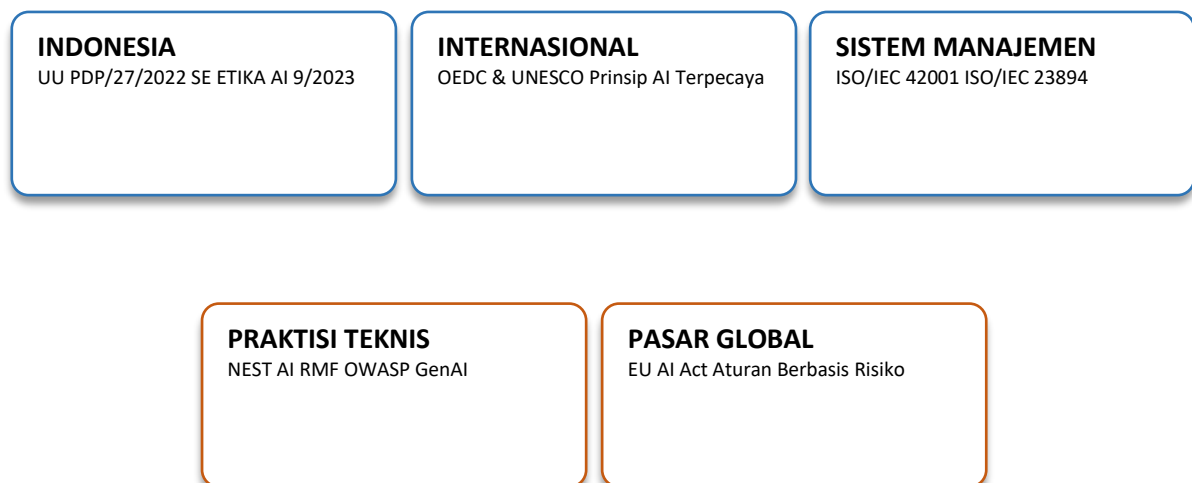
Kepatuhan AI berkembang cepat. Perusahaan Indonesia perlu memetakan kewajiban berdasarkan sektor, data, produk, konsumen, ketenagakerjaan, transaksi elektronik, dan keamanan. Surat Edaran Menteri Komunikasi dan Informatika Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial memberi rujukan etika bagi pelaku usaha dan penyelenggara konsultasi, pemrograman, serta aktivitas berbasis AI. Walaupun surat edaran bukan pengganti undang-undang sektoral, prinsipnya dapat digunakan untuk merancang kebijakan internal.

Perusahaan yang beroperasi atau melayani pasar global perlu memperhatikan aturan lintas yurisdiksi. *EU AI Act* menggunakan pendekatan berbasis risiko dan menetapkan

kewajiban yang berbeda untuk praktik terlarang, sistem berisiko tinggi, kewajiban transparansi, dan model tujuan umum. Relevansi bagi perusahaan dagang dapat muncul ketika sistem digunakan untuk perekrutan, akses layanan penting, biometrik, atau interaksi dengan konsumen di Uni Eropa. Pemetaan hukum perlu dilakukan berdasarkan peran organisasi sebagai penyedia, deployer, importir, atau distributor.

Standar bersifat sukarela tetapi dapat membantu membangun bukti kepatuhan. ISO/IEC 42001 menetapkan persyaratan sistem manajemen AI, sedangkan ISO/IEC 23894 memberi panduan manajemen risiko. NIST AI RMF menyediakan fungsi *Govern*, *Map*, *Measure*, dan *Manage*. Organisasi tidak harus menerapkan semua kerangka secara terpisah. *Crosswalk* dapat digunakan agar satu kontrol, seperti inventaris AI dan penilaian dampak, memenuhi beberapa kebutuhan sekaligus.

Kepatuhan harus diperlakukan sebagai proses dinamis. Daftar regulasi, pemilik kewajiban, bukti, dan status pemenuhan perlu diperbarui. Tim hukum tidak dapat bekerja sendirian karena kewajiban harus diterjemahkan ke desain teknis dan proses. Sebaliknya, tim teknis tidak boleh menafsirkan hukum tanpa bantuan yang tepat. Forum lintas fungsi membantu menyelesaikan perbedaan dan menetapkan tindakan yang proporsional.



**Gambar 6.4** Lanskap rujukan etika, risiko, keamanan, dan kepatuhan AI.

*Sumber: diolah untuk diktat ini.*

**Tabel 6.5** Peta awal kepatuhan AI

| Rujukan                     | Fokus                                                      | Implikasi perusahaan dagang                               |
|-----------------------------|------------------------------------------------------------|-----------------------------------------------------------|
| <b>UU 27/2022 PDP</b>       | Hak subjek, dasar pemrosesan, keamanan, dan tanggung jawab | Peta data, minimisasi, respons hak, dan insiden           |
| <b>SE Menkominfo 9/2023</b> | Nilai etika penggunaan kecerdasan artifisial               | Kebijakan internal dan prinsip responsible AI             |
| <b>ISO/IEC 42001:2023</b>   | Sistem manajemen AI                                        | Kebijakan, tujuan, operasi, audit, dan <i>improvement</i> |
| <b>ISO/IEC 23894:2023</b>   | Panduan risiko AI                                          | Integrasi risiko sepanjang siklus hidup                   |

|                        |                                       |                                                   |
|------------------------|---------------------------------------|---------------------------------------------------|
| <b>NIST AI RMF 1.0</b> | <i>Govern, Map, Measure, Manage</i>   | Profil, pengukuran, dan tindakan berbasis risiko  |
| <b>EU AI Act</b>       | Kewajiban berbasis kategori risiko    | Pemetaan peran dan pasar bila melayani wilayah EU |
| <b>OWASP GenAI</b>     | Ancaman aplikasi <i>generative AI</i> | <i>Threat model</i> dan pengujian keamanan        |

## 6.7 PENILAIAN DAMPAK AI

*AI impact assessment* adalah proses terstruktur untuk menilai tujuan, pihak terdampak, manfaat, risiko, data, model, keputusan, kontrol, dan rencana pemantauan sebelum sistem diterapkan. Penilaian ini membantu organisasi menemukan masalah ketika perubahan masih murah. Penilaian tidak hanya diperlukan untuk model yang dibangun sendiri; solusi vendor juga perlu dinilai karena organisasi tetap bertanggung jawab atas cara teknologi digunakan.

Penilaian dimulai dengan deskripsi *use case* dan keputusan yang dipengaruhi. Tim perlu menanyakan apakah AI benar-benar diperlukan, apakah metode yang lebih sederhana cukup, dan apakah manfaat sebanding dengan risiko. Selanjutnya dipetakan jenis data, kelompok terdampak, kemungkinan kesalahan, skala penggunaan, tingkat otonomi, serta reversibilitas keputusan. Sistem dengan dampak besar, skala luas, atau sulit dibalik memerlukan pemeriksaan lebih dalam.

Bagian penting penilaian adalah alternatif dan *residual risk*. Tim harus membandingkan desain, misalnya model otomatis penuh, rekomendasi dengan persetujuan manusia, atau aturan sederhana. Setelah kontrol dirancang, risiko residual dinilai dan pemilik bisnis memutuskan apakah penggunaan diterima, dibatasi, diuji ulang, atau dihentikan. Keputusan dan alasan harus terdokumentasi.

Penilaian dampak bukan dokumen sekali jadi. Perubahan tujuan, data, model dasar, vendor, kelompok pengguna, atau regulasi dapat memicu penilaian ulang. Organisasi perlu menetapkan material change criteria. Misalnya, pergantian model generatif, penambahan akses ke data sensitif, peningkatan otonomi, atau ekspansi ke negara baru wajib melalui review.

**Tabel 6.6 Struktur AI Impact Assessment**

| Bagian                | Pertanyaan inti                                       | Output                                        |
|-----------------------|-------------------------------------------------------|-----------------------------------------------|
| Tujuan dan kebutuhan  | Masalah apa diselesaikan dan apakah AI diperlukan?    | Justifikasi dan alternatif                    |
| Pihak terdampak       | Siapa memperoleh manfaat atau menanggung kerugian?    | <i>Stakeholder map</i>                        |
| Data                  | Apa sumber, legalitas, kualitas, dan sensitivitasnya? | Data map dan kontrol privasi                  |
| Keputusan dan otonomi | Apa yang dipengaruhi dan dapatkah dibalik?            | Klasifikasi dampak dan <i>oversight</i>       |
| Risiko dan kontrol    | Apa skenario risiko dan bagaimana ditangani?          | <i>Risk register</i> dan <i>residual risk</i> |

|             |                                                                         |                         |
|-------------|-------------------------------------------------------------------------|-------------------------|
| Pengujian   | Apa metrik kinerja, <i>fairness</i> , keamanan, dan <i>robustness</i> ? | Test plan dan hasil     |
| Operasi     | Bagaimana monitoring, banding, insiden, dan perubahan?                  | <i>Operational plan</i> |
| Persetujuan | Siapa menerima <i>residual risk</i> ?                                   | <i>Decision record</i>  |

## 6.8 PENGELOLAAN HAK KEKAYAAN INTELEKTUAL DAN KONTEN

AI generatif dapat menghasilkan teks, gambar, kode, dan desain yang menyerupai materi yang telah ada. Perusahaan perlu mengatur penggunaan *input* dan *output* agar tidak melanggar hak cipta, merek, rahasia dagang, atau lisensi. Karyawan tidak boleh memasukkan materi rahasia atau berlisensi ke layanan publik tanpa persetujuan. *Output* yang digunakan untuk publikasi atau komersial perlu diperiksa sumber, kemiripan, dan hak penggunaannya. Kepemilikan *output* bergantung pada kontrak layanan dan hukum yang berlaku. *Vendor* dapat memiliki ketentuan berbeda mengenai penggunaan data, pelatihan model, dan *indemnity*. Bagian hukum dan pengadaan perlu menilai ketentuan sebelum layanan digunakan. Untuk materi penting, organisasi sebaiknya menyimpan *prompt*, versi model, tanggal, hasil *review*, dan kontribusi manusia sebagai bukti proses penciptaan.

Risiko informasi palsu juga harus dikelola. AI dapat menghasilkan kutipan, angka, atau sumber yang tidak ada. Setiap *output* faktual perlu diverifikasi terhadap sumber otoritatif. Untuk konten pelanggan, perusahaan dapat menetapkan daftar topik yang tidak boleh dijawab otomatis, seperti nasihat hukum, kesehatan, atau komitmen kontraktual, kecuali sistem dirancang dan diawasi secara khusus.

**Tabel 6.7** Pengendalian kekayaan intelektual dan konten AI

| Risiko                             | Kontrol preventif                                   | Kontrol detektif/korektif                        |
|------------------------------------|-----------------------------------------------------|--------------------------------------------------|
| Input rahasia ke layanan publik    | Daftar data terlarang dan layanan <i>enterprise</i> | DLP, log, investigasi, dan edukasi               |
| Output mirip karya pihak lain      | Panduan penggunaan dan batas materi                 | <i>Similarity check</i> dan <i>legal review</i>  |
| Sumber palsu atau halusinasi       | <i>Grounding</i> dan daftar sumber otoritatif       | <i>Fact-check</i> dan kewajiban sitasi           |
| Lisensi model/library tidak sesuai | <i>Review</i> lisensi dan <i>procurement gate</i>   | Inventory komponen dan <i>audit license</i>      |
| Kepemilikan output tidak jelas     | Klausul kontrak dan pencatatan kontribusi manusia   | Arsip <i>prompt</i> , versi, dan <i>approval</i> |

### Studi Kasus: Chatbot PT Elektronika Sentosa

PT Elektronika Sentosa ingin menggunakan chatbot generatif untuk menjawab pertanyaan produk, status pesanan, dan kebijakan retur. Pada uji coba, chatbot mampu menjawab cepat, tetapi beberapa kali memberikan informasi garansi yang tidak sesuai. Tim juga menemukan bahwa knowledge base memuat nomor telepon pelanggan dari tiket lama.

Risiko mencakup misinformasi, kebocoran data, *prompt injection*, dan ekspektasi pelanggan bahwa chatbot memiliki kewenangan membuat keputusan.

Perusahaan membatasi ruang lingkup. Chatbot hanya boleh menjawab berdasarkan sumber yang disetujui, tidak boleh membuat kebijakan baru, dan harus mengalihkan kasus sengketa kepada petugas manusia. Data tiket dibersihkan dan informasi pribadi dipisahkan. *Output* divalidasi dengan *retrieval* dan aturan, sementara topik berisiko memiliki jawaban baku. Pelanggan diberi tahu bahwa mereka berinteraksi dengan AI dan dapat meminta petugas manusia.

Tim keamanan melakukan pengujian *prompt injection* dan menemukan cara memaksa chatbot menampilkan potongan dokumen internal. Akses *knowledge base* kemudian dipisahkan berdasarkan peran, dan hasil pencarian disaring sebelum diberikan ke model. Log dipantau untuk pola serangan, tetapi log tidak menyimpan data lebih lama dari kebutuhan. Komite AI menyetujui pilot terbatas dengan indikator: akurasi jawaban, tingkat eskalasi, keluhan, insiden privasi, dan waktu penyelesaian.

Setelah dua bulan, kepuasan meningkat, tetapi pertanyaan produk baru masih sering salah. Analisis menunjukkan proses pembaruan *knowledge base* terlambat. Perusahaan memperbaiki tata kelola konten dan menetapkan pemilik setiap kategori informasi. Kasus ini menunjukkan bahwa AI yang bertanggung jawab memerlukan kombinasi desain, data, keamanan, proses, komunikasi, dan pemantauan.

**Tabel 6.8** Kontrol chatbot PT Elektronika Sentosa

| Risiko                         | Kontrol                                                    | Indikator                          |
|--------------------------------|------------------------------------------------------------|------------------------------------|
| <b>Misinformasi garansi</b>    | RAG dari sumber resmi dan topik terlarang                  | Akurasi jawaban dan jumlah koreksi |
| <b>Kebocoran data</b>          | Pembersihan <i>knowledge base</i> dan akses berbasis peran | Insiden dan hasil <i>red test</i>  |
| <b><i>Prompt injection</i></b> | Filter, isolasi instruksi, dan tool restriction            | Percobaan serangan yang diblokir   |
| <b><i>Overreliance</i></b>     | Notifikasi AI dan eskalasi ke petugas                      | Rasio eskalasi dan keluhan         |
| <b>Konten usang</b>            | Pemilik konten dan SLA pembaruan                           | Usia dokumen dan error produk baru |

## KESIMPULAN

Etika, privasi, keamanan, dan kepatuhan harus dirancang sebagai satu sistem. Keadilan membutuhkan pemetaan dampak dan pengujian bias; transparansi membutuhkan informasi yang sesuai audiens; akuntabilitas membutuhkan pemilik dan bukti; privasi membutuhkan minimisasi, *lineage*, dan pemenuhan hak; keamanan membutuhkan pertahanan berlapis; serta kepatuhan membutuhkan pemetaan kewajiban yang dinamis. Penilaian dampak membantu menyatukan seluruh aspek sebelum sistem diterapkan.

Kepercayaan tidak dibangun oleh klaim bahwa AI canggih, tetapi oleh kemampuan organisasi menjelaskan tujuan, mencegah kerugian, menerima keluhan, memperbaiki

kesalahan, dan menunjukkan bukti pengawasan. Semakin besar otonomi dan dampak sistem, semakin kuat kontrol yang diperlukan.

### LATIHAN SOAL

1. Jelaskan lima sumber bias yang dapat muncul pada sistem AI perusahaan dagang.
2. Mengapa transparansi tidak selalu berarti membuka seluruh kode sumber?
3. Susun tiga kontrol *privacy by design* untuk model rekomendasi produk. Berikan contoh prompt injection tidak langsung dan cara mengendalikannya. Jelaskan perbedaan tanggung jawab pemilik bisnis, pemilik data, tim model, fungsi risiko, dan audit internal. Rancang mekanisme banding bagi pelanggan yang ditolak oleh model kredit. Buat daftar material change yang memicu penilaian dampak ulang. Analisis risiko hak kekayaan intelektual saat tim pemasaran menggunakan AI generatif.

### PILIHAN GANDA

1. Privacy by design dilakukan ...
  - A. setelah insiden
  - B. sejak tahap awal desain
  - C. hanya oleh auditor
  - D. hanya pada data publik
2. Prompt injection adalah ...
  - A. pembaruan perangkat
  - B. manipulasi instruksi model
  - C. metode enkripsi
  - D. jenis audit
3. Keadilan model sebaiknya dinilai ...
  - A. hanya dari rata-rata
  - B. per kelompok relevan dan dampak
  - C. dari ukuran model
  - D. dari biaya lisensi
4. Explainability lokal menjelaskan ...
  - A. satu keputusan tertentu
  - B. seluruh regulasi
  - C. semua data mentah
  - D. struktur organisasi
5. Excessive agency terjadi ketika ...
  - A. AI tidak punya akses
  - B. AI diberi kewenangan terlalu luas
  - C. model terlalu kecil
  - D. data sudah anonim
6. Data minimization berarti ...
  - A. menghapus semua data

- B. menggunakan data minimum yang relevan
  - C. menyimpan tanpa batas
  - D. membagikan ke vendor
7. AIIA digunakan untuk ...
- A. menilai dampak use case AI
  - B. menghitung pajak
  - C. mengganti audit keuangan
  - D. membuat iklan
8. Kontrol supply chain AI mencakup ...
- A. inventaris komponen dan due diligence
  - B. mengabaikan vendor
  - C. menghapus kontrak
  - D. mematikan log
9. Mekanisme banding mendukung ...
- A. fairness dan akuntabilitas
  - B. latensi
  - C. kompresi
  - D. routing
10. Transparansi kepada pelanggan dapat berupa ...
- A. notifikasi interaksi AI dan jalur bantuan
  - B. kode sumber penuh selalu
  - C. data pelanggan lain
  - D. password admin

# BAB 7

## STRATEGI MITIGASI RISIKO DALAM PENGGUNAAN AI

---

Bagaimana kontrol teknis, proses, manusia, dan kontrak bekerja sebagai satu sistem?

### CAPAIAN PEMBELAJARAN

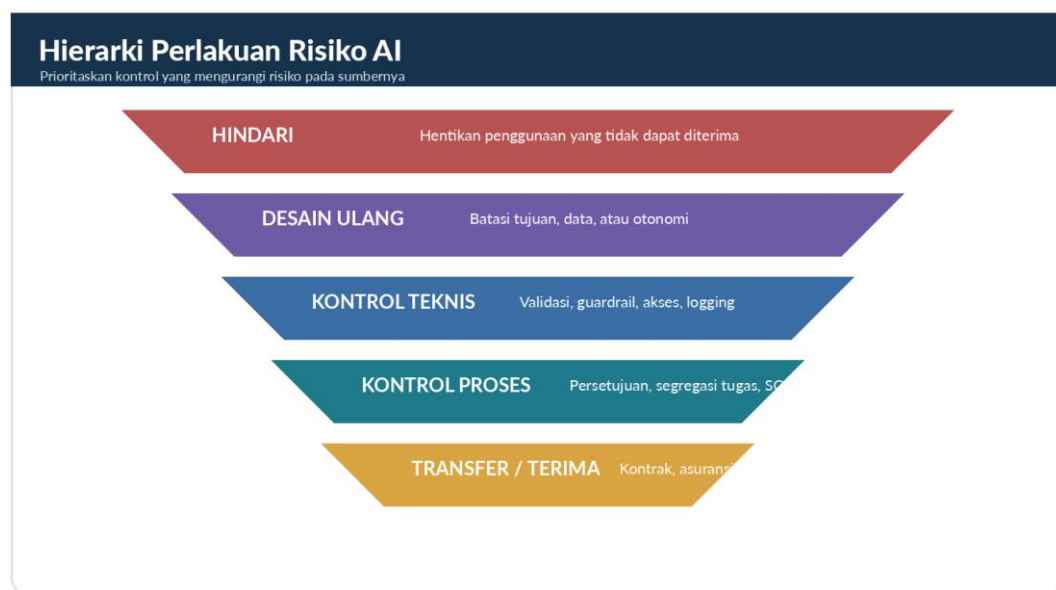
- Memilih strategi perlakuan risiko.
- Menyusun tata kelola dan RACI.
- Merancang human oversight.
- Menetapkan kontrol teknis, budaya, dan vendor.
- Membangun respons insiden dan fallback.

## 7.1 STRATEGI MITIGASI SEBAGAI SISTEM PENGENDALIAN

Mitigasi risiko AI bukan satu alat atau satu kebijakan. Ia merupakan kombinasi keputusan desain, kontrol teknis, proses kerja, kompetensi manusia, pengawasan, kontrak, dan rencana pemulihan. Organisasi sering gagal karena hanya menambahkan disclaimer atau meminta pengguna berhati-hati, sementara sumber risiko dibiarkan. Strategi yang kuat dimulai dengan menghilangkan atau mengurangi risiko pada desain, kemudian menambahkan lapisan deteksi dan respons.

Pilihan perlakuan risiko meliputi menghindari, mengurangi, memindahkan, atau menerima. Menghindari berarti tidak menggunakan AI untuk tujuan yang tidak sebanding dengan manfaat atau tidak dapat dikendalikan. Mengurangi berarti mengubah data, model, otonomi, atau proses. Memindahkan dapat dilakukan melalui kontrak dan asuransi, tetapi tanggung jawab reputasi dan hukum tidak selalu dapat dialihkan. Menerima risiko harus menjadi keputusan sadar dengan alasan, batas, pemilik, dan rencana pemantauan.

Kontrol perlu dirancang berdasarkan penyebab dan skenario, bukan daftar generik. Risiko halusinasi pada chatbot dapat dikurangi dengan retrieval dari sumber terverifikasi, pembatasan topik, validasi output, dan eskalasi manusia. Risiko salah harga memerlukan batas perubahan, aturan minimum-maksimum, simulasi, approval, dan rollback. Risiko fraud model membutuhkan monitoring pola baru, retraining, challenge oleh analis, dan investigasi.



**Gambar 7.1** Hierarki perlakuan risiko AI dari penghindaran hingga penerimaan residual.

Sumber: diolah untuk diktat ini.

