BAB III

METODOLOGI PENELITIAN

3.1 Gambaran Umum Objek Penelitian

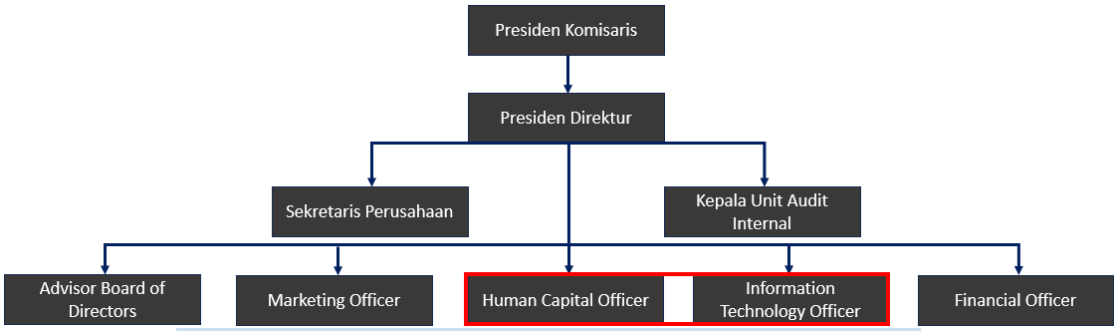
Pada pembahasan penelitian, objek yang digunakan adalah PT XYZ yang merupakan salah satu perseroan penyedia jaringan internet dan program televisi di Indonesia dengan jumlah total karyawan internal sekitar 860 orang. Perusahaan berdiri pertama kali pada tahun 1996 dengan kegiatan bisnis utamanya adalah perdagangan. Tetapi kemudian seiring berjalannya waktu, perusahaan mengubah bisnisnya ke bidang teknologi dan jasa penyediaan internet.

Hingga saat ini perusahaan telah mengembangangkan kegiatan usahanya dengan menyediakan pelayanan dalam bentuk telekomunikasi kabel, multimedia, internet berkecepatan tinggi, dan juga jasa konsultasi bisnis. Cabang PT XYZ terbentang di beberapa wilayah seperti Jabodetabek, Bandung, Surabaya, Malang, Gresik, Sidoarjo, Bali, Serang, Cilegon, Solo, Medan, Yogyakarta, dan Kediri.

Perusahaan berfokus dalam menyediakan internet untuk kalangan menengah dengan jumlah lebih dari 2 juta pelanggan di Indonesia. Selain itu, PT XYZ juga melayani penyediaan jaringan internet ke 2.400 institusi besar yang mencakup bidang pemerintahan, keuangan, perusahaan nasional, dan multinasional.

3.1.1 Struktur Organisasi PT XYZ

Berikut pada Gambar 3.1 merupakan struktur organisasi pada PT XYZ yang menunjukan urutan departemen perusahaan beserta nama jabatan untuk setiap pimpinannya.



Gambar 3. 1 Struktur Organisasi pada PT XYZ
Sumber: Narasumber

Berdasarkan Gambar 3.1 struktur organisasi tersebut, PT XYZ dipimpin oleh seorang Presiden Komisaris yang memiliki tugas untuk melakukan pengawasan atas pelaksanaan strategi perusahaan oleh masing-masing direksi departemen perusahaan. Kemudian, seorang Presiden Komisaris dalam melakukan tugas dan tanggung jawabnya dibantu oleh 3 pemangku kepentingan lainnya yaitu, Presiden Direktur yang bertugas untuk melakukan pengendalian internal dan mengelola pelaporan kepada para pemegang saham, Sekretaris Perusahaan yang bertugas sebagai penghubung antara direksi dan komisaris, dan juga Unit Audit Internal yang berwenang untuk memeriksa seluruh aktivitas di dalam perusahaan agar tetap sejalan dengan pedoman pelaksanaan perusahaan. Pada penelitian ini berfokus pada divisi pengelolaan sumber daya manusia dan teknologi informasi di perusahaan.

3.1.2 Visi dan Misi Perusahaan

a) **Visi:** Visi dari PT XYZ adalah untuk "Menjadi pilihan layanan penyediaan internet".
b) **Misi:** Misi dari PT XYZ yaitu untuk "Mengubah konsumen dengan internet berkecepatan tinggi".

