

User Manual (Panduan Pengguna)

Dokumen ini ditujukan untuk pengguna bisnis (Kepala SPI, Manajer Audit).

Akses Dashboard

- Platform: Power BI Desktop / Service.
- Login: Gunakan akun kepala_spi atau analis_user yang telah didaftarkan .

Navigasi Dashboard

- Halaman 1: Executive Oversight: Gunakan untuk melihat total potensi kerugian (Rp 25T) dan daftar Unit Kerja dengan risiko tertinggi (Top Risk Units).
- Halaman 2: Analytical Deep-Dive: Gunakan *Waterfall Chart* untuk menganalisis kontribusi kerugian berdasarkan kategori risiko (Finansial vs Operasional).
- Halaman 3: Audit & Risk: Gunakan grafik "Top 10 Auditor" untuk memantau produktivitas tim audit.

Fitur Interaktif

- Filter Tahun: Gunakan *slicer* di pojok kanan atas untuk memilih Tahun Audit (misal: 2024).
- Drill-Down: Klik kanan pada grafik batang unit kerja untuk melihat detail temuan spesifik di unit tersebut.
- Export: Klik opsi "Export data" pada tabel detail untuk mengunduh laporan ke Excel.

Operations Manual (Panduan Operasional)

Dokumen ini ditujukan untuk administrator database (DBA/IT).

Jadwal Job Harian

- 02:00 WIB: Job ETL_Daily_Load berjalan otomatis via SQL Server Agent.
- Pengecekan Kualitas: Prosedur usp_Run_DQ_Checks berjalan setelah ETL selesai untuk memvalidasi skor risiko dan integritas referensi.

Strategi Backup & Recovery

- Full Backup: Dijadwalkan setiap Minggu pukul 00:00. Disimpan di D:\Backup\DM_SPI_DW_Full.bak.
- Differential Backup: Dijadwalkan setiap Hari pukul 00:00.
- Transaction Log: Dijadwalkan setiap 6 jam untuk *point-in-time recovery*.

Troubleshooting

- Jika ETL gagal, cek tabel log di SQL Agent History.
- Jika Data Quality Check gagal (misal: ada *Orphan Records*), segera hubungi tim pengembang data.

Security Documentation

Dokumen ini menjelaskan mekanisme perlindungan data sensitif SPI.

Manajemen Akses (RBAC) Sistem menggunakan *Database Roles* untuk membatasi akses:

- db_kepala_spi: Akses Penuh (*Select, Execute*).
- db_analisis_audit: Akses Baca/Tulis ke *Staging*, Baca ke *DW*.
- db_viewer: Akses Baca Saja (*Read-Only*) ke Dashboard/Views.
- db_etl_operator: Hak eksekusi prosedur ETL.

Perlindungan Data (Data Masking)

- Kolom NIP Auditor (ID_Sistem_Sumber): Menggunakan fungsi partial(0, "XX-XXX-", 4) agar tidak terlihat oleh user biasa.
- Kolom Penanggung Jawab: Menggunakan fungsi default() untuk penyensoran penuh.
- Unmasking: Hanya role db_kepala_spi dan db_analisis_audit yang memiliki izin UNMASK untuk melihat data asli.

Audit Trail Setiap perubahan data (INSERT, UPDATE, DELETE) pada tabel sensitif dicatat otomatis ke dalam tabel dbo.AuditLog melalui *Database Trigger*, mencakup informasi pengguna (UserName) dan waktu kejadian (EventTime).