**Tabel 7.1** Contoh hierarki kontrol per risiko

| Risiko                      | Hindari/desain ulang | Kontrol teknis                   | Kontrol proses             | Residual            |
|-----------------------------|----------------------|----------------------------------|----------------------------|---------------------|
| Keputusan kredit tidak adil | Batasi otomasi penuh | Fairness test dan explainability | Banding dan review manusia | Dipantau per segmen |

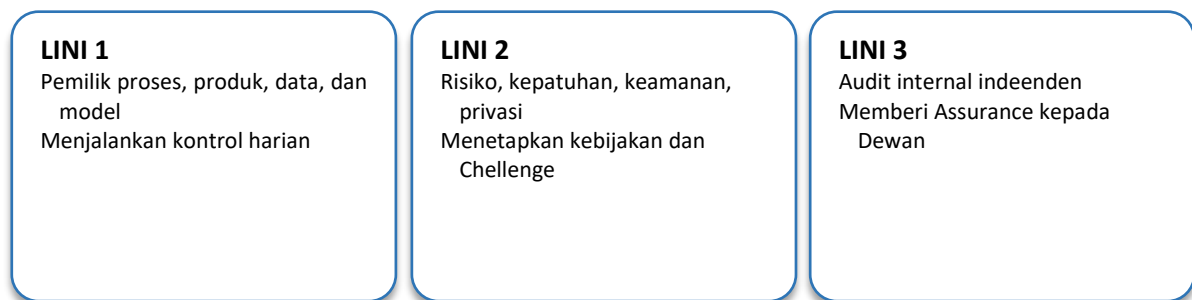
|                                   |                                    |                                 |                                  |                         |
|-----------------------------------|------------------------------------|---------------------------------|----------------------------------|-------------------------|
| <b>Chatbot membocorkan data</b>   | Jangan beri akses data tidak perlu | RAG berizin dan masking         | Escalation dan incident response | Diterima jika uji lulus |
| <b>Harga tidak wajar</b>          | Batasi produk dan otonomi          | Floor/ceiling dan anomaly alert | Approval dan rollback            | Pilot terbatas          |
| <b>Agen membuat pesanan salah</b> | Batasi alat dan nilai transaksi    | Allowlist dan rate limit        | Dual approval                    | Tidak boleh ekstrem     |

## 7.2 TATA KELOLA DAN PEMBAGIAN TANGGUNG JAWAB

Tata kelola memastikan bahwa keputusan mengenai AI tidak tercecer di antara bisnis, teknologi, risiko, dan hukum. Dewan atau pemilik menetapkan arah dan selera risiko; direksi memastikan sumber daya; komite AI menilai use case material; pemilik bisnis bertanggung jawab atas nilai dan dampak; pemilik data menjaga kualitas dan legalitas; tim teknis membangun kontrol; fungsi risiko dan kepatuhan memberikan challenge; audit internal memberikan assurance independen.

Model tiga lini membantu membedakan tanggung jawab. Lini pertama menjalankan dan memiliki risiko. Lini kedua menetapkan kerangka, memantau, dan menantang. Lini ketiga menilai secara independen apakah tata kelola dan kontrol efektif. Pemisahan ini tidak berarti silo. Informasi harus mengalir, tetapi fungsi assurance tidak boleh merancang kontrol yang kemudian diauditnya sendiri tanpa mitigasi independensi.

Komite etika dan tata kelola AI perlu memiliki mandat, kriteria eskalasi, jadwal, dan kewenangan. Komite tidak harus menilai semua eksperimen kecil, tetapi harus fokus pada use case berdampak tinggi, data sensitif, keputusan otomatis, penggunaan eksternal, dan perubahan material. Keputusan komite harus direkam: disetujui, disetujui dengan syarat, ditunda, atau ditolak.



*DEWAN / DIREKSI: menetapkan arah, selera Risiko dan pengawasan*

**Gambar 7.2** Model tiga lini dalam tata kelola AI.

Sumber: diolah untuk diktat ini.

**Tabel 7.2** RACI tata kelola AI

| Aktivitas                | Bisnis | Data/Model | Risiko/Kepatuhan | Keamanan | Audit |
|--------------------------|--------|------------|------------------|----------|-------|
| <b>Menetapkan tujuan</b> | A      | C          | C                | I        | I     |
| <b>Menilai data</b>      | C      | R/A        | C                | C        | I     |

|                        |     |   |     |   |     |
|------------------------|-----|---|-----|---|-----|
| Validasi model         | C   | R | A/C | C | I   |
| Menerima residual risk | A   | C | R/C | C | I   |
| Monitoring operasi     | A/R | R | C   | C | I   |
| Audit independen       | I   | C | C   | C | R/A |

### 7.3 KEBIJAKAN PENGGUNAAN DAN PENGENDALIAN SHADOW AI

*Acceptable Use Policy* menjelaskan penggunaan AI yang diperbolehkan, dibatasi, dan dilarang. Kebijakan harus menggunakan bahasa yang dipahami karyawan dan disertai contoh. Penggunaan untuk brainstorming data non-rahasia dapat diizinkan, sedangkan memasukkan data pelanggan, rahasia dagang, kredensial, atau dokumen kontrak ke layanan publik tanpa persetujuan harus dilarang. Output AI tidak boleh dianggap final tanpa review sesuai tingkat risiko.

Shadow AI muncul ketika karyawan menggunakan alat yang tidak disetujui karena alat resmi dianggap lambat atau tidak memadai. Larangan total tanpa alternatif sering mendorong perilaku tersembunyi. Organisasi perlu menyediakan kanal permintaan alat, sandbox aman, daftar layanan disetujui, dan proses evaluasi yang cepat. Monitoring teknis dapat membantu, tetapi pendekatan harus proporsional dan menghormati privasi karyawan. Kebijakan perlu mengatur identitas, akses, retensi, kepemilikan output, hak cipta, verifikasi fakta, pengungkapan penggunaan AI, dan pelaporan insiden. Untuk peran tertentu, aturan dapat lebih ketat. Staf hukum, keuangan, pengadaan, dan SDM menangani data serta keputusan sensitif. Pelatihan harus berbasis skenario pekerjaan, bukan hanya definisi umum.

**Tabel 7.3** Contoh klasifikasi penggunaan AI di tempat kerja

| Kategori                     | Contoh                                                                            | Syarat                                        |
|------------------------------|-----------------------------------------------------------------------------------|-----------------------------------------------|
| Diperbolehkan                | Brainstorming dan ringkasan materi publik                                         | Verifikasi dan tidak memasukkan data rahasia  |
| Diperbolehkan dengan kontrol | Draf laporan internal dan analisis data terbatas                                  | Layanan disetujui, masking, dan review        |
| Memerlukan persetujuan       | Konten pelanggan, kode produksi, dan keputusan bisnis                             | Risk assessment dan owner                     |
| Dilarang                     | Data pribadi sensitif ke chatbot publik, kredensial, atau keputusan diskriminatif | Tidak ada pengecualian tanpa otorisasi formal |

### 7.4 PENGAWASAN MANUSIA YANG BERMAKNA

Human oversight bermakna bukan sekadar menyediakan tombol persetujuan. Pengawas harus memiliki informasi, waktu, kompetensi, kewenangan, dan insentif untuk menolak. Jika ribuan alert muncul tanpa prioritas, manusia akan mengalami alert fatigue. Jika target kinerja mendorong persetujuan cepat, review berubah menjadi formalitas. Desain kontrol harus memperhitungkan beban kerja dan ergonomi keputusan.

Tingkat pengawasan disesuaikan dengan dampak. Human-in-the-loop cocok untuk keputusan kritis yang memerlukan persetujuan sebelum dijalankan. Human-on-the-loop cocok ketika sistem dapat bertindak tetapi dipantau dan dapat dihentikan. Human-over-the-loop mengatur batas, audit, dan eskalasi pada otomasi berisiko lebih rendah. Tidak ada satu tingkat yang selalu terbaik; pilihan harus didokumentasikan.

Mekanisme override harus dicatat. Override yang terlalu sedikit dapat menunjukkan overreliance, sedangkan terlalu banyak dapat menunjukkan model tidak berguna atau proses tidak cocok. Alasan override menjadi data pembelajaran. Organisasi juga perlu melindungi karyawan yang mengangkat masalah dan menyediakan jalur whistleblowing untuk perilaku sistem yang berbahaya atau tidak etis.

|   |                                                                                       |
|---|---------------------------------------------------------------------------------------|
| 1 | <b>Human-in-the-loop</b><br>Manusia Menyetujui setiap keputusan bisnis                |
| 2 | <b>Human-on-the-loop</b><br>Sistem bertindak, manusia memantau dan dapat menghentikan |
| 3 | <b>Human-over-the-loop</b><br>Manusia mengatur batas, audit, dan eskalasi             |
| 4 | <b>Otomasi terkendali</b><br>Keputusan rutin berisiko rendah dengan guardrail         |

**Gambar 7.3** Tingkat pengawasan manusia berdasarkan dampak dan otonomi.

Sumber: diolah untuk diktat ini.

**Tabel 7.4** Matriks pengawasan manusia

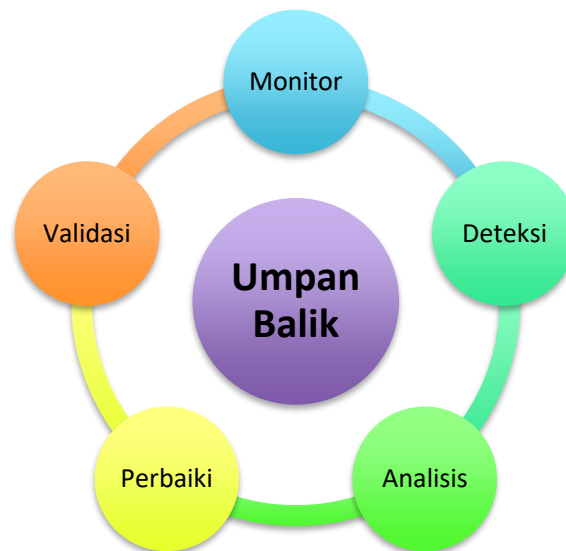
| Dampak/otonomi                     | Rendah                    | Sedang                       | Tinggi                              |
|------------------------------------|---------------------------|------------------------------|-------------------------------------|
| <b>Rekomendasi tanpa tindakan</b>  | Sampling berkala          | Review alert dan tren        | Review setiap kasus material        |
| <b>Tindakan dapat dibalik</b>      | Monitoring dan batas      | Human-on-the-loop            | Human-in-the-loop                   |
| <b>Tindakan sulit dibalik</b>      | Tidak dianjurkan otomatis | Persetujuan sebelum tindakan | Keputusan manusia dan second review |
| <b>Keselamatan/hak fundamental</b> | Pembatasan kuat           | Pilot terbatas               | Pertimbangkan tidak menggunakan AI  |

## 7.5 KONTROL TEKNIS, MLOPS, DAN LLMOPS

Kontrol teknis dimulai dari lingkungan pengembangan yang aman, version control, segregasi akses, dan pengelolaan rahasia. Setiap dataset, kode, model, prompt, knowledge base, serta konfigurasi harus memiliki versi dan pemilik. Perubahan produksi sebaiknya melalui pipeline dengan pengujian otomatis, approval, dan kemampuan rollback. Log harus cukup untuk investigasi tetapi tidak menyimpan data sensitif secara berlebihan.

Guardrail mencakup validasi input, pembatasan output, filter konten, aturan bisnis, dan pembatasan alat. Guardrail tidak sempurna dan harus diuji terhadap bypass. Pada AI generatif, retrieval-augmented generation dapat memperkuat grounding, tetapi kualitas

sumber dan izin akses tetap harus dikendalikan. Output yang menjalankan tindakan perlu divalidasi dengan skema dan aturan deterministik. Monitoring harus mencakup kinerja, drift, fairness, keamanan, biaya, latensi, dan perilaku pengguna. Ambang memicu tindakan yang jelas: investigasi, pembatasan, rollback, retraining, atau penghentian. Dashboard tanpa respons hanya menghasilkan rasa aman palsu. Pemilik indikator dan SLA tindak lanjut harus ditetapkan.



**Gambar 7.4** Siklus pemantauan, deteksi, analisis, perbaikan, dan validasi ulang.

*Sumber: diolah untuk diktat ini.*

**Tabel 7.5** Kontrol teknis sepanjang pipeline

| Tahap               | Kontrol                                         | Bukti                         |
|---------------------|-------------------------------------------------|-------------------------------|
| <b>Pengembangan</b> | Version control, peer review, secret management | Repository dan review log     |
| <b>Data</b>         | Validation, lineage, access, dan freshness      | Quality report dan access log |
| <b>Model</b>        | Baseline, test, robustness, dan fairness        | Test report dan model card    |
| <b>Rilis</b>        | Approval, feature flag, canary, rollback        | Release record                |
| <b>Operasi</b>      | Monitoring, alert, rate limit, dan kill switch  | Dashboard dan incident log    |
| <b>Perubahan</b>    | Regression test dan material change review      | Change log dan approval       |

## 7.6 LITERASI, BUDAYA, DAN MANAJEMEN PERUBAHAN

Literasi AI mencakup kemampuan memahami manfaat, keterbatasan, risiko, dan tanggung jawab. Karyawan tidak harus menjadi data scientist, tetapi perlu mengetahui kapan output harus diragukan, data apa yang tidak boleh dimasukkan, bagaimana memverifikasi fakta, dan ke mana melaporkan masalah. Pelatihan sebaiknya dibedakan untuk pengguna umum, manajer, pengembang, pemilik data, serta fungsi assurance.

Budaya yang sehat mendorong pertanyaan dan pelaporan. Jika kesalahan AI disembunyikan karena takut disalahkan, organisasi kehilangan kesempatan belajar. Near miss perlu dicatat seperti insiden. Pimpinan memberi contoh dengan tidak memaksakan

penggunaan AI hanya untuk mengejar tren dan dengan menerima keputusan menghentikan sistem ketika risiko tidak terkendali.

Manajemen perubahan perlu menjelaskan dampak terhadap peran. AI sering mengubah pekerjaan dari pelaksana menjadi reviewer atau kurator. Perubahan ini memerlukan keterampilan baru dan desain target yang realistis. Efisiensi tidak boleh dihitung hanya dari pengurangan waktu; biaya review, insiden, koreksi, dan penurunan kualitas harus dimasukkan.

**Tabel 7.6** Program literasi AI berbasis peran

| Audiens                 | Kompetensi                                      | Metode                                       | Frekuensi                    |
|-------------------------|-------------------------------------------------|----------------------------------------------|------------------------------|
| <b>Seluruh karyawan</b> | Penggunaan aman, verifikasi, dan pelaporan      | Microlearning dan simulasi phishing/deepfake | Saat onboarding dan tahunan  |
| <b>Manajer</b>          | Trade-off, oversight, dan residual risk         | Workshop kasus                               | Semesteran                   |
| <b>Pengembang</b>       | Secure AI, fairness, privacy, dan documentation | Lab dan code review                          | Triwulanan                   |
| <b>Pemilik data</b>     | Kualitas, lineage, dan hak data                 | Clinic data                                  | Triwulanan                   |
| <b>Risiko/audit</b>     | Framework, pengujian, dan bukti                 | Sertifikasi dan praktik                      | Tahunan plus update regulasi |

## 7.7 MANAJEMEN VENDOR DAN PIHAK KETIGA

Due diligence vendor mencakup stabilitas, keamanan, privasi, kinerja, dokumentasi, penggunaan data, subprosesor, lokasi pemrosesan, dan kemampuan pemulihan. Klaim pemasaran tidak cukup. Perusahaan perlu meminta bukti, laporan pengujian, sertifikasi yang relevan, serta penjelasan keterbatasan. Untuk layanan kritis, organisasi dapat melakukan proof of concept dengan data terkontrol.

Kontrak harus mengatur tujuan penggunaan data, larangan penggunaan ulang tanpa izin, notifikasi insiden, perubahan model, hak audit, SLA, dukungan investigasi, penghapusan data, kepemilikan output, tanggung jawab, dan exit plan. Ketergantungan vendor perlu dipantau. Jika model atau API dihentikan, perusahaan harus dapat bermigrasi tanpa kehilangan operasi dan bukti. Vendor risk tidak berakhir setelah kontrak. Kinerja dan perubahan harus dipantau. Pembaruan model dasar dapat mengubah output meskipun aplikasi internal tidak berubah. Organisasi perlu menetapkan material change notification dan melakukan regression testing. Daftar subprosesor dan komponen open-source perlu diperbarui.

**Tabel 7.7** Due diligence vendor AI

| Area            | Pertanyaan kunci                              | Bukti                                        |
|-----------------|-----------------------------------------------|----------------------------------------------|
| <b>Data</b>     | Apakah data digunakan ulang untuk pelatihan?  | DPA, privacy notice, dan konfigurasi         |
| <b>Keamanan</b> | Bagaimana akses, enkripsi, SDLC, dan insiden? | Sertifikasi, pen-test, dan laporan assurance |

|                    |                                         |                                              |
|--------------------|-----------------------------------------|----------------------------------------------|
| <b>Model</b>       | Apa batas, metrik, bias, dan perubahan? | System card dan change notice                |
| <b>Operasi</b>     | Apa SLA, kapasitas, dan pemulihan?      | SLA, BCP, dan status history                 |
| <b>Subprosesor</b> | Siapa pihak lain dan lokasi data?       | Daftar subprosesor dan mekanisme persetujuan |
| <b>Exit</b>        | Bagaimana ekspor dan penghapusan data?  | Exit plan dan deletion certificate           |

## 7.8 RESPONS INSIDEN DAN KEBERLANGSUNGAN

Insiden AI dapat berupa keputusan salah massal, bias, kebocoran data, manipulasi, model tidak tersedia, biaya tak terkendali, atau output berbahaya. Prosedur respons harus terhubung dengan keamanan siber, privasi, hukum, komunikasi, dan bisnis. Tim perlu mengetahui siapa yang dapat menghentikan model, menonaktifkan fitur, atau beralih ke proses manual.

Triage menilai dampak, skala, pihak terdampak, data, dan kewajiban notifikasi. Kontainmen dapat berupa rollback, blokir akses, pembatasan use case, atau penghentian sementara. Investigasi membutuhkan log, versi, input, output, perubahan, dan keputusan manusia. Setelah pemulihan, organisasi melakukan root cause analysis dan melacak tindakan sampai selesai.

*Business continuity* memastikan proses penting tetap berjalan ketika AI gagal. Fallback dapat berupa aturan sederhana, model cadangan, atau prosedur manual. Fallback harus diuji, bukan hanya ditulis. Organisasi juga perlu menyiapkan komunikasi yang jujur kepada pelanggan dan regulator apabila insiden material terjadi.

**Tabel 7.8** Playbook insiden AI

| Tahap               | Pertanyaan                                   | Tindakan minimum                                   |
|---------------------|----------------------------------------------|----------------------------------------------------|
| <b>Deteksi</b>      | Apa sinyal dan apakah bukti perlu diamankan? | Buat tiket, simpan log, dan hubungi on-call        |
| <b>Triage</b>       | Siapa terdampak dan seberapa luas?           | Tetapkan severity dan tim                          |
| <b>Kontainmen</b>   | Bagaimana menghentikan dampak?               | Disable, rollback, blokir, atau manual fallback    |
| <b>Investigasi</b>  | Apa akar teknis dan proses?                  | Analisis data, model, akses, vendor, dan keputusan |
| <b>Pemulihan</b>    | Apa syarat aman untuk rilis?                 | Perbaiki, validasi, approve, dan monitor ketat     |
| <b>Pembelajaran</b> | Apa yang harus diubah?                       | RCA, komunikasi, action plan, dan update kontrol   |

## 7.9. SISTEM HARGA DINAMIS PT NIAGA NUSANTARA

PT Niaga Nusantara menggunakan AI untuk merekomendasikan harga berdasarkan permintaan, stok, pesaing, dan promosi. Dalam simulasi, model beberapa kali menurunkan harga di bawah biaya karena data promosi terlambat. Risiko diperburuk oleh rencana memberi sistem kewenangan mengubah harga otomatis pada ribuan produk.

Tim menerapkan batas margin minimum, batas perubahan harian, dan approval untuk produk sensitif. Data promosi memiliki freshness check; jika terlambat, model tidak boleh

digunakan. Harga yang menyimpang dari distribusi normal memicu alert. Semua perubahan dicatat dan dapat di-rollback. Pada tahap awal, model hanya memberi rekomendasi. Setelah pilot stabil, otonomi diberikan untuk produk berisiko rendah dengan batas nilai. Produk obat, kebutuhan pokok tertentu, dan barang kontrak tetap memerlukan persetujuan. Komite menilai keluhan pelanggan, margin, fairness, dan anomali. Vendor data pesaing diwajibkan memberi notifikasi perubahan metode.

Kasus ini menunjukkan mitigasi berlapis. Tidak ada satu kontrol yang cukup. Batas bisnis mencegah kerugian, freshness check menjaga kualitas data, approval manusia mengendalikan dampak, monitoring mendeteksi penyimpangan, dan rollback mempercepat pemulihan.

**Tabel 7.9** Lapisan mitigasi sistem harga dinamis

| Lapisan              | Kontrol                                           | Tujuan                             |
|----------------------|---------------------------------------------------|------------------------------------|
| <b>Desain</b>        | Produk sensitif dikecualikan dan otonomi bertahap | Mengurangi blast radius            |
| <b>Data</b>          | Freshness check promosi dan pesaing               | Mencegah keputusan dari data usang |
| <b>Aturan bisnis</b> | Floor, ceiling, dan batas perubahan               | Mencegah harga ekstrem             |
| <b>Manusia</b>       | Approval untuk nilai material                     | Menjaga konteks dan akuntabilitas  |
| <b>Monitoring</b>    | Anomaly alert, margin, keluhan, fairness          | Deteksi dini                       |
| <b>Pemulihan</b>     | Rollback dan rekonsiliasi                         | Mempercepat koreksi                |

## KESIMPULAN

Mitigasi risiko AI menggabungkan penghindaran, desain ulang, kontrol teknis, kontrol proses, pengawasan manusia, budaya, vendor management, dan respons insiden. Kontrol harus terkait dengan skenario, memiliki pemilik, bukti, ambang, dan tindakan. Keberadaan kebijakan tidak membuktikan efektivitas. Organisasi perlu membangun kemampuan menghentikan sistem, bukan hanya meluncurkannya. Tata kelola yang baik memberi ruang inovasi karena batas dan jalur eskalasi jelas. Risiko residual diterima secara sadar dan dipantau, bukan diabaikan.

## LATIHAN SOAL

1. Susun hierarki kontrol untuk risiko halusinasi chatbot.
2. Jelaskan kapan human-in-the-loop lebih tepat daripada human-on-the-loop.
3. Buat lima aturan Acceptable Use Policy untuk AI generatif.
4. Rancang tiga indikator yang dapat menunjukkan overreliance pengguna.
5. Sebutkan klausul kontrak vendor AI yang paling penting bagi perlindungan data.
6. Buat skenario respons insiden ketika model harga mengubah ribuan produk secara salah.
7. Jelaskan cara menilai efektivitas program literasi AI.
8. Uraikan hubungan MLOps, monitoring, dan manajemen risiko.

**PILIHAN GANDA**

1. Kontrol paling kuat biasanya dimulai dari ...
  - a. desain dan sumber risiko
  - b. disclaimer
  - c. warna dashboard
  - d. audit tahunan saja
2. Human-in-the-loop berarti ...
  - a. manusia menyetujui keputusan kritis
  - b. AI tanpa manusia
  - c. vendor memutuskan
  - d. tidak ada log
3. Shadow AI adalah ...
  - a. AI transparan
  - b. alat AI yang digunakan tanpa persetujuan
  - c. model open source
  - d. AI yang tidak aktif
4. Kill switch digunakan untuk ...
  - a. mempercepat training
  - b. menghentikan sistem saat risiko tidak terkendali
  - c. menghapus kontrak
  - d. menambah data
5. RACI membantu ...
  - a. membagi peran dan akuntabilitas
  - b. menghitung akurasi
  - c. menentukan warna
  - d. mengganti enkripsi
6. Alert fatigue terjadi karena ...
  - a. terlalu banyak peringatan
  - b. kurang logo
  - c. model kecil
  - d. data terenkripsi
7. Canary release bertujuan ...
  - a. membatasi paparan awal
  - b. merilis ke semua pengguna
  - c. menghapus testing
  - d. mengganti owner
8. Kontrol vendor berakhir ...
  - a. setelah kontrak
  - b. tidak; perubahan dan kinerja tetap dipantau
  - c. setelah invoice
  - d. ketika audit selesai

- 9.** Fallback perlu ...
- a. ditulis dan diuji
  - b. dirahasiakan dari operasi
  - c. dihapus
  - d. hanya digunakan vendor
- 10.** Residual risk diterima oleh ...
- a. pihak berwenang sesuai appetite
  - b. siapa saja
  - c. model
  - d. pelanggan tanpa informasi

## BAB 8

# IMPLEMENTASI SISTEM MANAJEMEN RISIKO AI PADA PERUSAHAAN DAGANG

---

Bagaimana organisasi bergerak dari kebijakan menuju operasi yang terukur?

