BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Transformasi digital dan adopsi *multi-cloud* dan *Software as a Service* (SaaS) mendorong pertumbuhan pesat jumlah aplikasi, akun, dan *entitlement*. Pengelolaan manual atas siklus hidup identitas *Joiner Mover Leaver* (JML), permintaan akses, serta pencabutan hak saat *offboarding* tidak memadai karena kurang efisien, rentan kesalahan, dan sulit diaudit lintas sistem. Kondisi tersebut meningkatkan risiko *overprovisioning*, akun yatim, pelanggaran *Separation of Duties*, serta lemahnya pembuktian kepatuhan [1]. Rekomendasi penguatan kontrol identitas juga ditegaskan oleh otoritas keamanan [2].

Industri menempatkan *identity lifecycle management* sebagai kontrol preventif inti untuk menjamin bahwa identitas diciptakan, dipelihara, dan dinonaktifkan secara terstandar dengan jejak audit yang lengkap. Otomasi JML membantu memastikan hak akses selalu selaras dengan peran dan perubahan organisasi [3]. Upaya ini menekan *overprovisioning* dan mengurangi akun yatim [4]. Pada tataran tata kelola, penegakan *Separation of Duties* diperlukan guna mengurangi potensi penyalahgunaan kewenangan dan meningkatkan akuntabilitas melalui pemisahan fungsi kritis serta pembatasan kombinasi hak akses yang berkonflik [5].

Kebutuhan tersebut selaras dengan paradigma *Zero Trust* yang meniadakan kepercayaan implisit dan menekankan verifikasi berkelanjutan terhadap pengguna, perangkat, dan sesi. Dalam arsitektur ini, kemampuan identitas berperan utama untuk menerapkan prinsip *least privilege*, penegakan kebijakan kontekstual, dan pelacakan akses ujung ke ujung di lingkungan hibrida [6].

Dorongan regulasi dan risiko bisnis memperkuat urgensi tata kelola identitas di organisasi besar. Standar ISO/IEC 27001:2022 pada kontrol A.5.16 *Identity Management* menuntut pengelolaan identitas sepanjang siklus hidup agar hanya pihak berwenang yang memiliki hak akses yang tepat setiap saat [7]. Rujukan lain menekankan pentingnya bukti audit dan pengendalian risiko [8]. Di Indonesia, Undang-Undang Pelindungan Data Pribadi sudah berlaku penuh dengan masa transisi kepatuhan yang berakhir pada 17 Oktober 2024 [9]. Dampaknya, organisasi harus menerapkan tata kelola akses yang lebih ketat untuk melindungi data pribadi

[10].

Dari sisi risiko, data industri menunjukkan bahwa kredensial yang dicuri masih menjadi penyebab utama insiden dan pelanggaran data [11]. Biaya pemulihan pelanggaran juga meningkat dan menambah tekanan pada ketahanan operasional [12]. Ringkasan bisnis menegaskan arah yang sama [13]. Fakta tersebut menempatkan identitas sebagai perimeter baru, sehingga kontrol *Identity and Access Management* (IAM) yang kuat menjadi esensial.

Dalam konteks PT Asuransi Jasa Indonesia, sistem yang digunakan perlu ditingkatkan karena sudah usang dan tidak lagi didukung oleh vendor utama. IBM menyediakan jalur peningkatan dari platform lama menuju platform tata kelola identitas yang lebih baru.

Mempertahankan *IBM Security Identity Manager* (ISIM) yang berstatus *end of support* per 30 September 2022 berarti tidak ada lagi *patch* dan perbaikan resmi [14]. Siklus hidup produk IBM menjelaskan konsekuensi ketiadaan dukungan [15]. Jalur peningkatan ke *IBM Security Verify Governance* (ISVG) dipilih untuk mengembalikan akses ke tambalan keamanan, kemampuan modernisasi, dan dukungan vendor [16]. Dokumentasi resmi memberikan panduan teknis pelaksanaan peningkatan [17].

Sasaran bisnis PT Asuransi JASINDO berfokus pada penutupan sumber akses tidak sah di lingkungan identitas yang kompleks. Dengan platform yang didukung vendor, kebijakan akses adaptif lebih mudah diterapkan dan otomasi kontrol di titik kritis dapat dijalankan. Visibilitas dan *audit trail* menyeluruh juga lebih mudah dicapai [17].

Alasan finansial turut menguatkan rencana peningkatan. Kredensial curian tetap menjadi pemicu dominan insiden [11]. Biaya rata-rata pelanggaran global mencapai sekitar 4,88 juta dolar pada 2024, dan angkanya lebih tinggi untuk sektor keuangan [12]. Laporan khusus sektor keuangan memperinci risiko biaya tersebut [18]. Dengan peningkatan ke ISVG, biaya dapat digeser dari kerugian reaktif menuju belanja yang terencana melalui dukungan vendor dan pemendekan durasi insiden [16].

1.2 Maksud dan Tujuan Kerja Magang

Maksud pelaksanaan kerja magang adalah sebagai berikut.

1. Memperoleh pengalaman langsung dalam implementasi *Identity Governance and Administration* berskala *enterprise*.

2. Memperdalam kompetensi teknis pada *security governance*, *provisioning*, dan integrasi konektor.
3. Mengembangkan keterampilan otomasi siklus hidup identitas Joiner Mover Leaver serta standardisasi proses akses lintas aplikasi.
4. Meningkatkan kemampuan integrasi konektor untuk target sistem prioritas serta rekonsiliasi data yang konsisten.
5. Membangun kepekaan terhadap ketahanan layanan melalui perbaikan waktu pemulihan insiden dan pengurangan pekerjaan perbaikan berulang.

Adapun tujuan kerja magang pada PT GIT adalah sebagai berikut.

1. Melaksanakan persiapan teknis implementasi IBM Security Verify Governance (ISVG) pada lingkungan *proof of concept* (PoC) PT Asuransi JASINDO.
2. Menyusun dan memverifikasi kesiapan infrastruktur pendukung migrasi menuju ISVG melalui pencatatan *baseline*, pembuatan *backup*, uji konektivitas antar komponen, serta dokumentasi prosedur verifikasi untuk fase berikutnya.

1.3 Waktu dan Prosedur Pelaksanaan Kerja Magang

Pelaksanaan kerja magang di PT Global Innovation Technology merupakan perpanjangan kontrak selama enam bulan. Kegiatan dimulai pada 1 Februari 2025, kemudian diperpanjang mulai 1 Agustus 2025 sampai 31 Januari 2026. Skema kerja menggunakan pola *hybrid* dengan kehadiran di kantor pada hari Senin, Selasa, Kamis, dan Jumat serta bekerja dari rumah pada hari Rabu.

Jam kerja berlangsung dari pukul 08.30 sampai 17.30 WIB dengan waktu istirahat dari pukul 12.00 sampai 13.00. Ketentuan busana saat bekerja di kantor adalah sebagai berikut. Pada hari Selasa mengenakan batik. Pada hari Jumat diperbolehkan menggunakan atasan tanpa kerah. Pada hari kerja lainnya wajib menggunakan atasan berkerah. Untuk bawahan setiap hari menggunakan celana kain berwarna hitam.

Status pekerjaan dilakukan lewat rapat singkat setiap hari untuk membahas kemajuan, kendala, dan rencana hari ini. Rencana kerja dibuat di awal jam kerja, hasil kerja ditinjau di akhir jam kerja, dan perbaikan proses disepakati bersama. Penugasan, catatan kemajuan, dan pelaporan bukti kerja dilakukan di KejarTugas.