FEBY YOLANDA S
2313031068
2023 C

JAWABAN CASE STUDY 2

Kasus "IzinCerdas" ini adalah contoh sempurna dari "penyakit" birokrasi lama yang "dibungkus" dengan teknologi baru. Masalahnya jelas bukan di teknologinya semata, tapi pada proses bisnis dan integritas manusianya yang gagal bertransformasi. Untuk menyusun audit kinerjanya, pendekatan yang paling tepat adalah **Pendekatan Audit Kinerja Berbasis Risiko (Risk-Based Performance Audit)**, karena mengaudit semua fitur sistem ini hanya buang-buang waktu. Fokusnya harus pada area yang punya risiko paling tinggi dan paling "berdampak" berdasarkan temuan Ombudsman. Pertama, risikonya harus dipetakan. Jelas ada tiga risiko utama di sini: **Risiko Efektivitas** (Sistem gagal mencapai tujuan utama mempercepat layanan, terbukti dari keterlambatan 10 hari), **Risiko Transparansi/Operasional** (Sistem gagal memberikan kejelasan status), dan yang paling gawat, **Risiko Integritas** (Adanya penyalahgunaan wewenang meski sudah digital, ini *red flag* KKN). Prioritas tertinggi audit ini adalah membongkar Risiko Integritas dan Efektivitas. Kriteria auditnya akan sangat jelas: untuk efektivitas, membandingkan realisasi waktu terbit izin dengan Standar Pelayanan Minimal (SPM) atau SOP yang dijanjikan. Untuk integritas, kriterianya adalah *zero tolerance* terhadap intervensi manual yang melompati alur sistem.

Nah, untuk membongkar risiko-risiko ini, tidak bisa hanya mengandalkan wawancara atau cek dokumen fisik. Sistem "IzinCerdas" itu sendiri harus "diinterogasi" dengan **menggunakan teknologi digital audit**. Pertama, untuk membuktikan **Risiko Efektivitas** (keterlambatan 10 hari), teknik yang digunakan adalah **Process Mining**. Caranya dengan meminta *full event logs* dari server "IzinCerdas", lalu memasukkannya ke *software process mining*. Teknologi ini akan memvisualisasikan alur proses izin yang *sebenarnya* terjadi, bukan alur yang seharusnya di SOP. Dari situ akan terlihat jelas di "meja" pejabat mana atau di tahapan mana "bottleneck" atau kemacetan itu terjadi. Mungkin datanya akan menunjukkan 9 dari 10 hari keterlambatan itu terjadi hanya di satu titik persetujuan.

Kedua, dan ini yang paling krusial untuk membongkar **Risiko Integritas** (penyalahgunaan wewenang), adalah melakukan **Analisis Data (Data Analytics)** secara mendalam. Skrip *anomaly detection* harus dijalankan untuk mencari pola-pola ganjil. Misalnya: Apakah ada izin yang terbit "kilat" (misal, 1 jam selesai) padahal jenis izinnya sama dengan yang rata-rata 10 hari? Ini indikasi "jalur VVIP". Sebaliknya, apakah ada izin yang sengaja "diperlambat" tanpa alasan sistem? Ini bisa jadi modus "menunggu pelicin". Selain itu, perlu dilakukan **analisis jejak digital (audit trail)** terhadap *user* dengan hak akses super-admin atau pejabat kunci. Harus dicari: Apakah ada *user* yang bisa mengubah status izin secara manual (misal, dari "Ditolak" langsung jadi "Disetujui") tanpa melalui alur verifikasi sistem? Inilah "pintu belakang" digital yang paling sering dimanfaatkan untuk praktik penyalahgunaan wewenang. Dengan kombinasi audit berbasis risiko dan

penggunaan teknologi ini, bukti audit yang dihasilkan bisa sangat objektif dan kuantitatif, bukan lagi "katanya", tapi langsung dari data sistem itu sendiri.