### CAPAIAN PEMBELAJARAN

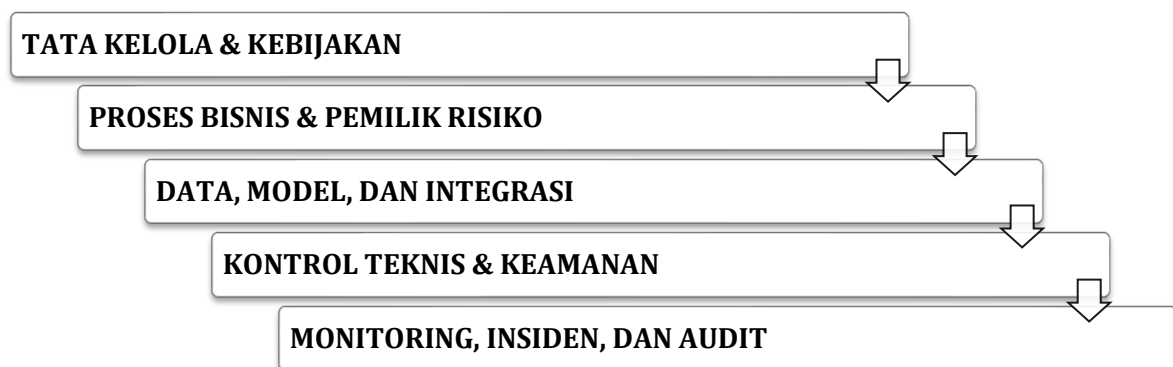
- Menyusun mandat dan sasaran program.
- Membangun inventaris dan klasifikasi.
- Merancang stage-gate dan paket dokumentasi.
- Menetapkan KRI, monitoring, dan insiden.
- Menyusun roadmap implementasi.

## 8.1 DARI KEBIJAKAN MENUJU SISTEM OPERASIONAL

Banyak organisasi memiliki kebijakan AI yang baik tetapi kesulitan menerapkannya. Kesenjangan terjadi karena kebijakan tidak diterjemahkan menjadi peran, alur kerja, artefak, indikator, dan keputusan. Implementasi sistem manajemen risiko AI bertujuan memastikan setiap use case melalui proses yang konsisten sejak gagasan, pengadaan, pembangunan, pengujian, penggunaan, pemantauan, sampai penghentian. Sistem tersebut harus cukup kuat untuk mengendalikan risiko, tetapi cukup sederhana agar digunakan oleh bisnis.

ISO/IEC 42001 memperkenalkan sistem manajemen AI yang dapat diintegrasikan dengan sistem manajemen lain. NIST AI RMF menggunakan fungsi Govern, Map, Measure, dan Manage. ISO/IEC 23894 memberi panduan risiko khusus AI. Perusahaan tidak perlu membuat tiga birokrasi berbeda. Unsur yang sama dapat digabungkan: kebijakan dan peran pada Govern, konteks dan pemetaan dampak pada Map, pengujian pada Measure, serta kontrol dan pemantauan pada Manage. Siklus Plan-Do-Check-Act membantu memastikan sistem terus diperbaiki.

Implementasi sebaiknya dimulai dari use case dan keputusan bisnis, bukan dari pembelian platform. Organisasi perlu menjawab masalah apa yang ingin diselesaikan, siapa yang diuntungkan, siapa yang dapat dirugikan, data apa yang digunakan, dan bagaimana keberhasilan diukur. Teknologi yang tidak memiliki pemilik bisnis akan menjadi eksperimen tanpa akuntabilitas. Sebaliknya, tekanan bisnis tanpa pengawasan teknis dapat menghasilkan penerapan yang berisiko.



**Gambar 8.1** Arsitektur berlapis untuk implementasi manajemen risiko AI.

*Sumber: diolah untuk diktat ini.*

### PRINSIP IMPLEMENTASI

Mulai dari tujuan dan risiko, bangun proses minimum yang dapat dijalankan, pilih pilot yang terukur, kumpulkan bukti, lalu tingkatkan skala secara bertahap.

## 8.2 MENETAPKAN MANDAT, RUANG LINGKUP, DAN SASARAN

Mandat menjelaskan alasan organisasi membangun tata kelola AI dan kewenangan yang diberikan kepada pemilik sistem. Mandat dapat berasal dari strategi digital, kebutuhan

risiko, regulasi, atau permintaan pelanggan. Dokumen mandat sebaiknya disetujui pimpinan dan mencakup prinsip, ruang lingkup, sumber daya, serta ekspektasi pelaporan. Tanpa mandat, komite dan fungsi risiko akan kesulitan meminta data atau menghentikan use case yang tidak aman.

Ruang lingkup perlu mendefinisikan apa yang dianggap sistem AI. Organisasi dapat mencakup machine learning, generative AI, algoritma keputusan, computer vision, dan otomasi yang menggunakan model. Definisi yang terlalu sempit dapat melewatkan sistem lama yang berdampak besar, sedangkan definisi terlalu luas membebani proses. Kriteria materialitas membantu: dampak keputusan, jenis data, jumlah pengguna, otonomi, skala, dan paparan eksternal.

Sasaran sistem manajemen harus terukur. Contohnya: seluruh use case material terinventarisasi; penilaian dampak selesai sebelum produksi; model kritis memiliki validasi independen; insiden dilaporkan dalam batas waktu; perubahan material melalui review; dan temuan audit diselesaikan tepat waktu. Sasaran sebaiknya dihubungkan dengan indikator dan target, tetapi tidak mendorong perilaku semu. Target 100 persen dokumen lengkap tidak bermanfaat jika kualitas review buruk.

**Tabel 8.1** Contoh sasaran sistem manajemen risiko AI

| Sasaran                        | Indikator                            | Target awal                 | Pemilik             |
|--------------------------------|--------------------------------------|-----------------------------|---------------------|
| <b>Visibilitas use case</b>    | Persentase use case terinventarisasi | 100% material dalam 3 bulan | CIO/Komite AI       |
| <b>Penilaian sebelum rilis</b> | Persentase use case melalui gate     | 100% sedang-tinggi          | Pemilik bisnis      |
| <b>Validasi independen</b>     | Model tinggi tervalidasi             | 100% sebelum produksi       | Model risk          |
| <b>Respons insiden</b>         | Waktu triage insiden tinggi          | Kurang dari 2 jam           | Security/Operations |
| <b>Perbaikan temuan</b>        | Temuan lewat jatuh tempo             | Di bawah 10%                | Pemilik tindakan    |

### 8.3 INVENTARISASI DAN KLASIFIKASI USE CASE AI

Inventaris AI adalah sumber kebenaran mengenai sistem yang dibangun, dibeli, atau digunakan. Inventaris minimal memuat nama, tujuan, pemilik bisnis, pemilik teknis, vendor, data, model, pengguna, keputusan yang dipengaruhi, status siklus hidup, lokasi operasi, dan tingkat risiko. Inventaris juga perlu mencakup eksperimen yang menggunakan data nyata serta alat generatif yang digunakan secara luas.

Klasifikasi risiko membantu menerapkan prinsip proportionality. Use case berisiko rendah dapat melalui proses ringkas, sedangkan use case tinggi memerlukan penilaian dampak, validasi independen, approval, dan monitoring lebih kuat. Faktor klasifikasi meliputi dampak terhadap hak atau akses layanan, data sensitif, otonomi, skala, reversibilitas, keselamatan, paparan publik, serta ketergantungan vendor. Skor otomatis dapat membantu, tetapi keputusan akhir perlu direview. Inventaris harus terhubung dengan aset lain: katalog data, CMDB, vendor register, risk register, dan incident register. Integrasi mengurangi

duplikasi dan memudahkan analisis konsentrasi. Bila satu vendor atau model dasar digunakan oleh banyak use case, organisasi dapat melihat risiko sistemik. Pemilik wajib memperbarui inventaris ketika status, data, model, atau tujuan berubah.

**Tabel 8.2** Elemen inventaris AI

| Kelompok data      | Elemen minimum                          | Contoh                             |
|--------------------|-----------------------------------------|------------------------------------|
| <b>Identitas</b>   | Nama, ID, status, versi                 | AI-INV-017, produksi, v3.2         |
| <b>Tujuan</b>      | Masalah, keputusan, pengguna            | Prediksi permintaan mingguan       |
| <b>Kepemilikan</b> | Owner bisnis, teknis, data, vendor      | Supply Chain, Data Team, Vendor X  |
| <b>Teknologi</b>   | Model, platform, API, lokasi            | Gradient boosting, cloud region ID |
| <b>Data</b>        | Sumber, kategori, sensitivitas          | POS, promosi, data pelanggan       |
| <b>Risiko</b>      | Klasifikasi, residual, approval         | Tinggi, sedang, Komite 12/2026     |
| <b>Operasi</b>     | KRI, insiden, perubahan, tanggal review | Drift, incident 2, review triwulan |

#### 8.4 STAGE-GATE SIKLUS HIDUP AI

Stage-gate membagi siklus hidup menjadi tahap dan titik keputusan. Tahap umum meliputi ide, desain, pembangunan atau pengadaan, pengujian, persetujuan rilis, operasi, perubahan, dan pensiun. Setiap gate memiliki kriteria dan bukti minimum. Keputusan dapat berupa lanjut, perbaiki, batasi, tunda, atau hentikan. Dengan demikian, risiko tidak dikumpulkan di akhir proyek ketika biaya perubahan sudah tinggi.

Pada gate ide, tim menilai kebutuhan, alternatif non-AI, manfaat, dan dampak awal. Pada desain, tim menetapkan data, arsitektur, kontrol, dan metrik. Pada build, tim menerapkan keamanan, versioning, serta dokumentasi. Pada test, dilakukan validasi kinerja, fairness, keamanan, privasi, dan kesiapan proses. Pada release, pemilik risiko menerima residual risk. Pada operasi, indikator dan insiden dipantau. Pada pensiun, akses ditutup, data dihapus atau diarsipkan, dan ketergantungan diputus.

Kriteria gate harus proporsional. Pilot internal kecil tidak memerlukan dokumen sebanyak model yang menentukan kredit pelanggan. Namun, kontrol minimum tetap berlaku: tujuan, pemilik, sumber data, batas, keamanan, dan review. Organisasi dapat menggunakan jalur cepat untuk risiko rendah dan jalur lengkap untuk risiko tinggi. Jalur cepat bukan pengecualian tanpa catatan; ia tetap memiliki bukti ringkas.



*Gate = Keputusan formal: lanjut, perbaiki, batasi, atau hentikan.*

**Gambar 8.2** Stage-gate dalam siklus hidup sistem AI.

*Sumber: diolah untuk diktat ini.*

**Tabel 8.3** Gate dan bukti minimum siklus hidup AI

| Gate             | Pertanyaan keputusan                               | Bukti minimum                                |
|------------------|----------------------------------------------------|----------------------------------------------|
| <b>Ide</b>       | Apakah AI diperlukan dan bernilai?                 | Business case, alternatif, impact screening  |
| <b>Desain</b>    | Apakah data, risiko, dan kontrol memadai?          | AI/IA, architecture, data plan, threat model |
| <b>Build/Buy</b> | Apakah solusi dibangun/dipilih dengan aman?        | Code review atau due diligence vendor        |
| <b>Test</b>      | Apakah kinerja, fairness, privacy, security lulus? | Validation report dan remediation            |
| <b>Release</b>   | Apakah residual risk diterima dan operasi siap?    | Approval, SOP, monitoring, rollback          |
| <b>Operate</b>   | Apakah sistem tetap dalam batas?                   | KRI, alert, incident, review                 |
| <b>Retire</b>    | Apakah data, akses, dan ketergantungan ditutup?    | Decommission checklist dan deletion evidence |

### 8.5 ORGANISASI, RACI, DAN MEKANISME KEPUTUSAN

Struktur tata kelola harus mengikuti ukuran organisasi. UMKM dapat menugaskan pemilik usaha, penanggung jawab TI, dan penasihat eksternal. Perusahaan menengah dapat membentuk forum lintas fungsi. Korporasi besar memerlukan komite di tingkat eksekutif, working group, serta peran khusus seperti model risk management atau responsible AI. Yang penting adalah kejelasan keputusan dan eskalasi, bukan jumlah komite.

RACI mengidentifikasi siapa *Responsible*, *Accountable*, *Consulted*, dan *Informed*. Satu aktivitas sebaiknya memiliki satu pihak accountable. Contohnya, pemilik bisnis accountable atas tujuan dan residual risk; tim data responsible membangun; keamanan consulted untuk threat model; audit internal informed atau melakukan assurance independen. RACI perlu disertai kewenangan nyata, termasuk siapa dapat menghentikan sistem.

Mekanisme keputusan perlu memiliki agenda, bahan, kriteria, *quorum*, konflik kepentingan, dan pencatatan. Komite harus menerima ringkasan yang memadai: tujuan, manfaat, risiko, hasil uji, residual risk, dan keputusan yang diminta. Pertemuan tidak boleh menjadi presentasi satu arah. Anggota perlu melakukan challenge dan mencatat syarat. Keputusan dengan syarat harus dilacak.

**Tabel 8.4** RACI implementasi program AI

| Aktivitas                         | Direksi | Komite AI | Bisnis | TI/Data | Risiko | Audit |
|-----------------------------------|---------|-----------|--------|---------|--------|-------|
| <b>Kebijakan dan appetite</b>     | A       | R         | C      | C       | C      | I     |
| <b>Inventaris dan klasifikasi</b> | I       | A         | R      | R       | C      | I     |
| <b>Stage-gate use case</b>        | I       | A         | R      | R       | C      | I     |
| <b>Validasi tinggi</b>            | I       | C         | C      | C       | R/A    | I     |
| <b>Monitoring dan insiden</b>     | I       | A         | R      | R       | C      | I     |
| <b>Audit program</b>              | I       | I         | C      | C       | C      | R/A   |

## 8.6 PENGELOLAAN DATA, MODEL, DAN DOKUMENTASI

Data governance untuk AI mencakup sumber, izin, kualitas, lineage, representativitas, akses, retensi, dan perubahan. Dataset sheet mendokumentasikan tujuan, populasi, periode, metode pengumpulan, transformasi, batasan, serta kelompok yang kurang terwakili. Katalog data membantu penemuan, tetapi organisasi tetap memerlukan kontrol penggunaan. Data yang tersedia tidak otomatis boleh digunakan untuk setiap tujuan.

Model governance mencakup identitas model, versi, tujuan, metrik, batas, pemilik, validasi, approval, dan status. Model card meringkas informasi bagi pengguna dan reviewer. Untuk model vendor, organisasi dapat membuat system card internal yang mendokumentasikan konfigurasi, prompt, knowledge base, guardrail, dan hasil pengujian. Perubahan model dasar harus diperlakukan sebagai perubahan material jika dapat mengubah perilaku.

Dokumentasi harus living. Pipeline dapat menghasilkan sebagian bukti secara otomatis, seperti versi kode, hasil uji, dan log rilis. Bukti manual tetap diperlukan untuk keputusan, dampak, dan penilaian etis. Kualitas lebih penting daripada volume. Template sebaiknya menggunakan pertanyaan yang membantu berpikir, bukan kolom yang diisi dengan kata “sesuai”.

**Tabel 8.5** Paket dokumentasi sistem AI

| Dokumen                     | Tujuan                                           | Pemilik       | Pembaruan                |
|-----------------------------|--------------------------------------------------|---------------|--------------------------|
| <b>Use-case charter</b>     | Menetapkan tujuan, keputusan, manfaat, dan batas | Bisnis        | Saat tujuan berubah      |
| <b>AI Impact Assessment</b> | Menilai dampak dan residual risk                 | Bisnis/Risiko | Perubahan material       |
| <b>Dataset sheet</b>        | Mendokumentasikan sumber dan batas data          | Data owner    | Dataset berubah          |
| <b>Model/System card</b>    | Meringkas model, metrik, batas, dan penggunaan   | Model owner   | Versi model berubah      |
| <b>Validation report</b>    | Memberi challenge independen                     | Validator     | Sebelum rilis/revalidasi |
| <b>Operational runbook</b>  | Monitoring, fallback, dan insiden                | Operations    | Proses berubah           |
| <b>Decision record</b>      | Mencatat approval dan syarat                     | Komite/Owner  | Setiap gate              |

## 8.7 VALIDASI, PERSETUJUAN, DAN PELUNCURAN TERKENDALI

Validasi independen penting untuk model material. Independensi dapat dicapai melalui tim berbeda, reviewer senior, atau pihak eksternal. Validator menilai kesesuaian tujuan, data, metodologi, hasil, robustness, fairness, keamanan, dan implementasi. Temuan diklasifikasikan dan pemilik menentukan tindakan. Model tidak seharusnya dirilis dengan temuan kritis tanpa persetujuan risiko yang jelas.

Peluncuran terkendali dapat menggunakan *sandbox*, *shadow mode*, *canary release*, A/B test, dan pilot terbatas. Shadow mode memungkinkan model menghasilkan rekomendasi

tanpa memengaruhi keputusan, sehingga kinerja dapat dibandingkan. Canary release membatasi sebagian pengguna. Feature flag memungkinkan penghentian cepat. Teknik ini mengurangi blast radius ketika masalah muncul.

Readiness review memastikan proses pendukung siap. Apakah pengguna dilatih? Apakah help desk memahami masalah? Apakah monitoring aktif? Apakah fallback tersedia? Apakah komunikasi pelanggan disiapkan? Model yang baik dapat gagal jika operasi belum siap. Rilis harus mencakup rollback plan dan kriteria penghentian.

**Tabel 8.6** Checklist kesiapan rilis

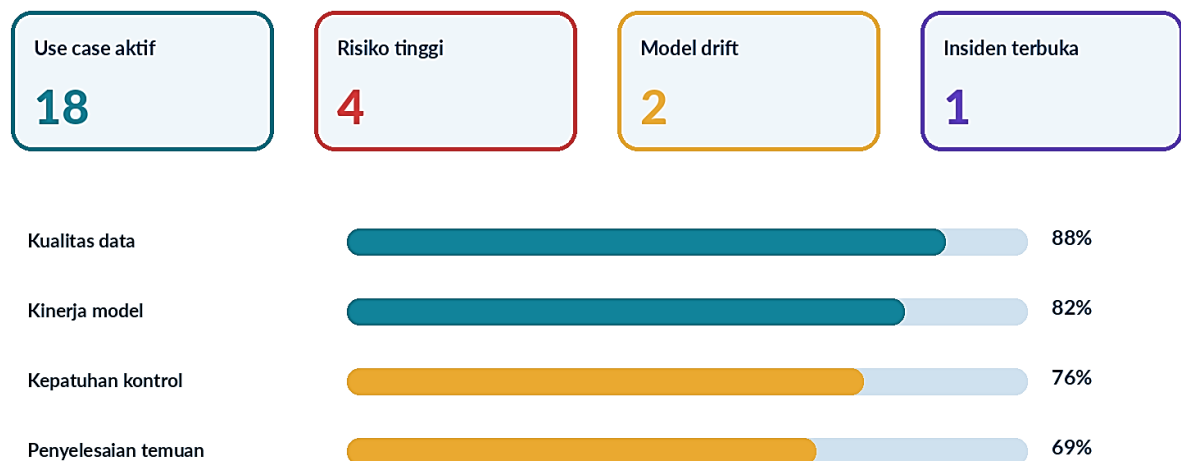
| Area                    | Kriteria                                                 | Status/Bukti |
|-------------------------|----------------------------------------------------------|--------------|
| <b>Bisnis</b>           | Tujuan, owner, user, dan manfaat terdefinisi             |              |
| <b>Risiko</b>           | AI/IA, residual risk, dan approval selesai               |              |
| <b>Data/model</b>       | Validation dan temuan kritis selesai                     |              |
| <b>Keamanan/privasi</b> | Threat test, access, retensi, dan DPA siap               |              |
| <b>Operasi</b>          | Monitoring, alert, help desk, dan fallback aktif         |              |
| <b>Pengguna</b>         | Pelatihan, panduan, dan komunikasi tersedia              |              |
| <b>Pemulihan</b>        | Feature flag, rollback, backup, dan kontak on-call diuji |              |

## 8.8 MONITORING, KRI, DASHBOARD, DAN PELAPORAN

Monitoring operasional mencakup availability, latensi, error, biaya, dan kapasitas. Monitoring model mencakup kinerja, drift, calibration, fairness, dan outlier. Monitoring risiko mencakup keluhan, override, insiden, pelanggaran kebijakan, dan dampak finansial. Indikator perlu dihubungkan dengan ambang serta tindakan. Setiap alarm memiliki pemilik dan SLA.

KRI berbeda dari KPI. KPI mengukur pencapaian, sedangkan KRI memberi sinyal peningkatan paparan risiko. Contoh KRI: persentase data terlambat, drift di atas ambang, peningkatan false positive, jumlah penggunaan alat tidak disetujui, atau konsentrasi use case pada satu vendor. KPI dapat berupa pengurangan waktu proses atau peningkatan service level. Keduanya perlu dibaca bersama agar efisiensi tidak menutupi risiko.

Dashboard untuk manajemen harus ringkas. Informasi penting mencakup jumlah use case per tingkat risiko, perubahan profil, insiden, temuan, model drift, status tindakan, dan keputusan yang dibutuhkan. Dashboard teknis dapat lebih rinci. Pelaporan perlu menjelaskan tren dan akar masalah, bukan hanya angka merah-hijau. Indikator yang selalu hijau mungkin menunjukkan ambang terlalu longgar.



**Gambar 8.3** Contoh dashboard risiko AI untuk komite manajemen.  
 Sumber: diolah untuk diktat ini.

**Tabel 8.7** Contoh KRI dan tindakan

| KRI                  | Ambang kuning          | Ambang merah        | Tindakan                          |
|----------------------|------------------------|---------------------|-----------------------------------|
| Data terlambat       | Lebih dari 2% record   | Lebih dari 5%       | Batasi model dan gunakan fallback |
| Drift fitur utama    | PSI 0,1-0,25           | Di atas 0,25        | Investigasi dan revalidasi        |
| False positive fraud | Naik 15% dari baseline | Naik 30%            | Kalibrasi dan sampling manual     |
| Keluhan terkait AI   | Tren naik 2 minggu     | Insiden massal      | Triage dan hentikan fitur         |
| Override manusia     | Di atas 20%            | Di atas 40%         | Review model atau proses          |
| Vendor availability  | Di bawah 99,8%         | Di bawah SLA kritis | Aktifkan alternatif dan eskalasi  |

## 8.9 MANAJEMEN PERUBAHAN DAN MATERIAL CHANGE

Sistem AI berubah melalui data baru, retraining, pembaruan library, model dasar, prompt, knowledge base, atau integrasi. Perubahan kecil dapat memiliki dampak besar. Organisasi perlu mendefinisikan material change, misalnya tujuan baru, data sensitif baru, perubahan kelompok pengguna, peningkatan otonomi, ekspansi geografis, atau penurunan metrik melewati batas.