3.2 Metode Penelitian

Penulisan penelitian ini menggunakan jenis penelitian kualitatif dengan mengumpulkan kebutuhan-kebutuhan PT XYZ dalam melakukan implementasi IGA serta mengumpulkan informasi terkait proses bisnis perusahaan yang berkaitan dengan manajemen siklus hidup karyawan. Pertanyaan wawancara ditanyakan kepada anggota dari divisi *human resource*, IT *Operation*, dan pemilik aplikasi target. Pendekatan kualitatif dilakukan untuk mendapatkan informasi secara deskriptif terkait alur pengelolaan karyawan saat ini Pada penelitian ini juga akan dilakukan penilaian kematangan terhadap klausul ISO 27001:2022 yang menggunakan metode *Security System Engineering Capability Maturity Model* (SSE-CMM).

Penelitian ini berfokus pada perbaikan tata kelola identitas dan akses perusahaan. Saat ini solusi dalam hal pengelolaan identitas dan akses dapat diselesaikan menggunakan solusi *Identity and Access Management* (IAM) dan juga *Identity Governance Administration* (IGA). Akan tetapi pemilihan kedua solusi tersebut perlu disesuaikan juga dengan kebutuhan perusahaan. Berikut pada Tabel 3.1 merupakan komparasi fitur antara solusi IGA dan IAM [38], [49]:

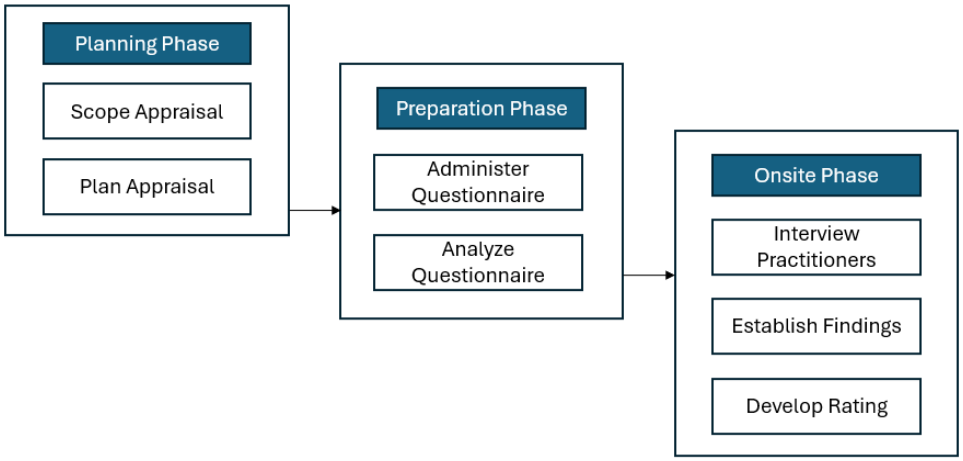
Tabel 3. 1 Komparasi fitur IGA dan IAM

Fungsi	IAM	IGA
Manajemen siklus hidup identitas	*Yes*	*Yes*
Alur automasi permintaan akses	*Yes*	*Yes*
Provisioning Akses	*Yes*	*Yes*
Single-Sign On	*Yes*	*No*
Policy Violation	*No*	*Yes*
Dokumentasi *Segregation of Duties* (SoD)	*No*	*Yes*
Sertifikasi Akses	*No*	*Yes*
Autentikasi Identitas	*Yes*	*No*
Multifactor Authentication (MFA)	*Yes*	*No*

Untuk menetapkan solusi yang lebih tepat sasaran bagi perusahaan, maka selanjutnya akan dilakukan penilaian menggunakan metode SSE-CMM berdasarkan pengelompokan kapabilitas operasional klausul ISO 27001:2022 yang berhubungan dengan IAM dan juga IGA. Hasl penilaian nantinya akan menunjukan kebutuhan perusahaan dan penentuan pemilihan solusi yang lebih tepat guna.