Perubahan material melalui penilaian ulang dan approval. Regression testing memastikan fungsi lama tidak rusak. Perubahan darurat dapat dipercepat, tetapi harus direview setelahnya. Change log harus menjelaskan apa, mengapa, siapa, hasil uji, dan rollback. Pada layanan vendor, perubahan dapat terjadi tanpa kontrol langsung; kontrak dan monitoring perlu mengatasinya.

Model drift bukan selalu alasan retraining. Tim perlu memahami penyebab. Retraining dengan data yang terkontaminasi dapat memperburuk masalah. Pilihan dapat berupa

memperbaiki data, mengubah fitur, menyesuaikan ambang, membatasi segmen, atau menghentikan model. Setiap tindakan perlu diuji dan disetujui.

**Tabel 8.8** Perubahan material dan respons

| Perubahan                      | Mengapa material                       | Respons minimum                          |
|--------------------------------|----------------------------------------|------------------------------------------|
| <b>Tujuan penggunaan baru</b>  | Dampak dan legal basis berubah         | AIIA dan approval ulang                  |
| <b>Data sensitif baru</b>      | Paparan privasi meningkat              | DPIA, security review, dan consent/basis |
| <b>Model dasar/vendor baru</b> | Perilaku dan supply chain berubah      | Regression, due diligence, dan red test  |
| <b>Otonomi meningkat</b>       | Blast radius dan akuntabilitas berubah | Oversight design dan limit               |
| <b>Ekspansi negara/segmen</b>  | Regulasi dan fairness berubah          | Legal review dan segment test            |
| <b>Metrik melewati batas</b>   | Kinerja tidak lagi dapat diterima      | Kontainmen, RCA, dan revalidasi          |

#### 8.10 RESPONS INSIDEN, KEBERLANGSUNGAN, DAN KOMUNIKASI

Rencana respons insiden AI harus selaras dengan keamanan siber dan privasi. Kategori insiden mencakup kegagalan kinerja, bias, data, keamanan, konten, operasi, vendor, dan kepatuhan. Severity ditetapkan berdasarkan dampak, skala, data sensitif, dan reversibilitas. Kontak on-call dan kewenangan kill switch harus jelas.

Alur respons meliputi deteksi, triage, kontainmen, investigasi, pemulihan, komunikasi, dan pembelajaran. Kontainmen dapat berupa menonaktifkan fitur, memblokir alat, rollback, atau beralih ke manual. Investigasi mengamankan bukti dan menghindari perubahan log. Komunikasi harus faktual, tidak spekulatif, dan dikoordinasikan dengan hukum. Simulasi tabletop membantu menguji kesiapan. Skenario dapat berupa chatbot membocorkan data, model harga salah, vendor tidak tersedia, atau deepfake meniru eksekutif. Peserta menilai keputusan, informasi, dan hambatan. Hasil simulasi menjadi action plan. Latihan perlu diulang setelah perubahan besar.



**Gambar 8.4** Alur respons insiden AI dari deteksi hingga pembelajaran.

*Sumber: diolah untuk diktat ini.*

**Tabel 8.9** Peran dalam respons insiden AI

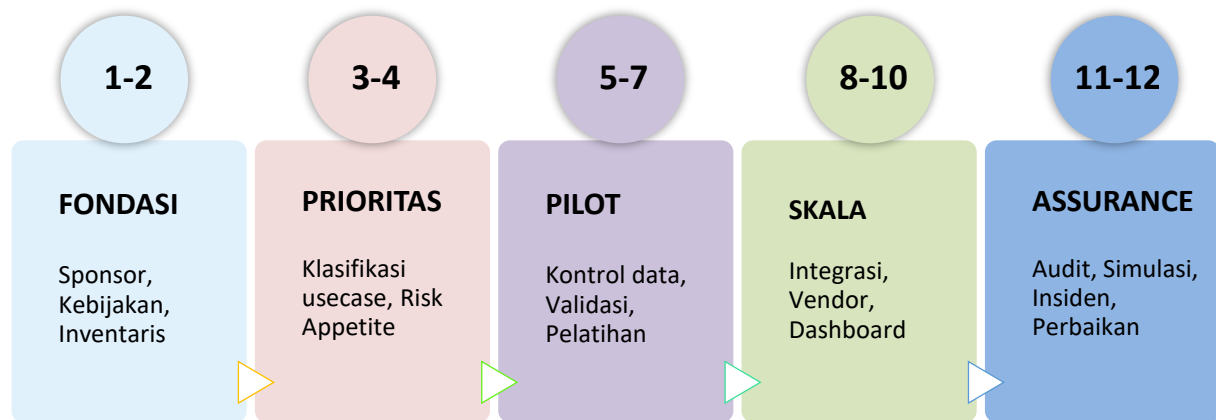
| Peran                     | Tanggung jawab                                     |
|---------------------------|----------------------------------------------------|
| <b>Incident commander</b> | Mengkoordinasikan keputusan, prioritas, dan status |
| <b>Pemilik bisnis</b>     | Menilai dampak pelanggan dan kontinuitas           |
| <b>Tim teknis/model</b>   | Mengamankan bukti, mendiagnosis, dan memperbaiki   |
| <b>Keamanan/privasi</b>   | Menilai serangan, data, notifikasi, dan forensik   |
| <b>Hukum/kepatuhan</b>    | Menilai kewajiban, kontrak, dan komunikasi         |
| <b>Komunikasi</b>         | Menyiapkan pesan internal dan eksternal            |
| <b>Audit/assurance</b>    | Mengamati independen dan menilai tindak lanjut     |

### 8.11 PETA JALAN IMPLEMENTASI 12 BULAN

Peta jalan perlu realistis. Bulan pertama fokus pada sponsor, mandat, definisi, dan tim inti. Bulan berikutnya menyusun kebijakan minimum, inventaris, dan klasifikasi. Setelah fondasi, organisasi memilih pilot yang bernilai tetapi tidak terlalu berisiko. Pilot digunakan untuk menguji template, gate, monitoring, dan pelatihan.

Pada fase skala, proses diintegrasikan dengan pengadaan, SDLC, data governance, keamanan, dan enterprise risk management. Dashboard dan pelaporan dikembangkan dari kebutuhan keputusan. Vendor kritis dinilai. Pada fase assurance, audit internal atau reviewer independen menilai desain dan efektivitas. Simulasi insiden dan management review menghasilkan rencana perbaikan. Peta jalan harus memiliki deliverable, pemilik, ketergantungan, anggaran, dan indikator. Organisasi sebaiknya tidak menunggu sistem

sempurna. Minimum viable governance dapat diluncurkan, kemudian diperbaiki. Namun, use case berisiko tinggi tidak boleh dijadikan eksperimen tanpa kontrol.



**Gambar 8.5** Peta jalan implementasi tata kelola AI selama 12 bulan.

*Sumber: diolah untuk diktat ini.*

**Tabel 8.10** Roadmap implementasi 12 bulan

| Periode     | Fokus       | Deliverable                                                 |
|-------------|-------------|-------------------------------------------------------------|
| Bulan 1-2   | Fondasi     | Mandat, definisi, sponsor, tim, dan prinsip                 |
| Bulan 3-4   | Visibilitas | Inventaris, klasifikasi, acceptable use, dan training dasar |
| Bulan 5-7   | Pilot       | Stage-gate, AIIA, model card, validasi, dan monitoring      |
| Bulan 8-10  | Integrasi   | Procurement, SDLC, vendor, dashboard, dan incident playbook |
| Bulan 11-12 | Assurance   | Audit, tabletop, management review, dan improvement plan    |

## 8.12 STUDI KASUS TERPADU PADA PT NIAGA NUSANTARA

PT Niaga Nusantara adalah perusahaan dagang omnichannel dengan toko, marketplace, gudang, dan program loyalitas. Perusahaan memiliki chatbot, prediksi permintaan, deteksi fraud, rekomendasi produk, dan pilot harga dinamis. Sistem dikembangkan oleh tim berbeda dan beberapa menggunakan vendor. Tidak ada inventaris terpadu. Ketika pelanggan mengeluh tentang rekomendasi yang tidak sesuai, manajemen kesulitan menemukan pemilik.

Direksi menetapkan program 12 bulan. Tim membuat inventaris dan menemukan 27 use case, termasuk lima alat generatif yang digunakan tanpa persetujuan. Use case diklasifikasikan. Model kredit dan harga dinamis masuk kategori tinggi; rekomendasi internal rendah. Kebijakan penggunaan diterbitkan dan alat alternatif aman disediakan. Komite lintas fungsi dibentuk.

Pilot governance diterapkan pada prediksi permintaan. Tim menggunakan stage-gate, dataset sheet, model card, validasi, dan monitoring. Setelah berhasil, proses diintegrasikan ke pengadaan dan pengembangan. Vendor diwajibkan memberi dokumentasi dan notifikasi perubahan. Dashboard memperlihatkan konsentrasi pada satu penyedia cloud, sehingga perusahaan menyiapkan rencana alternatif.

Pada bulan kesepuluh, simulasi insiden chatbot menunjukkan log tidak cukup untuk investigasi. Tim memperbaiki logging dan retensi. Audit internal menemukan bahwa beberapa approval terlalu umum. Komite memperjelas kriteria residual risk. Setelah setahun, perusahaan belum sempurna, tetapi memiliki visibilitas, pemilik, bukti, dan mekanisme belajar.

**Tabel 8.11** Hasil program PT Niaga Nusantara

| Masalah awal           | Tindakan                               | Hasil/bukti                     |
|------------------------|----------------------------------------|---------------------------------|
| Use case tersebar      | Inventaris dan owner                   | 27 use case terpetakan          |
| Shadow AI              | Policy dan alternatif aman             | Lima alat ditutup/dimigrasi     |
| Review tidak konsisten | Stage-gate dan template                | Approval dapat ditelusuri       |
| Ketergantungan vendor  | Concentration review dan exit plan     | Alternatif untuk layanan kritis |
| Log tidak memadai      | Simulasi insiden dan perbaikan logging | Investigasi dapat direperform   |
| Approval terlalu umum  | Kriteria residual risk diperjelas      | Keputusan lebih spesifik        |

### 8.13 MERANCANG SISTEM MANAJEMEN RISIKO AI

Peserta memilih perusahaan dagang nyata atau hipotetis. Proyek mencakup konteks, mandat, inventaris minimal lima use case, klasifikasi, struktur organisasi, RACI, stage-gate, daftar dokumen, KRI, roadmap, dan satu skenario insiden. Hasil disusun sebagai proposal implementasi 15-20 halaman dan dipresentasikan kepada “direksi”. Penilaian menggunakan rubrik: ketepatan konteks, kelengkapan risiko, proporsionalitas kontrol, kejelasan peran, keterukuran indikator, realistiknya roadmap, kualitas bukti, dan komunikasi. Peserta harus menunjukkan trade-off, bukan hanya daftar kontrol. Usulan perlu membedakan quick wins dan fondasi jangka panjang.

**Tabel 8.12** Rubrik proyek implementasi

| Kriteria                   | Bobot | Deskripsi kinerja unggul                                      |
|----------------------------|-------|---------------------------------------------------------------|
| Konteks dan strategi       | 15%   | Masalah, manfaat, pihak terdampak, dan batas jelas            |
| Inventaris dan klasifikasi | 15%   | Lengkap, konsisten, dan proporsional                          |
| Governance dan RACI        | 15%   | Peran, kewenangan, challenge, dan eskalasi jelas              |
| Proses dan kontrol         | 20%   | Stage-gate, data, model, monitoring, dan insiden terintegrasi |
| Roadmap dan sumber daya    | 15%   | Realistik, bertahap, dan memiliki dependensi                  |
| KRI dan assurance          | 10%   | Indikator dapat ditindaklanjuti dan audit-ready               |
| Komunikasi                 | 10%   | Ringkas, visual, dan dapat meyakinkan direksi                 |

### RINGKASAN BAB

Implementasi manajemen risiko AI mengubah prinsip menjadi proses operasi. Komponen utama meliputi mandat, ruang lingkup, inventaris, klasifikasi, stage-gate, peran, tata kelola data dan model, validasi, rilis terkendali, monitoring, perubahan, insiden, dan

assurance. Kerangka global dapat diintegrasikan agar tidak menambah birokrasi. Keberhasilan bergantung pada adopsi. Proses harus proporsional, terhubung dengan sistem yang sudah ada, dan menghasilkan keputusan. Organisasi memulai dari fondasi minimum, menguji melalui pilot, kemudian meningkatkan skala dan assurance.

### LATIHAN SOAL

1. Susun kriteria klasifikasi use case AI menjadi rendah, sedang, dan tinggi.
2. Jelaskan bukti minimum pada setiap stage-gate.
3. Buat RACI untuk model deteksi fraud.
4. Rancang lima KRI untuk chatbot pelanggan.
5. Sebutkan perubahan material yang memicu validasi ulang.
6. Buat skenario tabletop untuk kegagalan vendor model generatif.
7. Jelaskan perbedaan inventaris AI, katalog data, dan CMDB.
8. Rancang roadmap enam bulan untuk UMKM yang menggunakan AI.

### PILIHAN GANDA

1. Inventaris AI berfungsi sebagai ...
  - a. sumber kebenaran use case dan pemilik
  - b. daftar pegawai
  - c. laporan pajak
  - d. iklan
2. Stage-gate digunakan untuk ...
  - a. keputusan berbasis bukti tiap tahap
  - b. memperbanyak rapat
  - c. menghapus owner
  - d. mengganti hukum
3. Material change memerlukan ...
  - a. review dan pengujian ulang
  - b. tidak ada tindakan
  - c. hapus log
  - d. hanya email vendor
4. Shadow mode berarti ...
  - a. model berjalan tanpa memengaruhi keputusan nyata
  - b. model disembunyikan
  - c. AI dilarang
  - d. data dihapus
5. KRI memberi sinyal ...
  - a. peningkatan paparan risiko
  - b. warna merek
  - c. gaji
  - d. jumlah ruangan

6. Model card mendokumentasikan ...
  - a. tujuan, metrik, batas, dan penggunaan
  - b. hanya nama model
  - c. daftar pelanggan
  - d. kontrak kerja
7. Gate rilis harus memastikan ...
  - a. operasi, monitoring, fallback, dan approval siap
  - b. hanya akurasi
  - c. hanya desain UI
  - d. hanya biaya
8. AI inventory perlu dihubungkan dengan ...
  - a. data, vendor, risiko, dan insiden
  - b. media sosial saja
  - c. agenda rapat
  - d. absensi
9. Minimum viable governance berarti ...
  - a. fondasi minimum yang dapat dijalankan dan diperbaiki
  - b. tanpa kontrol
  - c. semua dokumen sekaligus
  - d. mengabaikan risiko tinggi
10. Management review digunakan untuk ...
  - a. menilai kinerja sistem dan peluang perbaikan
  - b. menulis kode
  - c. mengganti pelanggan
  - d. menghapus audit

# BAB 9

## AUDIT, KEPATUHAN, DAN PENINGKATAN BERKELANJUTAN

---

Bagaimana bukti, assurance, dan pembelajaran menjaga tata kelola AI tetap efektif?

### CAPAIAN PEMBELAJARAN

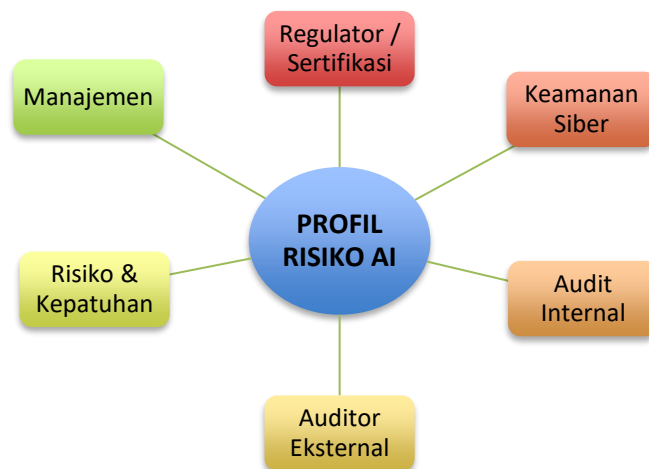
- Menyusun audit universe dan rencana berbasis risiko.
- Menguji tata kelola, data, model, keamanan, dan operasi.
- Menilai bukti dan menyusun temuan.
- Membangun assurance map dan maturity model.
- Merancang program peningkatan berkelanjutan.

### 9.1 PERAN AUDIT DAN ASSURANCE DALAM TATA KELOLA AI

Audit AI memberikan penilaian independen mengenai apakah tata kelola, manajemen risiko, dan kontrol sistem AI dirancang serta berjalan efektif. Audit tidak bertujuan menghambat inovasi atau menggantikan tanggung jawab manajemen. Assurance membantu dewan dan direksi memahami apakah informasi yang mereka terima dapat dipercaya, apakah risiko material telah dipetakan, dan apakah tindakan perbaikan benar-benar dilaksanakan.

Ruang lingkup audit dapat mencakup program tata kelola, satu model, satu proses, vendor, data, keamanan, atau kepatuhan. Auditor perlu memulai dari tujuan bisnis dan dampak, bukan sekadar algoritma. Model sederhana yang menentukan keputusan penting dapat lebih berisiko daripada model kompleks yang hanya membantu analisis internal. Audit berbasis risiko memprioritaskan sistem dengan dampak, otonomi, data sensitif, skala, dan perubahan tinggi.

Assurance berasal dari banyak pihak: manajemen, fungsi risiko, keamanan, privasi, validasi model, audit internal, auditor eksternal, regulator, dan sertifikasi. Koordinasi diperlukan agar tidak terjadi duplikasi atau celah. Assurance map menghubungkan risiko utama dengan pihak yang menguji, frekuensi, bukti, dan kesimpulan. Audit internal tetap menjaga independensi dan tidak menerima hasil fungsi lain secara otomatis tanpa menilai kualitasnya.



**Gambar 9.1** Peta assurance atas profil risiko AI.

Sumber: diolah untuk diktat ini.

#### PRINSIP AUDIT

Audit AI yang efektif berfokus pada bukti, dampak, dan keputusan. Auditor tidak harus menulis model, tetapi harus mampu menilai apakah klaim dapat dibuktikan dan apakah keterbatasan dikelola.

### 9.2 AUDIT UNIVERSE DAN PERENCANAAN BERBASIS RISIKO

Audit universe AI adalah daftar entitas yang dapat diaudit, seperti kebijakan, komite, inventaris, data, model, platform, use case, vendor, dan proses insiden. Universe harus

terhubung dengan inventaris AI dan diperbarui. Tanpa universe, audit cenderung memilih objek yang mudah dilihat dan melewatkan shadow AI atau ketergantungan sistemik.

*Risk assessment* audit mempertimbangkan dampak, data, otonomi, perubahan, insiden, keluhan, temuan, ketergantungan vendor, dan kematangan kontrol. Auditor juga mempertimbangkan kecepatan perubahan. Sistem generatif yang sering diperbarui mungkin membutuhkan review lebih sering daripada model statis. Hasil penilaian digunakan untuk rencana tahunan dan penugasan ad hoc.

*Tujuan audit harus spesifik.* Contohnya: menilai apakah inventaris lengkap; apakah penilaian dampak dilakukan sebelum rilis; apakah data dilindungi; apakah validasi independen; atau apakah monitoring mendeteksi drift. Kriteria audit dapat berasal dari kebijakan internal, kontrak, hukum, ISO/IEC 42001, NIST AI RMF, ISO/IEC 23894, OWASP, atau praktik industri. Kriteria harus disepakati dan relevan.

Rencana penugasan memuat ruang lingkup, periode, lokasi, sistem, tim, keahlian, metode, kebutuhan data, dan keterbatasan. Audit AI sering membutuhkan tim multidisiplin. Auditor internal dapat melibatkan data scientist, keamanan, hukum, atau spesialis independen, sambil menjaga pengelolaan konflik kepentingan

**Tabel 9.1** Contoh audit universe AI

| Entitas                    | Risiko utama                          | Frekuensi indikatif                   |
|----------------------------|---------------------------------------|---------------------------------------|
| Program tata kelola        | Mandat, peran, dan oversight lemah    | Tahunan                               |
| Inventaris dan klasifikasi | Shadow AI dan salah klasifikasi       | Semesteran                            |
| Model tinggi               | Kinerja, fairness, dan perubahan      | Tahunan atau saat material change     |
| Generative AI              | Prompt injection, data, dan konten    | Berbasis risiko/triwulanan monitoring |
| Vendor kritis              | Ketersediaan, data, dan concentration | Tahunan                               |
| Insiden dan BCP            | Respons lambat dan bukti tidak cukup  | Setelah insiden dan simulasi tahunan  |
| Data governance            | Kualitas, lineage, retensi, dan akses | Siklus audit data                     |

### 9.3 MEMAHAMI SISTEM DAN MENELUSURI SIKLUS HIDUP

Auditor perlu memahami alur dari tujuan hingga output. Walkthrough dimulai dengan pertanyaan: keputusan apa yang dipengaruhi, siapa pengguna, data apa masuk, bagaimana model memproses, kontrol apa bekerja, dan apa yang terjadi setelah output. Diagram arsitektur dan data lineage membantu, tetapi auditor perlu membandingkan dokumen dengan praktik.

Siklus hidup mencakup ide, desain, pengadaan, pembangunan, validasi, rilis, operasi, perubahan, dan pensiun. Auditor mengambil sampel use case dan menelusuri bukti pada setiap tahap. Apakah approval diberikan sebelum produksi? Apakah hasil uji lengkap? Apakah

perubahan vendor memicu review? Apakah sistem yang dihentikan benar-benar dicabut aksesnya?

Walkthrough pengguna penting. Auditor mengamati bagaimana output dibaca dan apakah manusia benar-benar melakukan review. Wawancara dapat mengungkap target yang mendorong bypass, kesulitan memahami penjelasan, atau ketergantungan pada spreadsheet. Bukti observasi perlu dikombinasikan dengan log dan reperformance.

**Tabel 9.2** Pertanyaan walkthrough sistem AI

| Tahap             | Pertanyaan auditor                          | Bukti                            |
|-------------------|---------------------------------------------|----------------------------------|
| <b>Tujuan</b>     | Keputusan apa dipengaruhi dan siapa owner?  | Charter dan wawancara            |
| <b>Input</b>      | Dari mana data dan siapa dapat mengubah?    | Lineage, access log, dan query   |
| <b>Model</b>      | Bagaimana versi, metrik, dan batas?         | Model card, repository, dan test |
| <b>Output</b>     | Bagaimana output digunakan dan direview?    | SOP, observasi, dan override log |
| <b>Monitoring</b> | Apa indikator dan siapa merespons?          | Dashboard, alert, dan tiket      |
| <b>Perubahan</b>  | Bagaimana retraining atau update disetujui? | Change record                    |
| <b>Insiden</b>    | Bagaimana sistem dihentikan dan dipulihkan? | Runbook dan exercise             |

### Audit Tata Kelola, Kebijakan, dan Akuntabilitas

Audit tata kelola menilai mandat, peran, kompetensi, agenda, keputusan, konflik kepentingan, dan pelaporan. Komite yang ada di atas kertas tetapi tidak menerima informasi risiko tidak efektif. Auditor memeriksa notulen, bahan rapat, keputusan bersyarat, tindak lanjut, dan eskalasi. Kualitas challenge lebih penting daripada jumlah rapat.

Kebijakan dinilai dari cakupan, kejelasan, persetujuan, komunikasi, penerapan, dan pembaruan. Auditor dapat menguji pengetahuan karyawan dan membandingkan penggunaan alat dengan daftar disetujui. Pengecualian perlu memiliki alasan, durasi, pemilik, dan kontrol kompensatif. Pengecualian yang terus diperpanjang menunjukkan kelemahan desain.

Akuntabilitas diuji melalui RACI, job description, approval, dan tindakan. Jika insiden terjadi, apakah pemilik dapat diidentifikasi? Apakah residual risk diterima oleh pihak berwenang? Apakah lini kedua memiliki akses dan kewenangan challenge? Apakah audit internal independen? Temuan tata kelola sering menjadi akar dari kelemahan teknis yang berulang.

**Tabel 9.3** Program audit tata kelola AI

| Tujuan kontrol         | Prosedur audit                      | Indikasi kelemahan                                |
|------------------------|-------------------------------------|---------------------------------------------------|
| Mandat jelas           | Periksa charter dan kewenangan      | Komite tidak dapat meminta data atau menghentikan |
| Keputusan berkualitas  | Sampel notulen dan challenge        | Semua use case disetujui tanpa syarat             |
| Peran akuntabel        | Bandingkan RACI dan praktik         | Tidak ada accountable owner                       |
| Kebijakan diterapkan   | Uji pengetahuan dan penggunaan alat | Shadow AI tinggi                                  |
| Pelaporan efektif      | Review dashboard dan eskalasi       | Risiko material tidak sampai direksi              |
| Independensi assurance | Nilai konflik dan reporting line    | Validator menguji modelnya sendiri tanpa review   |

#### 9.4 AUDIT DATA DAN PRIVASI

Audit data menilai legalitas, tujuan, kualitas, representativitas, lineage, akses, retensi, dan perubahan. Auditor memilih sampel dataset dan menelusuri sumber sampai penggunaan. Bukti dapat berupa persetujuan, kontrak, katalog, query, log akses, aturan kualitas, dan hasil rekonsiliasi. Data yang diperoleh secara sah dapat tetap tidak sesuai untuk tujuan model jika tidak representatif.

Pengujian kualitas dapat direperform. Auditor dapat menghitung missing value, duplikasi, outlier, ketidakkonsistenan kode, atau perubahan distribusi. Hasil dibandingkan dengan ambang dan laporan manajemen. Jika dashboard selalu menunjukkan data baik, auditor menilai definisi dan kemungkinan data berkualitas buruk dikeluarkan dari pengukuran. Privasi diuji melalui minimisasi, akses, enkripsi, pseudonimisasi, retensi, pemenuhan hak, dan respons insiden. Auditor menilai apakah data sensitif muncul di log, prompt, atau lingkungan uji. Untuk generative AI, auditor dapat menguji apakah sistem mengungkapkan informasi dari knowledge base kepada pengguna yang tidak berhak.

Dataset sheet dan data lineage menjadi bukti penting, tetapi auditor perlu memverifikasi. Sampel record dapat ditelusuri ke sumber dan transformasi. Perubahan data setelah validasi perlu diidentifikasi. Kontrol data yang kuat mengurangi risiko model dan mempermudah investigasi.

**Tabel 9.4** Prosedur audit data AI

| Area              | Prosedur                                              | Bukti                             |
|-------------------|-------------------------------------------------------|-----------------------------------|
| Legalitas/tujuan  | Telusuri dasar dan penggunaan aktual                  | Charter, consent/basis, kontrak   |
| Kualitas          | Reperform missing, duplicate, outlier, reconciliation | Query dan hasil perhitungan       |
| Representativitas | Bandingkan distribusi dengan populasi                 | Segment analysis                  |
| Lineage           | Telusuri sampel dari sumber ke fitur                  | Mapping dan transformation log    |
| Akses             | Review role dan sampel log                            | IAM, approvals, dan access review |
| Retensi           | Uji penghapusan dan arsip                             | Deletion log dan storage scan     |
| Privasi           | Uji data sensitif di log/prompt/test                  | DLP result dan sample evidence    |

#### 9.5 AUDIT MODEL, KINERJA, FAIRNESS, DAN EXPLAINABILITY

Audit model dimulai dengan tujuan dan metrik. Auditor menilai apakah metrik sesuai dampak dan apakah hasil dilaporkan jujur. Untuk fraud, akurasi saja tidak cukup. Untuk prediksi permintaan, rata-rata kesalahan dapat menutupi kegagalan pada produk penting. Auditor memeriksa segmentasi, periode, data uji, baseline, dan interval ketidakpastian.

Reperformance dapat dilakukan dengan menjalankan ulang sebagian pengujian menggunakan data dan kode yang dikendalikan. Auditor membandingkan hasil dengan laporan. Jika tidak memiliki akses kode, auditor dapat menggunakan test set dan black-box testing. Perbedaan perlu diselidiki. Reproducibility menunjukkan kualitas versioning dan dokumentasi.

Fairness audit menilai kelompok, metrik, ambang, dan proses banding. Auditor memeriksa apakah kelompok terdampak dipertimbangkan dan apakah perbedaan memiliki

alasan. Pengujian dapat dilakukan pada sampel sintetis atau historis. Auditor juga menilai fairness operasional: apakah review manusia konsisten dan apakah keluhan ditangani.

Explainability dinilai berdasarkan kebutuhan pengguna. Auditor dapat meminta pengguna menjelaskan output dan mengamati apakah penjelasan membantu. Penjelasan yang hanya dapat dipahami pengembang tidak memadai untuk petugas bisnis. Auditor menilai apakah keterbatasan dijelaskan dan apakah keputusan penting dapat ditinjau.

**Tabel 9.5** Prosedur audit model

| Area                       | Prosedur                            | Pertanyaan kesimpulan                     |
|----------------------------|-------------------------------------|-------------------------------------------|
| <b>Tujuan dan baseline</b> | Bandingkan dengan metode sederhana  | Apakah AI memberi nilai tambahan?         |
| <b>Metrik</b>              | Reperform dan uji per segmen        | Apakah metrik sesuai dampak?              |
| <b>Calibration</b>         | Bandingkan probabilitas dan outcome | Apakah skor dapat diinterpretasikan?      |
| <b>Fairness</b>            | Hitung perbedaan hasil/error        | Apakah perbedaan dikelola dan dijelaskan? |
| <b>Explainability</b>      | Uji penjelasan dengan pengguna      | Apakah pengguna dapat bertindak benar?    |
| <b>Robustness</b>          | Stress test dan out-of-distribution | Apakah kegagalan terkendali?              |
| <b>Reproducibility</b>     | Jalankan versi dan data yang sama   | Apakah hasil dapat direplikasi?           |

## 9.6 AUDIT KEAMANAN DAN KETAHANAN

Audit keamanan mencakup identitas, akses, rahasia, jaringan, API, data, model, prompt, plugin, dan supply chain. Auditor menilai threat model dan apakah ancaman khusus AI dipertimbangkan. Pengujian dapat mencakup prompt injection, akses tidak sah, output handling, excessive agency, dan kebocoran data, dilakukan secara aman dengan izin.

*Least privilege* sangat penting. Auditor memeriksa alat yang dapat dipanggil agen, batas transaksi, dan approval. Akun layanan dengan akses luas merupakan risiko. Log tindakan harus dapat dikaitkan dengan pengguna, model, dan waktu. Kill switch dan rollback diuji melalui simulasi.

Ketahanan mencakup fallback, pemulihan, vendor outage, dan kapasitas. Auditor menilai RTO, RPO, backup, model cadangan, dan prosedur manual. Tabletop exercise memberikan bukti kesiapan, tetapi temuan harus ditindaklanjuti. Ketergantungan pada satu vendor atau model dasar perlu dilaporkan.

**Tabel 9.6** Prosedur audit keamanan AI

| Risiko                  | Prosedur                                 | Kontrol yang diharapkan                |
|-------------------------|------------------------------------------|----------------------------------------|
| <b>Prompt injection</b> | Uji skenario langsung dan tidak langsung | Isolasi, tool allowlist, validation    |
| <b>Data leakage</b>     | Coba ekstraksi data pada role berbeda    | Least privilege dan filtering          |
| <b>Excessive agency</b> | Review tools, limit, dan approval        | Batas nilai, dual control, kill switch |
| <b>Supply chain</b>     | Inventaris komponen dan update           | Due diligence, pinning, patching       |

|                        |                                 |                                            |
|------------------------|---------------------------------|--------------------------------------------|
| <b>Model/API abuse</b> | Uji rate dan autentikasi        | Rate limit, monitoring, dan access control |
| <b>Recovery</b>        | Simulasikan outage dan rollback | Fallback, backup, dan runbook teruji       |

### 9.7 AUDIT OPERASI, MONITORING, DAN PERUBAHAN

Auditor menilai apakah indikator relevan, data lengkap, ambang disetujui, dan alarm ditindaklanjuti. Sampel alert ditelusuri dari deteksi hingga penyelesaian. Alert yang ditutup tanpa alasan atau SLA yang berulang kali terlewat menunjukkan kelemahan. Auditor juga mencari risiko yang tidak memiliki indikator.

Drift monitoring diuji dengan membandingkan distribusi dan performa. Auditor menilai siapa memutuskan retraining dan apakah perubahan melalui validasi. Model yang sering retrain otomatis memerlukan guardrail lebih kuat. Perubahan prompt dan knowledge base juga harus masuk change management.

Override manusia dianalisis. Tingkat override, alasan, dan hasil dapat menunjukkan masalah. Auditor dapat membandingkan cabang atau pengguna untuk mendeteksi inkonsistensi. Overreliance dapat terlihat ketika output diterima tanpa review, sedangkan underreliance ketika model diabaikan meski berguna.

**Tabel 9.7** Audit operasi dan monitoring

| <b>Objek</b>     | <b>Prosedur</b>                    | <b>Red flag</b>                        |
|------------------|------------------------------------|----------------------------------------|
| <b>KRI</b>       | Nilai definisi, sumber, dan ambang | Indikator selalu hijau tanpa challenge |
| <b>Alert</b>     | Sampel dari deteksi ke penutupan   | Ditutup tanpa analisis atau SLA lewat  |
| <b>Override</b>  | Analisis tren per user/cabang      | Terlalu rendah/tinggi tanpa alasan     |
| <b>Drift</b>     | Reperform distribusi dan performa  | Retraining otomatis tanpa review       |
| <b>Perubahan</b> | Sampel change dan regression test  | Prompt/model berubah tanpa approval    |
| <b>Keluhan</b>   | Telusuri ke perbaikan sistem       | Keluhan tidak masuk monitoring         |

### 9.8 AUDIT VENDOR DAN KONTRAK

Audit pihak ketiga menilai due diligence, kontrak, SLA, subprosesor, lokasi data, perubahan, insiden, dan exit plan. Auditor memeriksa apakah vendor risk rating sesuai bukti dan apakah kelemahan ditangani. Sertifikasi vendor membantu tetapi tidak menggantikan penilaian konteks penggunaan.

Kontrak diuji terhadap kebutuhan. Apakah vendor boleh menggunakan data untuk pelatihan? Apakah notifikasi insiden tepat waktu? Apakah organisasi memiliki log dan data saat kontrak berakhir? Apakah perubahan model diinformasikan? Apakah hak audit realistis? Klausul tanpa mekanisme pelaksanaan tidak cukup.

Auditor dapat meminta laporan assurance vendor dan menilai ruang lingkup, periode, pengecualian, serta tanggapan manajemen. Shared responsibility perlu jelas. Banyak insiden terjadi karena masing-masing pihak mengira kontrol dilakukan pihak lain.

**Tabel 9.8** Audit vendor AI

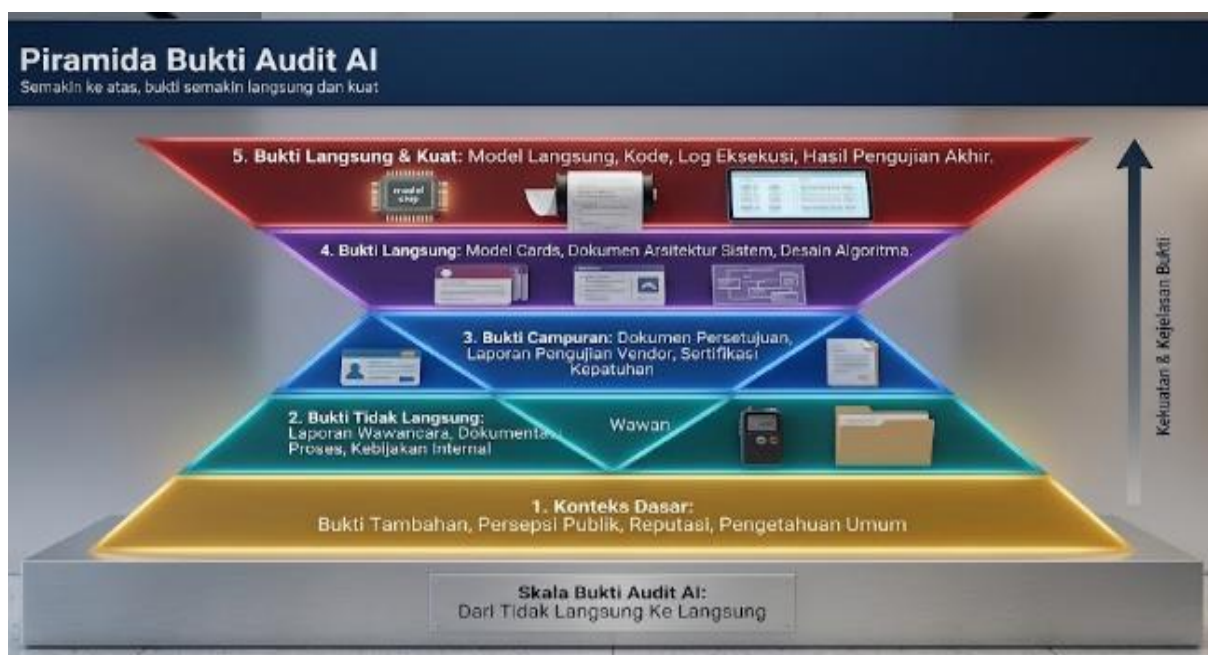
| Area                 | Prosedur                                   | Bukti                              |
|----------------------|--------------------------------------------|------------------------------------|
| <b>Due diligence</b> | Bandinkan rating dengan bukti              | Assessment dan assurance report    |
| <b>Kontrak</b>       | Uji klausul data, insiden, perubahan, exit | Agreement dan DPA                  |
| <b>SLA</b>           | Analisis availability, support, dan breach | Status log dan service review      |
| <b>Subprosesor</b>   | Verifikasi daftar dan lokasi               | Vendor register                    |
| <b>Change notice</b> | Sampel update model/vendor                 | Notification dan regression result |
| <b>Exit</b>          | Simulasikan ekspor/penghapusan             | Exit test dan deletion certificate |

### 9.9 BUKTI AUDIT, SAMPLING, DAN ANALITIK

Bukti audit harus cukup, relevan, dan andal. Reperformance dan observasi langsung umumnya lebih kuat daripada pernyataan. Log sistem, konfigurasi, hasil uji, kontrak, dan approval menjadi bukti penting. Auditor perlu memastikan integritas log dan chain of custody ketika insiden.

Sampling dapat berbasis risiko, statistik, atau judgment. Auditor dapat memilih model kritis, perubahan besar, alert, override, atau keluhan. Analitik memungkinkan pemeriksaan populasi, misalnya seluruh transaksi atau seluruh akses. Namun, script audit juga perlu divalidasi. Kesalahan query dapat menghasilkan kesimpulan salah.

Ketika menggunakan AI dalam audit, auditor harus menerapkan kontrol yang sama: data sensitif, verifikasi output, dokumentasi, dan human review. AI dapat membantu membaca dokumen, menemukan pola, atau membuat ringkasan, tetapi kesimpulan audit tetap tanggung jawab auditor.

**Gambar 9.2** Piramida kekuatan bukti audit AI.

Sumber: diolah untuk diktat ini.

**Tabel 9.9** Hierarki contoh bukti audit

| Kekuatan             | Contoh                                              | Catatan                                    |
|----------------------|-----------------------------------------------------|--------------------------------------------|
| <b>Sangat kuat</b>   | Reperformance, observasi kontrol, dan log immutable | Langsung dan dapat diverifikasi            |
| <b>Kuat</b>          | Konfigurasi, hasil uji, ticket, dan approval        | Perlu memeriksa integritas dan cakupan     |
| <b>Sedang</b>        | Dokumen, model card, dan laporan manajemen          | Perlu dibandingkan dengan praktik          |
| <b>Lemah</b>         | Wawancara dan pernyataan                            | Berguna untuk konteks, bukan bukti tunggal |
| <b>Tidak memadai</b> | Klaim tanpa dukungan                                | Tidak dapat menjadi dasar kesimpulan       |

### Pelaporan Temuan dan Tindak Lanjut

Temuan audit yang baik menjelaskan kondisi, kriteria, sebab, dampak, dan rekomendasi. Pada AI, temuan juga perlu menjelaskan ketidakpastian dan skenario. Bahasa harus dapat dipahami manajemen tanpa menghilangkan substansi teknis. Risiko tidak boleh dilebihkan, tetapi juga tidak boleh disamarkan.

Rating temuan mempertimbangkan dampak, kemungkinan, kecepatan, skala, dan kontrol. Temuan teknis kecil dapat menjadi material jika memengaruhi banyak use case. Root cause harus dicari. Menambah review manual mungkin tidak menyelesaikan kualitas data atau insentif yang salah.

Action plan memiliki pemilik, tenggat, deliverable, dan kriteria penutupan. Audit memverifikasi bukti, bukan hanya menerima status. Risiko yang diterima perlu mendapat persetujuan sesuai kewenangan. Temuan berulang dilaporkan sebagai isu sistemik.

**Tabel 9.10** Struktur temuan audit AI

| Unsur              | Isi contoh                                                               |
|--------------------|--------------------------------------------------------------------------|
| <b>Kondisi</b>     | Model kredit memiliki false rejection lebih tinggi pada segmen tertentu  |
| <b>Kriteria</b>    | Kebijakan fairness mewajibkan pengujian per segmen dan banding efektif   |
| <b>Sebab</b>       | Fitur proksi tidak direview dan data pelanggan baru kurang representatif |
| <b>Dampak</b>      | Akses layanan tidak adil, keluhan, dan risiko reputasi/hukum             |
| <b>Rekomendasi</b> | Review fitur, data tambahan, kalibrasi, banding, dan monitoring          |
| <b>Action plan</b> | Owner, tanggal, shadow test, dan bukti penutupan                         |

### Kematangan dan Peningkatan Berkelanjutan

Model kematangan membantu organisasi memahami posisi dan prioritas. Tingkat ad hoc ditandai eksperimen tersebar dan respons reaktif. Tingkat berulang memiliki kontrol lokal. Tingkat terdefinisi memiliki kebijakan, inventaris, dan peran. Tingkat terukur memiliki KRI, validasi, dan audit. Tingkat adaptif menggunakan pembelajaran dan perubahan lingkungan untuk memperbaiki sistem.

Penilaian kematangan tidak boleh menjadi lomba mencapai tingkat tertinggi. Tidak semua area memerlukan level lima. Tujuan adalah kecocokan dengan risiko dan strategi. Skor

harus didukung bukti. Organisasi dapat memiliki kematangan tinggi pada keamanan tetapi rendah pada fairness. Roadmap diarahkan pada kesenjangan material.

Management review menilai kinerja sistem manajemen, perubahan konteks, insiden, audit, sumber daya, dan peluang perbaikan. Lessons learned dari insiden dan near miss diintegrasikan ke kebijakan, pelatihan, dan desain. Benchmark eksternal dapat digunakan, tetapi tidak menggantikan konteks.



**Gambar 9.3** Model kematangan tata kelola AI lima tingkat.

Sumber: diolah untuk diktat ini.

**Tabel 9.11** Penilaian kematangan tata kelola AI

| Level                | Karakteristik                                            | Prioritas perbaikan                       |
|----------------------|----------------------------------------------------------|-------------------------------------------|
| <b>1 Ad hoc</b>      | Eksperimen tersebar, owner tidak jelas, respons reaktif  | Inventaris, owner, dan larangan minimum   |
| <b>2 Berulang</b>    | Kontrol lokal, template berbeda, ketergantungan individu | Kebijakan dan klasifikasi konsisten       |
| <b>3 Terdefinisi</b> | Stage-gate, peran, dokumentasi, dan pelatihan            | Integrasi dan kualitas pelaksanaan        |
| <b>4 Terukur</b>     | KRI, validasi, audit, dan dashboard                      | Analitik akar masalah dan assurance map   |
| <b>5 Adaptif</b>     | Pembelajaran insiden, automation control, dan benchmark  | Antisipasi emerging risk dan inovasi aman |

### Crosswalk Audit terhadap Kerangka Utama

*Crosswalk* membantu auditor menghubungkan kriteria. Tata kelola ISO/IEC 42001 dapat dipetakan ke Govern NIST AI RMF. Konteks dan penilaian dampak terkait Map. Pengujian dan metrik terkait *Measure*. Kontrol, respons, dan monitoring terkait Manage. ISO/IEC 23894 memberi panduan untuk integrasi risiko.

*Crosswalk* tidak berarti standar identik. Auditor perlu memahami tujuan dan ruang lingkup. Satu bukti dapat mendukung beberapa kriteria, tetapi kesimpulan tetap spesifik.

*Crosswalk* mengurangi duplikasi dan membantu manajemen melihat bagaimana program memenuhi berbagai ekspektasi.

| Crosswalk Kerangka Tata Kelola dan Audit AI  |                              |               |                    |                    |
|----------------------------------------------|------------------------------|---------------|--------------------|--------------------|
| Satu kontrol dapat memenuhi beberapa rujukan |                              |               |                    |                    |
| Area                                         | ISO 42001                    | NIST AI RMF   | ISO 23894          | Audit              |
| Tata kelola                                  | AIMS & kebijakan             | Govern        | Integrasi risiko   | Desain & oversight |
| Konteks                                      | Kebutuhan organisasi         | Map           | Konteks & kriteria | Scoping            |
| Pengukuran                                   | Evaluasi kinerja             | Measure       | Analisis risiko    | Testing            |
| Perlakuan                                    | Perencanaan & operasi        | Manage        | Treatment          | Remediasi          |
| Perbaikan                                    | Internal audit & improvement | Govern/Manage | Monitoring         | Follow-up          |

**Gambar 9.4** Crosswalk kerangka tata kelola dan audit AI.

Sumber: diolah untuk diktat ini.