3.2.1 Penilaian Kematangan menggunakan SSE-CMM

Penilaian menggunakan metode SSE-CMM digunakan untuk mengetahui kondisi kematangan perusahaan saat ini terhadap klausul ISO 27001:2022 yang berhubungan dengan pengelolaan identitas dan hak akses. Berikut pada Gambar 3.2 merupakan langkah-langkah penilaian kematangan berdasarkan buku panduan penilaian SSE-CMM:



Gambar 3. 2 Langkah pada Metode SSE-CMM
Sumber: [54], [55]

Berdasarkan Gambar 3.2 dapat diperoleh langkah-langkah penilaian menggunakan metode SSE-CMM pada penelitian yang dilakukan saat ini. Langkah-langkah tersebut sudah disesuaikan dengan keadaan pada penelitian yang terdiri dari 3 bagian yaitu, tahapan perencanaann *(Planning Phase)*, tahapan persiapan *(Preparation Phase)*, dan tahapan pelaksanaan *(Onsite Phase)* dengan rincian sebagai berikut:

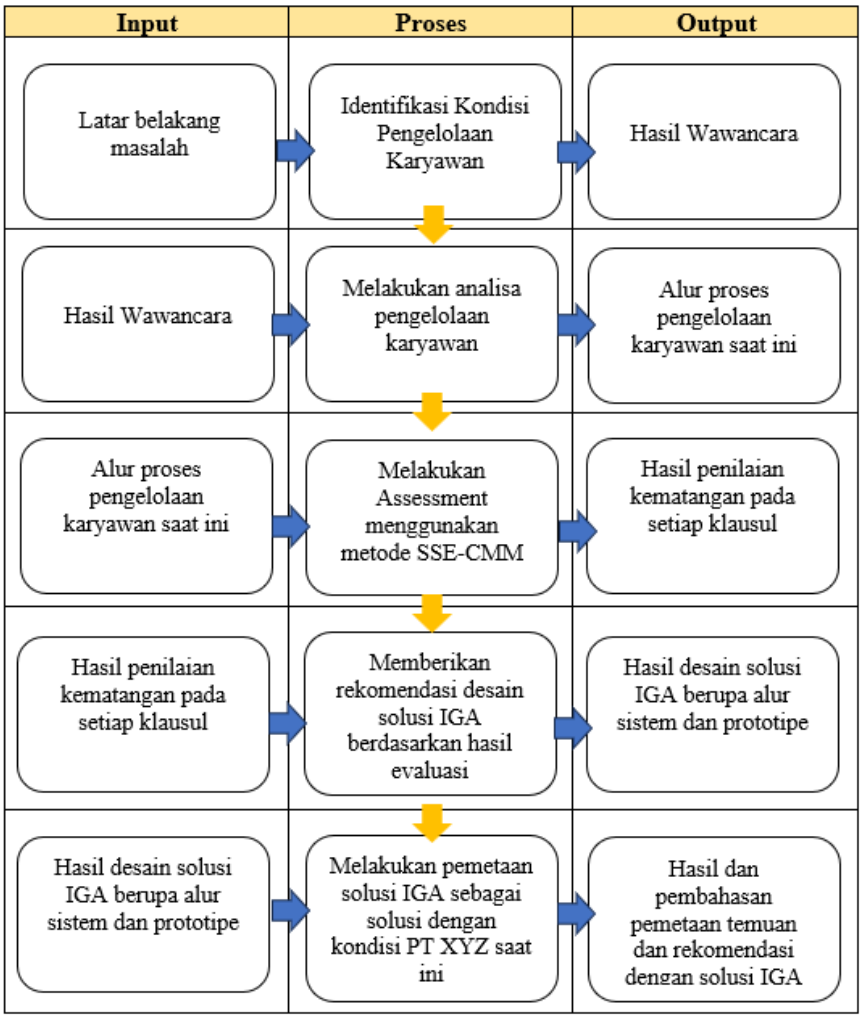
1. Tahapan perencanaan dilakukan dengan menetapkan ruang lingkup penilaian yang akan dilakukan. Pada penelitian ini ruang lingkup yang ditetapkan adalah klausul ISO 27001:2022 yang berhubungan dengan *Identity Governance Administration* (IGA) yaitu, A.5.3 tentang pemisahan tugas, A.5.15 tentang kontrol akses, A.5.16 tentang manajemen identitas, dan A.5.18 tentang hak akses.

Kemudian tahapan ini juga dilanjutkan dengan menetapkan pertemuan dengan narasumber nantinya.