**Tabel 9.12** Crosswalk kerangka utama

| Area                       | ISO/IEC 42001                       | NIST AI RMF   | ISO/IEC 23894            | Bukti audit                  |
|----------------------------|-------------------------------------|---------------|--------------------------|------------------------------|
| <b>Governance</b>          | Leadership, policy, roles           | Govern        | Integrasi ke organisasi  | Charter, RACI, minutes       |
| <b>Context/impact</b>      | Context and planning                | Map           | Scope, context, criteria | AIIA dan stakeholder map     |
| <b>Measurement</b>         | Performance evaluation              | Measure       | Risk analysis/evaluation | Validation dan KRI           |
| <b>Treatment/operation</b> | Planning and operation              | Manage        | Risk treatment           | Controls, runbook, incident  |
| <b>Improvement</b>         | Internal audit, review, improvement | Govern/Manage | Monitoring and review    | Audit, CAPA, lessons learned |

### Studi Kasus Audit: Model Kredit Pelanggan PT Niaga Nusantara

Audit internal memilih model kredit karena menentukan limit bayar kemudian. Tujuan audit adalah menilai tata kelola, data, kinerja, fairness, explainability, dan monitoring. Auditor menelusuri approval, dataset, model card, validasi, dan keluhan. Ditemukan bahwa model akurat secara rata-rata tetapi false rejection lebih tinggi pada pelanggan baru dari wilayah tertentu.

Analisis menunjukkan variabel alamat dan jenis perangkat menjadi proksi yang kuat. Tim model tidak mendokumentasikan alasan. Mekanisme banding ada, tetapi pelanggan sulit mengakses. Auditor melakukan reperformance dan mengonfirmasi perbedaan. Temuan dinilai tinggi karena memengaruhi akses layanan dan reputasi.

Manajemen menghapus variabel, menambah data, mengkalibrasi ambang, dan memperbaiki banding. Rilis dilakukan melalui shadow mode. Monitoring fairness ditambahkan. Audit menutup temuan setelah memverifikasi hasil dan proses. Kasus menunjukkan bahwa audit menggabungkan bukti teknis dan pengalaman pengguna.

**Tabel 9.13** Ringkasan temuan audit model kredit

| Area       | Temuan                              | Tindakan                            |
|------------|-------------------------------------|-------------------------------------|
| Data       | Pelanggan baru kurang terwakili     | Tambah data dan batasi generalisasi |
| Fitur      | Alamat dan perangkat menjadi proksi | Hapus/review dan uji sensitivitas   |
| Fairness   | False rejection berbeda material    | Kalibrasi dan threshold review      |
| Banding    | Sulit ditemukan pelanggan           | Perbaiki UX, SLA, dan human review  |
| Monitoring | Hanya metrik rata-rata              | Tambahkan per segmen dan keluhan    |
| Rilis      | Perubahan langsung produksi         | Gunakan shadow mode dan approval    |

#### Proyek Akhir: Program Audit AI

Peserta menyusun program audit untuk satu use case. Dokumen mencakup tujuan, ruang lingkup, kriteria, risiko, prosedur, sampel, data, keahlian, dan format temuan. Peserta melakukan simulasi walkthrough dan membuat minimal tiga kertas kerja: tata kelola, data/model, dan operasi/keamanan.

Hasil akhir berupa laporan audit ringkas kepada direksi dan lampiran teknis. Penilaian memperhatikan relevansi prosedur, kualitas bukti, logika temuan, materialitas, rekomendasi, dan komunikasi. Peserta harus membedakan fakta, interpretasi, dan keterbatasan.

**Tabel 9.14** Rubrik proyek audit AI

| Kriteria                    | Bobot | Kinerja unggul                                           |
|-----------------------------|-------|----------------------------------------------------------|
| Scoping dan risk assessment | 15%   | Objek, dampak, kriteria, dan prioritas jelas             |
| Program audit               | 20%   | Prosedur terkait risiko dan dapat dilaksanakan           |
| Bukti dan analitik          | 20%   | Bukti cukup, integritas dinilai, dan reperformance tepat |
| Temuan                      | 20%   | Kondisi-kriteria-sebab-dampak kuat dan material          |
| Rekomendasi                 | 15%   | Proporsional, mengatasi akar, dan dapat ditindaklanjuti  |
| Komunikasi dan etika        | 10%   | Ringkas, objektif, independen, dan menjaga kerahasiaan   |

#### KESIMPULAN

Audit AI memberikan assurance bahwa tata kelola dan kontrol bekerja. Proses mencakup universe, perencanaan, pemahaman sistem, pengujian tata kelola, data, model, keamanan, operasi, vendor, bukti, pelaporan, dan tindak lanjut. Audit harus berbasis risiko dan multidisiplin.

Peningkatan berkelanjutan terjadi ketika temuan, insiden, dan perubahan menjadi pembelajaran. Kematangan bukan jumlah dokumen, tetapi kemampuan organisasi mengambil keputusan yang dapat dipertanggungjawabkan dan memperbaiki diri.

### **LATIHAN SOAL**

1. Susun audit universe AI perusahaan dagang.
2. Jelaskan perbedaan validasi model dan audit internal.
3. Buat lima prosedur audit untuk data pelatihan.
4. Rancang pengujian prompt injection yang aman.
5. Jelaskan cara menilai efektivitas human oversight.
6. Buat contoh temuan dengan unsur kondisi, kriteria, sebab, dampak, dan rekomendasi.
7. Susun assurance map untuk model harga dinamis.
8. Jelaskan risiko auditor menggunakan generative AI.

### **PILIHAN GANDA**

1. Audit AI bertujuan utama ...
  - A. memberi assurance independen
  - B. membangun model
  - C. menggantikan manajemen
  - D. menjual vendor
2. Bukti paling kuat adalah ...
  - A. reperformance dan observasi
  - B. pernyataan tanpa bukti
  - C. poster
  - D. asumsi
3. Audit universe adalah ...
  - A. daftar objek yang dapat diaudit
  - B. daftar pelanggan
  - C. kode sumber
  - D. struktur gaji
4. Reproducibility berarti ...
  - A. hasil dapat dijalankan ulang dengan versi/data yang sama
  - B. model selalu benar
  - C. tidak ada perubahan
  - D. dokumen rahasia
5. Temuan audit yang baik memuat ...
  - A. kondisi, kriteria, sebab, dampak, rekomendasi
  - B. warna dan logo
  - C. hanya opini
  - D. hanya angka

6. Assurance map membantu ...
  - A. mengkoordinasikan sumber assurance
  - B. mengganti auditor
  - C. menghapus risiko
  - D. menambah vendor
7. Audit penggunaan AI oleh auditor juga memerlukan ...
  - A. verifikasi, privasi, dan human review
  - B. tanpa kontrol
  - C. data publik saja selalu
  - D. tidak ada dokumentasi
8. Kematangan level ad hoc ditandai ...
  - A. kontrol reaktif dan tidak konsisten
  - B. dashboard terukur
  - C. audit terintegrasi
  - D. perbaikan adaptif
9. Sampling berbasis risiko memilih ...
  - A. objek dengan dampak dan paparan tinggi
  - B. hanya objek mudah
  - C. secara acak tanpa tujuan selalu
  - D. tidak ada sampel
10. Tindak lanjut audit ditutup setelah ...
  - A. bukti perbaikan diverifikasi
  - B. owner mengirim email
  - C. tanggal lewat
  - D. temuan dihapus

## GLOSARIUM

| Istilah                            | Definisi                                                                                                                   |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>AI Impact Assessment (AIIA)</b> | Penilaian terstruktur atas tujuan, pihak terdampak, data, manfaat, risiko, kontrol, dan residual risk suatu sistem AI.     |
| <b>AI inventory</b>                | Daftar terpusat seluruh sistem, model, alat, dan use case AI beserta pemilik, status, data, dan risikonya.                 |
| <b>AI management system</b>        | Sistem kebijakan, proses, peran, sumber daya, evaluasi, dan perbaikan untuk mengelola AI secara konsisten.                 |
| <b>Algorithmic bias</b>            | Pola keluaran yang secara sistematis menghasilkan kerugian atau perlakuan tidak adil akibat data, desain, atau penggunaan. |
| <b>Alert fatigue</b>               | Kondisi ketika terlalu banyak peringatan membuat pengguna mengabaikan atau menyetujui alert tanpa analisis.                |
| <b>Anomaly detection</b>           | Teknik untuk mengenali pola yang berbeda secara signifikan dari perilaku normal.                                           |
| <b>Audit universe</b>              | Kumpulan objek yang berpotensi diaudit dan menjadi dasar perencanaan audit berbasis risiko.                                |
| <b>Augmented intelligence</b>      | Pemanfaatan AI untuk memperkuat kemampuan manusia, bukan menggantikan penilaian dan tanggung jawab.                        |
| <b>Calibration</b>                 | Kesesuaian antara probabilitas yang diprediksi model dan frekuensi hasil yang benar-benar terjadi.                         |
| <b>Canary release</b>              | Peluncuran sistem kepada sebagian kecil pengguna untuk membatasi dampak dan mengamati masalah.                             |
| <b>Concept drift</b>               | Perubahan hubungan antara input dan target sehingga pola yang dipelajari model tidak lagi berlaku.                         |
| <b>Data drift</b>                  | Perubahan distribusi data input dibandingkan data pelatihan atau baseline.                                                 |
| <b>Data lineage</b>                | Rekaman aliran data dari sumber, transformasi, fitur, model, hingga output.                                                |
| <b>Data minimization</b>           | Prinsip menggunakan data yang relevan dan sesedikit mungkin untuk tujuan yang sah.                                         |
| <b>Dataset sheet</b>               | Dokumen yang menjelaskan asal, tujuan, komposisi, pengumpulan, transformasi, batas, dan risiko dataset.                    |
| <b>Deepfake</b>                    | Konten sintetis atau dimanipulasi yang meniru orang, suara, gambar, atau peristiwa secara meyakinkan.                      |
| <b>Differential privacy</b>        | Teknik matematis untuk membatasi informasi tentang individu yang dapat disimpulkan dari hasil analisis.                    |
| <b>Explainability</b>              | Kemampuan menyediakan alasan atau representasi yang membantu memahami keluaran model.                                      |
| <b>Excessive agency</b>            | Risiko ketika agen AI memiliki kewenangan, alat, atau otonomi yang terlalu luas.                                           |
| <b>Fairness</b>                    | Upaya mengelola perlakuan dan dampak agar perbedaan yang merugikan tidak terjadi tanpa alasan yang sah.                    |

|                                   |                                                                                                                    |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>False negative</b>             | Kasus berisiko yang salah dinilai sebagai normal atau aman.                                                        |
| <b>False positive</b>             | Kasus normal yang salah ditandai sebagai berisiko.                                                                 |
| <b>Feature</b>                    | Variabel input yang digunakan model untuk menghasilkan prediksi atau keputusan.                                    |
| <b>Feature flag</b>               | Mekanisme untuk mengaktifkan atau menonaktifkan fitur tanpa perubahan besar pada aplikasi.                         |
| <b>Generative AI</b>              | AI yang menghasilkan konten baru seperti teks, gambar, audio, video, atau kode.                                    |
| <b>Guardrail</b>                  | Batas teknis atau aturan yang menjaga sistem tetap pada penggunaan dan output yang diizinkan.                      |
| <b>Hallucination</b>              | Output AI yang terdengar meyakinkan tetapi tidak benar, tidak didukung sumber, atau direka.                        |
| <b>Human-in-the-loop</b>          | Pengaturan ketika manusia harus menyetujui sebelum keputusan atau tindakan kritis dijalankan.                      |
| <b>Human-on-the-loop</b>          | Pengaturan ketika sistem bertindak dan manusia memantau serta dapat menghentikan.                                  |
| <b>Human oversight</b>            | Pengawasan manusia yang memiliki informasi, kompetensi, waktu, dan kewenangan untuk mengintervensi.                |
| <b>Inference</b>                  | Proses model menggunakan input untuk menghasilkan prediksi, skor, rekomendasi, atau konten.                        |
| <b>Interpretability</b>           | Derajat kemudahan memahami hubungan internal antara input, proses, dan output model.                               |
| <b>Key risk indicator (KRI)</b>   | Indikator yang memberi peringatan mengenai peningkatan paparan atau kemungkinan risiko.                            |
| <b>Kill switch</b>                | Mekanisme untuk menghentikan fungsi AI secara cepat ketika risiko tidak terkendali.                                |
| <b>Knowledge base</b>             | Kumpulan sumber informasi yang digunakan sistem untuk pencarian atau grounding.                                    |
| <b>Large language model (LLM)</b> | Model bahasa berskala besar yang dilatih pada data teks untuk memahami dan menghasilkan bahasa.                    |
| <b>Least privilege</b>            | Prinsip memberi akses dan kewenangan minimum yang diperlukan.                                                      |
| <b>Material change</b>            | Perubahan yang cukup signifikan sehingga memerlukan penilaian, pengujian, atau persetujuan ulang.                  |
| <b>Model card</b>                 | Dokumen ringkas mengenai tujuan, data, metrik, batasan, penggunaan, risiko, dan pemilik model.                     |
| <b>Model drift</b>                | Penurunan atau perubahan perilaku model dari waktu ke waktu.                                                       |
| <b>Model risk</b>                 | Risiko kerugian atau keputusan buruk akibat kesalahan, keterbatasan, atau penyalahgunaan model.                    |
| <b>MLOps</b>                      | Praktik mengelola pembangunan, rilis, monitoring, dan perubahan model machine learning secara terkontrol.          |
| <b>Near miss</b>                  | Kejadian yang hampir menimbulkan dampak tetapi tertahan atau tidak terjadi, dan tetap bernilai untuk pembelajaran. |
| <b>Out-of-distribution</b>        | Data yang berbeda secara material dari pola data yang digunakan untuk melatih atau menguji model.                  |

|                                             |                                                                                                           |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| <b>Overreliance</b>                         | Ketergantungan berlebihan pada output AI tanpa verifikasi atau penilaian kritis.                          |
| <b>Precision</b>                            | Proporsi prediksi positif yang benar di antara seluruh prediksi positif.                                  |
| <b>Privacy by design</b>                    | Pendekatan yang memasukkan perlindungan data sejak tahap awal desain.                                     |
| <b>Prompt injection</b>                     | Upaya memanipulasi model melalui instruksi yang mengubah atau melemahkan aturan sistem.                   |
| <b>Pseudonymization</b>                     | Pengolahan data agar identitas tidak dapat dikaitkan tanpa informasi tambahan yang disimpan terpisah.     |
| <b>Recall</b>                               | Proporsi kasus positif yang berhasil ditemukan oleh model.                                                |
| <b>Red teaming</b>                          | Pengujian adversarial terstruktur untuk mencari cara sistem dapat gagal atau disalahgunakan.              |
| <b>Regression testing</b>                   | Pengujian untuk memastikan perubahan tidak merusak fungsi atau kontrol yang sebelumnya berjalan.          |
| <b>Residual risk</b>                        | Risiko yang tersisa setelah kontrol diperhitungkan.                                                       |
| <b>Retrieval-augmented generation (RAG)</b> | Teknik menggabungkan model generatif dengan pencarian sumber untuk memberi konteks yang lebih terkontrol. |
| <b>Risk appetite</b>                        | Jumlah dan jenis risiko yang bersedia diambil organisasi untuk mencapai tujuan.                           |
| <b>Risk tolerance</b>                       | Batas operasional yang lebih spesifik terhadap penyimpangan atau paparan risiko.                          |
| <b>Risk velocity</b>                        | Kecepatan dampak muncul dan menyebar setelah peristiwa risiko.                                            |
| <b>Rollback</b>                             | Pengembalian sistem ke versi atau kondisi sebelumnya yang stabil.                                         |
| <b>Shadow AI</b>                            | Penggunaan alat AI tanpa persetujuan, inventarisasi, atau pengawasan organisasi.                          |
| <b>Shadow mode</b>                          | Pengoperasian model tanpa memengaruhi keputusan nyata untuk membandingkan kinerja.                        |
| <b>Stage-gate</b>                           | Pendekatan siklus hidup dengan tahap dan titik keputusan berdasarkan bukti.                               |
| <b>Stress testing</b>                       | Pengujian sistem pada kondisi ekstrem, perubahan, atau skenario yang merugikan.                           |
| <b>Synthetic data</b>                       | Data buatan yang meniru karakteristik data nyata untuk tujuan pengujian atau pelatihan.                   |
| <b>System card</b>                          | Dokumentasi sistem AI secara menyeluruh, termasuk konfigurasi, komponen, batas, dan hasil uji.            |
| <b>Threat model</b>                         | Analisis aset, pelaku ancaman, jalur serangan, dampak, dan kontrol.                                       |
| <b>Three Lines Model</b>                    | Model pembagian peran antara pemilik/operasi, fungsi risiko/kepatuhan, dan audit internal.                |
| <b>Tool calling</b>                         | Kemampuan model atau agen memanggil aplikasi, API, database, atau fungsi eksternal.                       |
| <b>Training data poisoning</b>              | Manipulasi data pelatihan untuk mengubah perilaku model.                                                  |

|                        |                                                                                         |
|------------------------|-----------------------------------------------------------------------------------------|
| <b>Validation</b>      | Penilaian independen atas kesesuaian tujuan, data, metodologi, hasil, dan implementasi. |
| <b>Version control</b> | Mekanisme pencatatan dan pengelolaan perubahan kode, model, data, prompt, atau dokumen. |
| <b>Whistleblowing</b>  | Saluran aman untuk melaporkan pelanggaran, risiko, atau perilaku tidak etis.            |

## LAMPIRAN A. FORMULIR USULAN USE CASE AI

|                                     |  |
|-------------------------------------|--|
| Nama use case                       |  |
| Sponsor/pemilik bisnis              |  |
| Masalah dan sasaran                 |  |
| Mengapa AI diperlukan               |  |
| Alternatif non-AI                   |  |
| Pengguna dan pihak terdampak        |  |
| Keputusan/tindakan yang dipengaruhi |  |
| Data dan sumber                     |  |
| Model/vendor/platform               |  |
| Tingkat otonomi                     |  |
| Manfaat dan KPI                     |  |
| Risiko awal                         |  |
| Klasifikasi awal                    |  |
| Rencana pilot                       |  |
| Persetujuan                         |  |

## LAMPIRAN B.

### TEMPLATE AI RISK REGISTER

Misalnya AI digunakan untuk **membantu penyusunan laporan perpajakan**:

| ID    | Use case/proses                         | Risiko                                                 | Penyebab                                                                    | Dampak                                       | Inheren | Kontrol                                                                       | Residual | Owner                         | Tindakan/tenggat                                      |
|-------|-----------------------------------------|--------------------------------------------------------|-----------------------------------------------------------------------------|----------------------------------------------|---------|-------------------------------------------------------------------------------|----------|-------------------------------|-------------------------------------------------------|
| AI-01 | Penyusunan laporan perpajakan dengan AI | AI menghasilkan informasi/perhitungan pajak yang salah | Data tidak lengkap, prompt kurang tepat, atau informasi pajak tidak terbaru | Kesalahan pelaporan dan potensi sanksi pajak | 20      | Verifikasi output AI oleh staf pajak dan pengecekan terhadap regulasi terbaru | 10       | Tax Manager                   | Membuat SOP verifikasi output AI; 30 September 2026   |
| AI-02 | Analisis data keuangan menggunakan AI   | Data rahasia perusahaan terekspos                      | Pengguna memasukkan data sensitif ke platform AI publik                     | Kebocoran data dan risiko reputasi           | 20      | Pembatasan jenis data yang boleh dimasukkan dan kebijakan keamanan data       | 8        | IT Manager                    | Menetapkan kebijakan penggunaan AI; 30 September 2026 |
| AI-03 | Pembuatan materi pembelajaran dengan AI | Materi mengandung informasi yang tidak akurat          | AI menghasilkan informasi yang keliru atau sumber tidak valid               | Mahasiswa menerima informasi yang salah      | 12      | Dosen melakukan review dan memeriksa sumber akademik                          | 6        | Dosen/Koordinator Mata Kuliah | Review materi sebelum digunakan; setiap semester      |

## LAMPIRAN C.

### TEMPLATE AI IMPACT ASSESSMENT

#### 1. Tujuan dan Kebutuhan

|                            |  |
|----------------------------|--|
| Tujuan sistem              |  |
| Keputusan yang dipengaruhi |  |
| Alternatif tanpa AI        |  |
| Manfaat yang diharapkan    |  |
| Kriteria keberhasilan      |  |

#### 2. Pihak Terdampak

|                              |  |
|------------------------------|--|
| Kelompok pengguna            |  |
| Kelompok rentan              |  |
| Manfaat per kelompok         |  |
| Kerugian potensial           |  |
| Mekanisme konsultasi/banding |  |

#### 3. Data

|                                |  |
|--------------------------------|--|
| Sumber dan legalitas           |  |
| Kategori data pribadi          |  |
| Kualitas dan representativitas |  |
| Lineage                        |  |
| Retensi dan penghapusan        |  |

#### 4. Model dan Keputusan

|                     |  |
|---------------------|--|
| Jenis model/vendor  |  |
| Metrik dan baseline |  |
| Tingkat otonomi     |  |
| Explainability      |  |
| Batas penggunaan    |  |

#### 5. Risiko dan Kontrol

|                      |  |
|----------------------|--|
| Skenario risiko      |  |
| Kontrol preventif    |  |
| Kontrol detektif     |  |
| Fallback dan insiden |  |
| Residual risk        |  |

## 6. Persetujuan dan Review

|                           |  |
|---------------------------|--|
| Pemilik risiko            |  |
| Validator                 |  |
| Komite/otoritas           |  |
| Syarat persetujuan        |  |
| Tanggal review berikutnya |  |

## LAMPIRAN D. DATASET SHEET

|                                                 |  |
|-------------------------------------------------|--|
| Nama dan versi dataset                          |  |
| Tujuan penggunaan                               |  |
| Pemilik                                         |  |
| Sumber dan metode pengumpulan                   |  |
| Periode dan populasi                            |  |
| Variabel utama                                  |  |
| Data pribadi/sensitif                           |  |
| Transformasi dan cleaning                       |  |
| Kualitas dan ambang                             |  |
| Representativitas dan kelompok kurang terwakili |  |
| Lisensi/kontrak                                 |  |
| Retensi dan penghapusan                         |  |
| Keterbatasan                                    |  |
| Perubahan terakhir                              |  |

## LAMPIRAN E.

### MODEL CARD / SYSTEM CARD

|                                |  |
|--------------------------------|--|
| Nama, ID, versi, dan status    |  |
| Tujuan dan pengguna            |  |
| Model dasar/algoritma          |  |
| Data pelatihan/knowledge base  |  |
| Metrik dan hasil per segmen    |  |
| Baseline                       |  |
| Fairness dan explainability    |  |
| Security/red-team test         |  |
| Batas dan penggunaan terlarang |  |
| Human oversight                |  |
| Monitoring dan KRI             |  |
| Fallback dan rollback          |  |
| Vendor/komponen                |  |
| Approval dan tanggal review    |  |

## LAMPIRAN F.

### CHECKLIST DUE DILIGENCE VENDOR AI

| Pertanyaan                                      | Ya                       | Tidak                    | Catatan/Bukti |
|-------------------------------------------------|--------------------------|--------------------------|---------------|
| Profil dan stabilitas vendor                    | <input type="checkbox"/> | <input type="checkbox"/> |               |
| Arsitektur dan lokasi layanan                   | <input type="checkbox"/> | <input type="checkbox"/> |               |
| Penggunaan ulang data untuk training            | <input type="checkbox"/> | <input type="checkbox"/> |               |
| Daftar subprosesor                              | <input type="checkbox"/> | <input type="checkbox"/> |               |
| Enkripsi dan kontrol akses                      | <input type="checkbox"/> | <input type="checkbox"/> |               |
| Secure development dan vulnerability management | <input type="checkbox"/> | <input type="checkbox"/> |               |
| Hasil pen-test/assurance                        | <input type="checkbox"/> | <input type="checkbox"/> |               |
| Dokumentasi model dan keterbatasan              | <input type="checkbox"/> | <input type="checkbox"/> |               |
| Fairness dan safety testing                     | <input type="checkbox"/> | <input type="checkbox"/> |               |
| SLA dan support                                 | <input type="checkbox"/> | <input type="checkbox"/> |               |
| Notifikasi insiden                              | <input type="checkbox"/> | <input type="checkbox"/> |               |
| Notifikasi perubahan model                      | <input type="checkbox"/> | <input type="checkbox"/> |               |
| Hak audit                                       | <input type="checkbox"/> | <input type="checkbox"/> |               |
| Kepemilikan output/IP                           | <input type="checkbox"/> | <input type="checkbox"/> |               |
| Exit, portabilitas, dan penghapusan data        | <input type="checkbox"/> | <input type="checkbox"/> |               |

## LAMPIRAN G. FORMULIR INSIDEN AI

|                                       |  |
|---------------------------------------|--|
| ID insiden                            |  |
| Tanggal/waktu deteksi                 |  |
| Pelapor dan kontak                    |  |
| Sistem/use case/versi                 |  |
| Deskripsi dan bukti awal              |  |
| Kategori dan severity                 |  |
| Pihak/data terdampak                  |  |
| Tindakan kontainmen                   |  |
| Keputusan kill switch/rollback        |  |
| Kewajiban notifikasi                  |  |
| Root cause                            |  |
| Pemulihan dan validasi                |  |
| Komunikasi                            |  |
| Action plan dan owner                 |  |
| Tanggal penutupan dan lessons learned |  |

## LAMPIRAN H.

### PROGRAM AUDIT AI DAN FORMULIR TEMUAN

#### 1. Program Audit

| Risiko/tujuan kontrol | Prosedur | Populasi/sampel | Bukti | Hasil/referensi kertas kerja |
|-----------------------|----------|-----------------|-------|------------------------------|
|                       |          |                 |       |                              |
|                       |          |                 |       |                              |
|                       |          |                 |       |                              |
|                       |          |                 |       |                              |
|                       |          |                 |       |                              |
|                       |          |                 |       |                              |
|                       |          |                 |       |                              |
|                       |          |                 |       |                              |

#### 2. Formulir Temuan

|               |  |
|---------------|--|
| Judul temuan  |  |
| Kondisi       |  |
| Kriteria      |  |
| Sebab         |  |
| Dampak/risiko |  |
| Rating        |  |
| Rekomendasi   |  |

|                             |  |
|-----------------------------|--|
| Tanggapan manajemen         |  |
| Action plan, owner, tenggat |  |
| Bukti penutupan             |  |

## LATIHAN SOAL AKHIR BUKU

Paket praktikum ini dirancang agar mahasiswa tidak berhenti pada pemahaman konsep. Setiap lembar kerja mengarahkan mahasiswa untuk mengubah konsep manajemen risiko dan tata kelola AI menjadi bukti kerja yang dapat diperiksa: peta proses, risk register, penilaian dampak, rancangan kontrol, dashboard, respons insiden, dan program audit. Praktikum dapat dikerjakan secara individual atau berkelompok dengan menggunakan data simulasi maupun data organisasi yang telah dianonimkan.

### 1. Pemetaan Proses Pembelian dan Titik Risiko

#### TUJUAN PRAKTIKUM

Mengidentifikasi tujuan, aktivitas, data, keputusan, kontrol, dan titik kegagalan pada proses pembelian.

#### Skenario

PT Sinar Niaga membeli lebih dari 1.200 jenis barang dari 85 pemasok. Pesanan dibuat oleh bagian pembelian, penerimaan dilakukan di gudang, sedangkan pembayaran diproses oleh keuangan. Selama tiga bulan terakhir terjadi keterlambatan pengiriman, perbedaan kuantitas, perubahan harga setelah pesanan disetujui, dan faktur ganda. Manajemen ingin menggunakan analitik untuk memprioritaskan transaksi yang perlu diperiksa tanpa menghilangkan tanggung jawab pemilik proses.

#### Instruksi Kerja

1. Gambarkan alur proses dari permintaan pembelian sampai pembayaran.
2. Tuliskan tujuan kontrol pada setiap tahap.
3. Identifikasi sekurang-kurangnya delapan risiko dan penyebabnya.
4. Tentukan data yang dapat menjadi sinyal risiko.
5. Usulkan kontrol preventif, detektif, dan korektif.

#### Lembar Kerja

| Komponen                 | Analisis/Jawaban |
|--------------------------|------------------|
| Tahap proses dan pemilik | .....<br>.....   |
| Tujuan proses/kontrol    | .....<br>.....   |
| Peristiwa risiko         | .....<br>.....   |

| Komponen                    | Analisis/Jawaban |
|-----------------------------|------------------|
| Penyebab dan dampak         | .....<br>.....   |
| Data/sinyal yang diperlukan | .....<br>.....   |
| Kontrol yang diusulkan      | .....<br>.....   |
| Bukti pengujian             | .....<br>.....   |
| Kesimpulan kelompok         | .....<br>.....   |

*Bukti yang dikumpulkan: peta proses, data pendukung, asumsi, perhitungan, keputusan, serta daftar tindak lanjut yang dapat diverifikasi.*

## 2. Penyusunan AI Risk Register Persediaan

### TUJUAN PRAKTIKUM

Menyusun risk register untuk sistem peramalan permintaan dan replenishment persediaan.

### Skenario

CV Pangan Sejahtera menggunakan model peramalan untuk menentukan jumlah pemesanan produk cepat rusak. Model memanfaatkan penjualan historis, promosi, hari libur, cuaca, dan data ketersediaan pemasok. Pada musim tertentu model menghasilkan kelebihan stok, sedangkan pada cabang lain terjadi kekosongan. Tim bisnis menyalahkan model, sedangkan tim data menilai pengguna sering mengubah rekomendasi tanpa dokumentasi.

### Instruksi Kerja

1. Tentukan sasaran bisnis dan batas toleransi risikonya.
2. Susun sekurang-kurangnya sepuluh risiko yang mencakup data, model, manusia, proses, vendor, dan keamanan.
3. Nilai likelihood, impact, velocity, dan detectability.
4. Dokumentasikan kontrol yang ada dan residual risk.
5. Pilih lima prioritas serta pemilik action plan.

## Lembar Kerja

| Komponen                          | Analisis/Jawaban |
|-----------------------------------|------------------|
| ID dan kategori risiko            | .....<br>.....   |
| Pernyataan sebab-peristiwa-dampak | .....<br>.....   |
| Kontrol yang ada                  | .....<br>.....   |
| Likelihood/impact                 | .....<br>.....   |
| Velocity/detectability            | .....<br>.....   |
| Residual risk                     | .....<br>.....   |
| Pemilik dan tenggat               | .....<br>.....   |
| Indikator keberhasilan            | .....<br>.....   |

*Bukti yang dikumpulkan: peta proses, data pendukung, asumsi, perhitungan, keputusan, serta daftar tindak lanjut yang dapat diverifikasi.*

## 3. Audit Kualitas Data untuk Model AI

### TUJUAN PRAKTIKUM

Menilai kelengkapan, akurasi, konsistensi, ketepatan waktu, validitas, dan representativitas data.

### Skenario

Sebuah distributor elektronik hendak membangun model prediksi retur. Data berasal dari kasir, marketplace, gudang, layanan pelanggan, dan penyedia logistik. Nomor produk

tidak selalu sama antar-sistem, alasan retur banyak yang kosong, dan sebagian transaksi marketplace terlambat masuk ke data warehouse. Manajemen meminta bukti bahwa dataset cukup layak sebelum pelatihan model dimulai.

### Instruksi Kerja

1. Buat daftar elemen data kritis dan definisinya.
2. Tetapkan aturan validasi serta ambang penerimaan.
3. Rancang sampel dan prosedur rekonsiliasi sumber-ke-target.
4. Analisis bias representasi kanal, wilayah, dan kelompok produk.
5. Susun keputusan go, conditional go, atau no-go beserta alasannya.

### Lembar Kerja

| Komponen              | Analisis/Jawaban |
|-----------------------|------------------|
| Elemen data kritis    | .....<br>.....   |
| Sumber dan pemilik    | .....<br>.....   |
| Aturan kualitas       | .....<br>.....   |
| Metode pengujian      | .....<br>.....   |
| Hasil/pengecualian    | .....<br>.....   |
| Dampak terhadap model | .....<br>.....   |
| Tindakan perbaikan    | .....<br>.....   |
| Keputusan kelayakan   | .....<br>.....   |

*Bukti yang dikumpulkan: peta proses, data pendukung, asumsi, perhitungan, keputusan, serta daftar tindak lanjut yang dapat diverifikasi.*

#### 4. Deteksi Anomali Transaksi Penjualan

##### TUJUAN PRAKTIKUM

Merancang skenario deteksi anomali yang dapat ditindaklanjuti dan tidak menghasilkan alert berlebihan.

##### Skenario

PT Ritel Bersama mengalami peningkatan pembatalan, diskon manual, retur tanpa bukti, dan transaksi di luar jam operasional. Tim audit ingin menggunakan rule-based analytics sebagai tahap awal sebelum mempertimbangkan machine learning. Riwayat menunjukkan bahwa promosi musiman dan perbedaan jam buka antarcabang sering menyebabkan false positive.

##### Instruksi Kerja

1. Tetapkan populasi, periode, dan unit analisis.
2. Susun minimal enam aturan deteksi dan rasionalnya.
3. Tentukan kriteria prioritas alert.
4. Rancang prosedur verifikasi serta dokumentasi keputusan.
5. Usulkan metrik precision, recall, false positive rate, dan nilai kerugian yang dicegah.

##### Lembar Kerja

| Komponen                | Analisis/Jawaban |
|-------------------------|------------------|
| Risiko yang dituju      | .....<br>.....   |
| Aturan/skenario deteksi | .....<br>.....   |
| Data dan parameter      | .....<br>.....   |
| Pengecualian yang sah   | .....<br>.....   |
| Prioritas alert         | .....<br>.....   |
| Langkah verifikasi      | .....<br>.....   |

| Komponen                    | Analisis/Jawaban |
|-----------------------------|------------------|
| Metrik efektivitas          | .....<br>.....   |
| Keputusan dan tindak lanjut | .....<br>.....   |

*Bukti yang dikumpulkan: peta proses, data pendukung, asumsi, perhitungan, keputusan, serta daftar tindak lanjut yang dapat diverifikasi.*

## 5. Perancangan Model Skoring Risiko

### TUJUAN PRAKTIKUM

Menyusun model skoring yang transparan untuk memprioritaskan risiko operasional dan AI.

### Skenario

Komite risiko PT Niaga Prima menerima lebih dari 150 risiko dari unit kerja. Matriks likelihood-impact tidak cukup membedakan risiko yang sama-sama berada pada zona tinggi. Komite ingin menambahkan velocity, detectability, tingkat paparan, dan efektivitas kontrol, tetapi tetap menjaga model agar mudah dipahami pengguna.

### Instruksi Kerja

1. Definisikan skala setiap faktor dan bukti penilaiannya.
2. Tentukan bobot serta alasan bisnisnya.
3. Hitung contoh skor untuk lima risiko.
4. Lakukan sensitivity analysis terhadap perubahan bobot.
5. Rancang aturan eskalasi dan review berkala.

### Lembar Kerja

| Komponen         | Analisis/Jawaban |
|------------------|------------------|
| Faktor penilaian | .....<br>.....   |
| Definisi skala   | .....<br>.....   |
| Bobot            | .....<br>.....   |

| Komponen             | Analisis/Jawaban |
|----------------------|------------------|
| Sumber bukti         | .....<br>.....   |
| Contoh perhitungan   | .....<br>.....   |
| Hasil sensitivitas   | .....<br>.....   |
| Ambang eskalasi      | .....<br>.....   |
| Catatan keterbatasan | .....<br>.....   |

*Bukti yang dikumpulkan: peta proses, data pendukung, asumsi, perhitungan, keputusan, serta daftar tindak lanjut yang dapat diverifikasi.*

## 6. AI Impact Assessment untuk Personalisasi Harga

### TUJUAN PRAKTIKUM

Menilai manfaat, dampak, fairness, privasi, transparansi, dan mekanisme keberatan sebelum implementasi.

### Skenario

Sebuah platform perdagangan ingin memberikan harga dan promosi berbeda berdasarkan perilaku pelanggan, lokasi, perangkat, riwayat transaksi, dan respons terhadap kampanye. Tim pemasaran memperkirakan peningkatan konversi, tetapi tim hukum mengkhawatirkan diskriminasi harga, penggunaan data yang tidak proporsional, serta ketidakjelasan penjelasan kepada pelanggan.

### Instruksi Kerja

1. Nyatakan kebutuhan dan alternatif non-AI.
2. Petakan pihak yang terdampak langsung dan tidak langsung.
3. Identifikasi data pribadi serta dasar pemrosesannya.
4. Uji potensi disparitas dan dampak terburuk.
5. Rancang transparansi, opt-out, keberatan, dan persetujuan.

## Lembar Kerja

| Komponen                | Analisis/Jawaban |
|-------------------------|------------------|
| Tujuan dan manfaat      | .....<br>.....   |
| Alternatif non-AI       | .....<br>.....   |
| Pihak terdampak         | .....<br>.....   |
| Data dan legal basis    | .....<br>.....   |
| Risiko fairness/privasi | .....<br>.....   |
| Kontrol dan oversight   | .....<br>.....   |
| Hak pengguna            | .....<br>.....   |
| Keputusan serta syarat  | .....<br>.....   |

*Bukti yang dikumpulkan: peta proses, data pendukung, asumsi, perhitungan, keputusan, serta daftar tindak lanjut yang dapat diverifikasi.*

## 7. Due Diligence Vendor AI

### TUJUAN PRAKTIKUM

Mengevaluasi eputu teknis, hukum, operasional, keamanan, dan keberlangsungan vendor.

### Skenario

PT Sentosa hendak membeli layanan chatbot eputusan berbasis cloud. Vendor menjanjikan implementasi cepat dan biaya rendah, tetapi kontrak standar tidak menjelaskan eputu data, penggunaan prompt untuk pelatihan, waktu retensi, hak audit, subprocessor, dan

dukungan saat insiden. Tim pengadaan harus memberikan rekomendasi sebelum penandatanganan.

**Instruksi Kerja**

- 1. Susun pertanyaan due diligence berdasarkan kategori eputu.
- 2. Tentukan bukti minimum yang harus diserahkan vendor.
- 3. Nilai red flag dan eputu residual.
- 4. Rancang klausul kontrak serta SLA kritis.
- 5. Tetapkan exit plan dan portabilitas data.

**Lembar Kerja**

| Komponen            | Analisis/Jawaban |
|---------------------|------------------|
| Kategori penilaian  | .....<br>.....   |
| Pertanyaan kunci    | .....<br>.....   |
| Bukti yang diminta  | .....<br>.....   |
| Hasil dan red flag  | .....<br>.....   |
| Risiko residual     | .....<br>.....   |
| Klausul/SLA         | .....<br>.....   |
| Rencana pemantauan  | .....<br>.....   |
| Keputusan pengadaan | .....<br>.....   |

*Bukti yang dikumpulkan: peta proses, data pendukung, asumsi, perhitungan, eputusan, serta daftar tindak lanjut yang dapat diverifikasi.*

## 8. Desain Human Oversight yang Bermakna

### TUJUAN PRAKTIKUM

Menentukan titik intervensi manusia, kompetensi reviewer, kewenangan override, dan bukti review.

### Skenario

Model kredit pelanggan merekomendasikan limit dan tenor otomatis. Dalam pilot, petugas selalu mengikuti rekomendasi karena menganggap model lebih objektif. Beberapa pelanggan lama menerima limit terlalu rendah akibat data transaksi yang belum lengkap. Manajemen ingin menghindari rubber-stamping tanpa menghilangkan efisiensi.

### Instruksi Kerja

1. Klasifikasikan keputusan berdasarkan tingkat dampaknya.
2. Tentukan kapan review manusia wajib dilakukan.
3. Rancang informasi yang harus dilihat reviewer.
4. Tetapkan aturan override dan second approval.
5. Usulkan indikator alert fatigue dan automation bias.

### Lembar Kerja

| Komponen                | Analisis/Jawaban |
|-------------------------|------------------|
| Jenis keputusan         | .....<br>.....   |
| Dampak dan materialitas | .....<br>.....   |
| Titik review manusia    | .....<br>.....   |
| Informasi bagi reviewer | .....<br>.....   |
| Kewenangan override     | .....<br>.....   |
| Bukti keputusan         | .....<br>.....   |

| Komponen                 | Analisis/Jawaban |
|--------------------------|------------------|
| Indikator bias/kelelahan | .....<br>.....   |
| Kontrol perbaikan        | .....<br>.....   |

*Bukti yang dikumpulkan: peta proses, data pendukung, asumsi, perhitungan, keputusan, serta daftar tindak lanjut yang dapat diverifikasi.*

## 9. Penyusunan KRI dan Dashboard AI

### TUJUAN PRAKTIKUM

Membangun indikator peringatan dini yang menghubungkan kinerja model, risiko bisnis, dan kontrol.

### Skenario

Direksi menerima laporan akurasi model setiap bulan, tetapi tidak mengetahui dampak kesalahan terhadap margin, pelanggan, kepatuhan, dan operasi. Tim risiko diminta menyusun dashboard ringkas yang membedakan indikator kinerja, indikator risiko, dan indikator kontrol serta menyediakan ambang hijau-kuning-merah.

### Instruksi Kerja

1. Pilih sasaran dan risiko utama.
2. Rancang minimal dua KPI, dua KRI, dan dua KCI per risiko utama.
3. Tentukan rumus, sumber, pemilik, frekuensi, dan ambang.
4. Susun logika eskalasi.
5. Buat narasi manajemen untuk satu periode pelaporan.

### Lembar Kerja

| Komponen            | Analisis/Jawaban |
|---------------------|------------------|
| Indikator dan jenis | .....<br>.....   |
| Definisi/rumus      | .....<br>.....   |
| Sumber data         | .....<br>.....   |

| Komponen                  | Analisis/Jawaban |
|---------------------------|------------------|
| Pemilik                   | .....<br>.....   |
| Frekuensi                 | .....<br>.....   |
| Ambang hijau-kuning-merah | .....<br>.....   |
| Tindakan eskalasi         | .....<br>.....   |
| Catatan kualitas data     | .....<br>.....   |

*Bukti yang dikumpulkan: peta proses, data pendukung, asumsi, perhitungan, keputusan, serta daftar tindak lanjut yang dapat diverifikasi.*

## 10. Tabletop Exercise Insiden AI

### TUJUAN PRAKTIKUM

Menguji kesiapan organisasi menghadapi insiden AI melalui simulasi lintas fungsi.

### Skenario

Pada pukul 09.00 chatbot pelanggan mulai memberikan instruksi pengembalian dana yang salah. Pukul 10.00 unggahan pelanggan menjadi viral. Pukul 11.00 tim menemukan bahwa basis pengetahuan belum diperbarui dan guardrail dapat dilewati dengan prompt tertentu. Sebagian percakapan mungkin memuat data pribadi. Direksi meminta status dan rencana tindakan sebelum siang.

### Instruksi Kerja

1. Tetapkan klasifikasi dan komandan insiden.
2. Susun tindakan 0-2 jam, 2-24 jam, dan 1-7 hari.
3. Tentukan bukti yang harus diamankan.
4. Rancang komunikasi internal, pelanggan, vendor, dan regulator.
5. Lakukan post-incident review dan pembaruan kontrol.

## Lembar Kerja

| Komponen                  | Analisis/Jawaban |
|---------------------------|------------------|
| Waktu/inject skenario     | .....<br>.....   |
| Keputusan tim             | .....<br>.....   |
| Pemilik tindakan          | .....<br>.....   |
| Bukti yang diamankan      | .....<br>.....   |
| Komunikasi                | .....<br>.....   |
| Risiko lanjutan           | .....<br>.....   |
| Kriteria pemulihan        | .....<br>.....   |
| Pelajaran dan action plan | .....<br>.....   |

*Bukti yang dikumpulkan: peta proses, data pendukung, asumsi, perhitungan, keputusan, serta daftar tindak lanjut yang dapat diverifikasi.*

## 11. Penyusunan Program Audit AI

### TUJUAN PRAKTIKUM

Menyusun tujuan, ruang lingkup, prosedur, sampel, bukti, dan kriteria evaluasi audit AI.

### Skenario

Audit internal akan memeriksa sistem rekomendasi promosi yang telah digunakan selama 18 bulan. Sistem dikelola bersama oleh pemasaran, data science, IT, dan vendor cloud.

Audit sebelumnya hanya menilai keamanan umum, sementara dokumentasi model dan bukti monitoring belum pernah diuji.

#### Instruksi Kerja

1. Susun risk assessment awal dan audit universe.
2. Tentukan tujuan serta scope audit.
3. Rancang prosedur tata kelola, data, model, keamanan, operasi, dan vendor.
4. Tentukan populasi, metode sampling, dan reperformance.
5. Susun format temuan dan tindak lanjut.

#### Lembar Kerja

| Komponen               | Analisis/Jawaban |
|------------------------|------------------|
| Risiko/tujuan kontrol  | .....<br>.....   |
| Kriteria               | .....<br>.....   |
| Prosedur audit         | .....<br>.....   |
| Populasi/sampel        | .....<br>.....   |
| Bukti yang diharapkan  | .....<br>.....   |
| Hasil pengujian        | .....<br>.....   |
| Potensi temuan         | .....<br>.....   |
| Referensi kertas kerja | .....<br>.....   |

*Bukti yang dikumpulkan: peta proses, data pendukung, asumsi, perhitungan, keputusan, serta daftar tindak lanjut yang dapat diverifikasi.*

## 12. Roadmap Kematangan Tata Kelola AI

### TUJUAN PRAKTIKUM

Menilai kondisi saat ini dan menyusun roadmap peningkatan 12-24 bulan.

### Skenario

Perusahaan memiliki beberapa use case AI yang dikembangkan terpisah. Tidak ada inventaris pusat, standar dokumentasi berbeda, peran persetujuan tidak jelas, dan monitoring bergantung pada masing-masing tim. Direksi menginginkan tata kelola yang proporsional tanpa menghentikan inovasi.

### Instruksi Kerja

1. Nilai tingkat kematangan pada governance, people, process, data, technology, risk, compliance, dan assurance.
2. Tentukan target maturity yang realistis.
3. Identifikasi quick wins dan ketergantungan.
4. Susun roadmap per kuartal.
5. Tetapkan indikator manfaat dan risiko transformasi.

### Lembar Kerja

| Komponen          | Analisis/Jawaban |
|-------------------|------------------|
| Domain kematangan | .....<br>.....   |
| Kondisi saat ini  | .....<br>.....   |
| Bukti             | .....<br>.....   |
| Target            | .....<br>.....   |
| Gap utama         | .....<br>.....   |
| Inisiatif         | .....<br>.....   |

| Komponen               | Analisis/Jawaban          |
|------------------------|---------------------------|
| Pemilik/tenggat        | <p>.....</p> <p>.....</p> |
| Indikator keberhasilan | <p>.....</p> <p>.....</p> |

*Bukti yang dikumpulkan: peta proses, data pendukung, asumsi, perhitungan, keputusan, serta daftar tindak lanjut yang dapat diverifikasi.*

## SOAL DISKUSI

Studi kasus berikut dirancang untuk diskusi kelas, ujian berbasis kasus, atau proyek kelompok. Mahasiswa diharapkan menghubungkan konteks bisnis dengan risiko, data, kontrol, etika, implementasi, dan assurance. Tidak selalu tersedia satu jawaban tunggal; kualitas jawaban dinilai dari ketepatan asumsi, kekuatan bukti, konsistensi analisis, dan kelayakan rekomendasi.

### 1. Algoritma Harga dan Persepsi Ketidakadilan

#### Konteks Kasus

PT Belanja Kita menerapkan harga dinamis pada aplikasi. Harga berubah berdasarkan permintaan, persediaan, waktu, lokasi, dan respons pelanggan terhadap promosi. Setelah peluncuran, beberapa pelanggan membandingkan tangkapan layar dan menemukan perbedaan harga pada produk yang sama. Media sosial menuduh perusahaan mendiskriminasi kelompok tertentu. Tim data menjelaskan bahwa model tidak memakai atribut sensitif secara langsung, tetapi variabel lokasi, perangkat, dan pola pembelian mungkin menjadi proxy. Tim hukum meminta penjelasan, sementara pemasaran menolak menghentikan sistem karena konversi meningkat 12 persen.

#### Pertanyaan Analitis

1. Apakah kenaikan konversi cukup untuk mempertahankan sistem? Jelaskan trade-off-nya.
2. Petakan risiko bisnis, etika, privasi, hukum, reputasi, dan model.
3. Tentukan analisis fairness dan data yang diperlukan.
4. Rancang opsi mitigasi jangka pendek dan jangka panjang.
5. Susun pesan kepada pelanggan dan direksi.

#### Kerangka Jawaban dan Bukti

| Komponen                                 | Analisis/Jawaban |
|------------------------------------------|------------------|
| Sasaran dan keputusan yang dipertaruhkan | .....<br>.....   |
| Pihak terdampak                          | .....<br>.....   |
| Pernyataan risiko prioritas              | .....<br>.....   |
| Data/bukti yang diperlukan               | .....<br>.....   |
| Kontrol dan opsi respons                 | .....<br>.....   |

| Komponen                       | Analisis/Jawaban |
|--------------------------------|------------------|
| Keputusan serta alasan         | .....<br>.....   |
| Risiko residual dan monitoring | .....<br>.....   |

## 2. Prediksi Permintaan yang Gagal pada Musim Bencana

### Konteks Kasus

Model peramalan distributor bahan pokok dilatih dari data lima tahun dan berkinerja baik pada kondisi normal. Ketika banjir besar mengganggu beberapa wilayah, pola permintaan, akses jalan, dan kapasitas pemasok berubah drastis. Model tetap merekomendasikan alokasi berdasarkan pola historis sehingga cabang terdampak mengalami kekosongan, sementara cabang lain kelebihan stok. Pengguna sebenarnya dapat melakukan override, tetapi banyak yang tidak melakukannya karena percaya pada skor keyakinan yang tinggi.

### Pertanyaan Analitis

1. Identifikasi model risk dan operational risk dalam kasus.
2. Jelaskan hubungan drift, uncertainty, dan automation bias.
3. Rancang trigger untuk mode krisis dan fallback manual.
4. Tentukan data eksternal serta monitoring yang diperlukan.
5. Susun post-incident action plan.

### Kerangka Jawaban dan Bukti

| Komponen                                 | Analisis/Jawaban |
|------------------------------------------|------------------|
| Sasaran dan keputusan yang dipertaruhkan | .....<br>.....   |
| Pihak terdampak                          | .....<br>.....   |
| Pernyataan risiko prioritas              | .....<br>.....   |
| Data/bukti yang diperlukan               | .....<br>.....   |
| Kontrol dan opsi respons                 | .....<br>.....   |

| Komponen                       | Analisis/Jawaban |
|--------------------------------|------------------|
| Keputusan serta alasan         | .....<br>.....   |
| Risiko residual dan monitoring | .....<br>.....   |

### 3. Chatbot Mengungkap Informasi Internal

#### Konteks Kasus

Chatbot layanan pelanggan menggunakan retrieval-augmented generation dari dokumen prosedur, FAQ, dan katalog. Seorang pengguna menemukan bahwa dengan instruksi bertahap, chatbot dapat menampilkan potongan dokumen internal yang seharusnya hanya untuk karyawan. Dokumen tersebut tidak memuat rahasia dagang besar, tetapi berisi alamat email internal, ambang diskon, dan alur eskalasi fraud. Vendor menyatakan masalah berada pada konfigurasi akses perusahaan, sedangkan tim internal menilai platform tidak memberikan guardrail yang memadai.

#### Pertanyaan Analitis

1. Klasifikasikan insiden dan pihak yang harus terlibat.
2. Identifikasi kelemahan data, akses, aplikasi, vendor, dan monitoring.
3. Tentukan bukti digital yang harus dipertahankan.
4. Rancang containment, eradication, recovery, dan komunikasi.
5. Usulkan pengujian keamanan sebelum peluncuran ulang.

#### Kerangka Jawaban dan Bukti

| Komponen                                 | Analisis/Jawaban |
|------------------------------------------|------------------|
| Sasaran dan keputusan yang dipertaruhkan | .....<br>.....   |
| Pihak terdampak                          | .....<br>.....   |
| Pernyataan risiko prioritas              | .....<br>.....   |
| Data/bukti yang diperlukan               | .....<br>.....   |
| Kontrol dan opsi respons                 | .....<br>.....   |

| Komponen                       | Analisis/Jawaban |
|--------------------------------|------------------|
| Keputusan serta alasan         | .....<br>.....   |
| Risiko residual dan monitoring | .....<br>.....   |

#### 4. Model Kredit untuk Pelanggan Grosir

##### Konteks Kasus

Perusahaan dagang memberi limit kredit kepada toko kecil berdasarkan histori pembelian, pembayaran, lokasi, jenis usaha, umur usaha, dan interaksi dengan sales. Model baru menurunkan tingkat piutang bermasalah, tetapi banyak pelanggan baru memperoleh limit sangat rendah karena tidak memiliki histori. Sales kemudian memasukkan transaksi percobaan dan catatan optimistis untuk meningkatkan skor. Audit menemukan bahwa override sering dilakukan tanpa alasan terstruktur.

##### Pertanyaan Analitis

1. Analisis risiko data, perilaku manusia, insentif, dan fairness.
2. Tentukan model governance dan segregation of duties yang diperlukan.
3. Rancang kebijakan cold-start bagi pelanggan baru.
4. Tentukan pengujian override dan indikator manipulasi.
5. Buat rekomendasi kepada komite kredit.

##### Kerangka Jawaban dan Bukti

| Komponen                                 | Analisis/Jawaban |
|------------------------------------------|------------------|
| Sasaran dan keputusan yang dipertaruhkan | .....<br>.....   |
| Pihak terdampak                          | .....<br>.....   |
| Pernyataan risiko prioritas              | .....<br>.....   |
| Data/bukti yang diperlukan               | .....<br>.....   |
| Kontrol dan opsi respons                 | .....<br>.....   |

| Komponen                       | Analisis/Jawaban |
|--------------------------------|------------------|
| Keputusan serta alasan         | .....<br>.....   |
| Risiko residual dan monitoring | .....<br>.....   |

## 5. Shadow AI di Divisi Pemasaran

### Konteks Kasus

Divisi pemasaran menggunakan beberapa alat generative AI gratis untuk membuat materi kampanye, menganalisis komentar pelanggan, dan menyusun segmentasi. Tidak ada inventaris resmi. Sebagian staf memasukkan ringkasan percakapan pelanggan dan proposal mitra ke layanan publik. Hasil AI sering langsung dipublikasikan karena target kampanye sangat ketat. Tim IT baru mengetahui praktik tersebut setelah satu akun diblokir oleh penyedia layanan.

### Pertanyaan Analitis

1. Mengapa larangan total belum tentu efektif?
2. Petakan jenis data dan tingkat sensitivitasnya.
3. Rancang acceptable use policy dan jalur alat yang disetujui.
4. Tentukan program literasi serta monitoring shadow AI.
5. Susun roadmap transisi tanpa menghentikan operasi pemasaran.

### Kerangka Jawaban dan Bukti

| Komponen                                 | Analisis/Jawaban |
|------------------------------------------|------------------|
| Sasaran dan keputusan yang dipertaruhkan | .....<br>.....   |
| Pihak terdampak                          | .....<br>.....   |
| Pernyataan risiko prioritas              | .....<br>.....   |
| Data/bukti yang diperlukan               | .....<br>.....   |
| Kontrol dan opsi respons                 | .....<br>.....   |

| Komponen                       | Analisis/Jawaban |
|--------------------------------|------------------|
| Keputusan serta alasan         | .....<br>.....   |
| Risiko residual dan monitoring | .....<br>.....   |

## 6. Vendor Mengubah Model Tanpa Pemberitahuan

### Konteks Kasus

Sistem verifikasi dokumen berbasis AI disediakan sebagai layanan. Setelah pembaruan vendor, tingkat penolakan dokumen pelanggan meningkat tajam. Vendor menyatakan pembaruan meningkatkan keamanan dan diterapkan untuk seluruh klien. Kontrak tidak mewajibkan pemberitahuan perubahan model, menyediakan versi sebelumnya, atau memberikan metrik per segmen. Perusahaan kesulitan membuktikan dampak karena log detail hanya disimpan selama tujuh hari.

### Pertanyaan Analitis

1. Identifikasi kegagalan kontrak dan vendor governance.
2. Tentukan klausul material change, logging, rollback, audit right, dan SLA.
3. Rancang proses validasi ulang setelah perubahan.
4. Tentukan kompensasi dan perlindungan pelanggan.
5. Susun exit strategy serta kriteria vendor alternatif.

### Kerangka Jawaban dan Bukti

| Komponen                                 | Analisis/Jawaban |
|------------------------------------------|------------------|
| Sasaran dan keputusan yang dipertaruhkan | .....<br>.....   |
| Pihak terdampak                          | .....<br>.....   |
| Pernyataan risiko prioritas              | .....<br>.....   |
| Data/bukti yang diperlukan               | .....<br>.....   |
| Kontrol dan opsi respons                 | .....<br>.....   |

| Komponen                       | Analisis/Jawaban |
|--------------------------------|------------------|
| Keputusan serta alasan         | .....<br>.....   |
| Risiko residual dan monitoring | .....<br>.....   |

## 7. Fraud Detection dengan False Positive Tinggi

### Konteks Kasus

Model deteksi fraud menandai 8 persen transaksi sebagai mencurigakan, jauh di atas kapasitas tim investigasi. Karena alert menumpuk, analis mulai menutup kasus dengan cepat dan beberapa transaksi benar-benar fraud terlewat. Model memiliki recall tinggi tetapi precision rendah. Manajemen meminta ambang dinaikkan, sedangkan tim risiko khawatir kerugian meningkat.

### Pertanyaan Analitis

1. Jelaskan trade-off precision, recall, kapasitas, dan dampak.
2. Rancang triage serta risk-based prioritization.
3. Tentukan peran rules, model, dan investigator.
4. Usulkan metrik efektivitas end-to-end, bukan model saja.
5. Rancang eksperimen perubahan threshold yang aman.

### Kerangka Jawaban dan Bukti

| Komponen                                 | Analisis/Jawaban |
|------------------------------------------|------------------|
| Sasaran dan keputusan yang dipertaruhkan | .....<br>.....   |
| Pihak terdampak                          | .....<br>.....   |
| Pernyataan risiko prioritas              | .....<br>.....   |
| Data/bukti yang diperlukan               | .....<br>.....   |
| Kontrol dan opsi respons                 | .....<br>.....   |

| Komponen                       | Analisis/Jawaban |
|--------------------------------|------------------|
| Keputusan serta alasan         | .....<br>.....   |
| Risiko residual dan monitoring | .....<br>.....   |

## 8. AI untuk Seleksi Pemasok

### Konteks Kasus

Perusahaan menilai pemasok dengan model yang menggabungkan harga, kualitas, ketepatan pengiriman, kapasitas, lokasi, kepatuhan, dan ulasan. Pemasok kecil mengeluh selalu kalah karena data historis terbatas dan tidak memiliki sertifikasi mahal. Procurement menilai model objektif, tetapi sustainability team menemukan bahwa indikator sosial dan lingkungan hanya berbobot kecil karena dianggap sulit diukur.

### Pertanyaan Analitis

1. Tentukan tujuan yang sah dan konflik antar-sasaran.
2. Analisis bias terhadap pemasok kecil dan pemasok baru.
3. Rancang data tambahan serta proses keberatan.
4. Tentukan human oversight dalam keputusan pengadaan.
5. Usulkan balanced scorecard dan governance model.

### Kerangka Jawaban dan Bukti

| Komponen                                 | Analisis/Jawaban |
|------------------------------------------|------------------|
| Sasaran dan keputusan yang dipertaruhkan | .....<br>.....   |
| Pihak terdampak                          | .....<br>.....   |
| Pernyataan risiko prioritas              | .....<br>.....   |
| Data/bukti yang diperlukan               | .....<br>.....   |
| Kontrol dan opsi respons                 | .....<br>.....   |

| Komponen                       | Analisis/Jawaban |
|--------------------------------|------------------|
| Keputusan serta alasan         | .....<br>.....   |
| Risiko residual dan monitoring | .....<br>.....   |

## 9. Deepfake dan Social Engineering pada Pembayaran

### Konteks Kasus

Staf keuangan menerima panggilan video yang tampak berasal dari direktur dan meminta pembayaran mendesak kepada rekening baru. Suara, wajah, dan gaya bicara terlihat meyakinkan. Staf hampir memproses transaksi karena email pendukung juga tampak berasal dari akun resmi. Sistem keamanan tidak mendeteksi malware; serangan berfokus pada manipulasi manusia dan penyalahgunaan identitas.

### Pertanyaan Analitis

1. Petakan tahapan serangan dan kontrol yang gagal.
2. Rancang prosedur out-of-band verification.
3. Tentukan perubahan otorisasi pembayaran dan limit.
4. Susun program simulasi serta literasi deepfake.
5. Rancang respons insiden dan pelestarian bukti.

### Kerangka Jawaban dan Bukti

| Komponen                                 | Analisis/Jawaban |
|------------------------------------------|------------------|
| Sasaran dan keputusan yang dipertaruhkan | .....<br>.....   |
| Pihak terdampak                          | .....<br>.....   |
| Pernyataan risiko prioritas              | .....<br>.....   |
| Data/bukti yang diperlukan               | .....<br>.....   |
| Kontrol dan opsi respons                 | .....<br>.....   |

| Komponen                       | Analisis/Jawaban |
|--------------------------------|------------------|
| Keputusan serta alasan         | .....<br>.....   |
| Risiko residual dan monitoring | .....<br>.....   |

## 10. Audit AI Menemukan Bukti yang Tidak Lengkap

### Konteks Kasus

Audit internal memeriksa model rekomendasi stok. Tim model dapat menunjukkan kode dan metrik akurasi, tetapi tidak memiliki versi dataset, catatan persetujuan, alasan pemilihan fitur, hasil fairness test, atau bukti review setelah drift. Pemilik bisnis menyatakan model tetap bermanfaat dan tidak pernah menyebabkan insiden besar. Auditor harus menilai apakah kekurangan dokumentasi merupakan masalah administratif atau kelemahan kontrol yang material.

### Pertanyaan Analitis

1. Tentukan kriteria audit dan bukti minimum.
2. Bedakan design deficiency dan operating deficiency.
3. Nilai dampak dari tidak adanya traceability.
4. Rancang prosedur alternatif dan reperformance.
5. Susun temuan, rating, rekomendasi, dan action plan.

### Kerangka Jawaban dan Bukti

| Komponen                                 | Analisis/Jawaban |
|------------------------------------------|------------------|
| Sasaran dan keputusan yang dipertaruhkan | .....<br>.....   |
| Pihak terdampak                          | .....<br>.....   |
| Pernyataan risiko prioritas              | .....<br>.....   |
| Data/bukti yang diperlukan               | .....<br>.....   |
| Kontrol dan opsi respons                 | .....<br>.....   |

| Komponen                       | Analisis/Jawaban          |
|--------------------------------|---------------------------|
| Keputusan serta alasan         | <p>.....</p> <p>.....</p> |
| Risiko residual dan monitoring | <p>.....</p> <p>.....</p> |

## DAFTAR PUSTAKA

- Badshah, A., Daud, A., Alharbey, R., Banjar, A., Bukhari, A., et al. (2024). Big Data Applications: Overview, Challenges and Future. *Artificial Intelligence Review*, 57, 290.
- Committee of Sponsoring Organizations of the Treadway Commission. (2004). *Enterprise Risk Management - Integrated Framework*.
- Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise Risk Management - Integrating with Strategy and Performance*.
- Dahana, PT. (2025). Peluncuran aplikasi E-Manrisk untuk manajemen risiko terintegrasi.
- Davenport, T. H., & Mittal, N. (2020). How artificial intelligence will transform decision making.
- European Union. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), sebagaimana diperbarui.
- Febriani, F., & Prasetya, M. E. (2025). Evaluation of risk management implementation using COSO ERM 2017 framework: A case study at PT XYZ. *Journal of Accounting and Business Education*, 9(2), 112-128.
- Hanggraeni, D. (2015). *Manajemen Risiko Perusahaan Terintegrasi dan Good Corporate Governance*. UI Press.
- Hopkin, P. (2018). *Fundamentals of Risk Management*. Kogan Page.
- Institute of Internal Auditors. (2020). *The IIA Three Lines Model*.
- International Organization for Standardization. (2018). *ISO 31000:2018 Risk management - Guidelines*.
- International Organization for Standardization. (2023a). *ISO/IEC 23894:2023 Information technology - Artificial intelligence - Guidance on risk management*.
- International Organization for Standardization. (2023b). *ISO/IEC 42001:2023 Information technology - Artificial intelligence - Management system*.
- Jagatheesaperumal, S. K., Rahouti, M., Ahmad, K., Al-Fuqaha, A., & Guizani, M. (2022). The Duo of Artificial Intelligence and Big Data for Industry 4.0: Applications, Techniques, Challenges, and Future Research Directions. *IEEE Internet of Things Journal*, 9(15), 12861–12885.
- Jamarani, A., Haddadi, S., Sarvizadeh, R., Haghi Kashani, M., Akbari, M., et al. (2024). Big Data and Predictive Analytics: A Systematic Review of Applications. *Artificial Intelligence Review*, 57, 176.
- Jan, Z., Ahamed, F., Mayer, W., Patel, N., Grossmann, G., Stumptner, M., & Kuusk, A. (2023). Artificial Intelligence for Industry 4.0: Systematic Review of Applications, Challenges, and Opportunities. *Expert Systems with Applications*, 216, 119456.

- Kaplan, R. S., & Mikes, A. (2012). Managing risks: A new framework. Harvard Business Review.
- Kementerian Komunikasi dan Informatika Republik Indonesia. (2023). Surat Edaran Menteri Komunikasi dan Informatika Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial.
- Lam, J. (2014). Enterprise Risk Management: From Incentives to Controls. Wiley.
- Monks, R. A. G., & Minow, N. (2011). Corporate Governance. Wiley.
- National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST AI 100-1.
- National Institute of Standards and Technology. (2024). Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile, NIST AI 600-1.
- OECD. (2024). OECD AI Principles.
- Open Worldwide Application Security Project. (2026). OWASP GenAI LLM Top 10 2026.
- Provost, F., & Fawcett, T. (2013). Data Science for Business. O'Reilly Media.
- Prowanta, E. (2025). Best Practice Implementasi Manajemen Risiko ISO 31000:2018. Penerbit Buku Kompas.
- Rath, S., Pandey, M., & Rautaray, S. S. (2025). Synergistic Review of Automation Impact of Big Data, AI, and ML in Current Data Transformative Era. F1000Research, 14, 253.
- Republik Indonesia. (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.
- Sutrisno. (2023). Manajemen Risiko: Substansi dan Fundamental. Rajawali Pers.
- UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence.
- Vaughan, E. J., & Vaughan, T. M. (1997). Fundamentals of Risk and Insurance. Wiley.

Sri Wahyuning, S.Kom., M.Si

# MANAJEMEN RISIKO PERUSAHAAN DAGANG BERBASIS ARTIFICIAL INTELLIGENCE

Konsep, Kerangka, Identifikasi, Analisis, Mitigasi,  
Implementasi, dan Audit



Sri Wahyuning, S.Kom., M.Si. merupakan dosen pada Program Studi D4 Akuntansi Perpajakan, Universitas STEKOM Semarang. Menyelesaikan pendidikan S1 di Universitas STEKOM dan pendidikan S2 di STIE Dharma Putra Semarang.

Memiliki bidang keahlian yang meliputi Akuntansi, Perpajakan, Sistem Informasi Akuntansi, Laboratorium Akuntansi Keuangan, dan Statistika. Dalam kegiatan akademik, aktif mengampu berbagai mata kuliah, antara lain Dasar Akuntansi, Akuntansi Keuangan, Perpajakan, Akuntansi Lanjutan, Sistem Informasi Akuntansi, dan FinTech.

Selain kegiatan pengajaran, aktif dalam penelitian dan publikasi ilmiah, khususnya pada bidang perpajakan dan sistem informasi akuntansi. Beberapa karya ilmiah yang telah dipublikasikan antara lain "Pengaruh Pemutihan Berkala dan Literasi Wajib Pajak terhadap Kepatuhan PKB Orang Pribadi di Kota Semarang" dan "Pengembangan Sistem Informasi Akuntansi Persediaan Barang Berbasis Web Menggunakan Metode Average".

Dalam kegiatan pengabdian kepada masyarakat, aktif melaksanakan pelatihan dan pendampingan bagi UMKM, khususnya dalam bidang akuntansi dan perpajakan.

Saat ini juga aktif dalam pengembangan bahan ajar dan penulisan buku yang mengintegrasikan akuntansi, teknologi digital, dan Artificial Intelligence, salah satunya buku berjudul "Manajemen Risiko Perusahaan Dagang Berbasis Artificial Intelligence".



YAYASAN PRIMA AGUS TEKNIK

## PENERBIT :

YAYASAN PRIMA AGUS TEKNIK  
Jl. Majapahit No. 605 Semarang  
Telp. (024) 6723456. Fax. 024-6710144  
Email : penerbit\_ypat@stekom.ac.id

ISBN 978-634-7695-57-4 (PDF)



9

786347

695574