2. Tahapan persiapan dilakukan dengan membuat kuesioner dan menganalisa kuesioner agar sesuai dengan tujuan penilaian yang dilakukan. Pada penelitian ini kuesioner dibuat dengan mengacu pada klausul ISO 27001:2022 yang berhubungan dengan *Identity Governance Administration* (IGA). Setiap pertanyaan dianalisa kesesuaiannya dengan *guidelines* pada dokumen ISO 27001:2022. Kemudian referensi pembuatan bentuk pertanyaan menggunakan *toolkit auditing* yang dipublikasikan oleh beberapa praktisi audit ISO 27001 [19], [56], [57]. Pembuatan pertanyaan terdiri dari 5 pertanyaan untuk masing-masing kontrol yang dievaluasi.
3. Tahapan pelaksanaan dilakukan dengan melakukan wawancara dengan praktisi berdasarkan kuesioner yang sudah dibuat. Berdasarkan penjelasan dari narasumber maka akan didapatkan keterangan yang dapat menjadi temuan-temuan sebagai bahan pemberian rekomendasi. Setelah melakukan wawancara dan mendapatkan temuan, maka dilanjutkan dengan memberikan analisa *rating* atau menentukan tingkat kematangan saat ini. Kalkulasi pada tingkat kematangan akan berdasarkan dengan skala *maturity model* yang disediakan oleh metode SSE-CMM

3.2.2 Alur Penelitian

Pada Gambar 3.3 merupakan alur penelitian yang digunakan. Alur tersebut mengacu pada penelitian yang telah dilakukan sebelumnya oleh Dimas Pramudya dkk dalam Evaluasi Tata Kelola berstandar ISO 27001:2013 menggunakan SSE-CMM dan juga penelitian yang dilakukan oleh Piski Sundari dan Wella [22] [14],



Gambar 3. 3 Alur Penelitian
Sumber: [14], [22]

Berdasarkan Gambar 3.3, berikut adalah penjelasan lebih lanjut terkait alur penelitian yang akan dilakukan:

1. Tahap pertama dilakuakan dengan melakukan identifikasi kondisi perusahaan tentang pengelolaan karyawan. Untuk mengidentifikasi kondisi dilakukan dengan melalui tahap wawancara dan akan menghasilkan hasil wawancara berupa penjelasan komprehensif tentang kondisi pengelolaan karyawan saat ini.
2. Hasil wawancara kemudian akan digambarkan ke dalam alur proses untuk memudahkan proses desain solusi yang diajukan.

3. Kemudian, dilakukan penilaian kematangan perusahaan menggunakan klausul Annex-A pada ISO 27001:2022 yang berhubungan dengan IGA. Metode penilaian akan menggunakan metode SSE-CMM untuk memudahkan evaluasi terhadap keadaan perusahaan. Metode SSE-CMM memiliki kategori untuk setiap level yang menjadi gambaran untuk kondisi perusahaan saat ini jika dilihat dari sisi keamanan informasi. Hasil dari penilaian yang dilakukan akan menunjukkan skor dan level kematangan perusahaan saat ini. Tahapan yang dilalui pada saat melakukan *maturity assessment* akan mengacu pada langkah-langkah melakukan penilaian menggunakan metode SSE-CMM.
4. Hasil penilaian kematangan menggunakan ISO 27001:2022 dan syarat pengembangan solusi akan digunakan sebagai dasar dalam membuat rekomendasi solusi IGA untuk PT XYZ. Hasil perancangan akan berupa UML yang menggambarkan alur sistem dan rancangan desain UI menggunakan Figma. Perancangan sistem dan desain UI akan berdasarkan fitur dan *flow* dasar dari *tools* yang dipakai yaitu, SailPoint.
5. Setelah melakukan perancangan solusi IGA, maka kemudian hasil rancangan akan dipetakan dengan hasil temuan pada *assessment* klausul Annex-A ISO 27001:2022. Hal ini bertujuan agar mengetahui bagaimana solusi IGA dapat memperbaiki kondisi perusahaan.
6. Hasil akhir desain solusi IGA akhirnya akan dipetakan dengan kebutuhan perusahaan dan klausul Annex-A ISO 27001:2022 yang berkaitan dengan tata kelola akses.

3.3 Teknik Pengumpulan Data

Pengumpulan data dilakukan dengan melakukan wawancara untuk mendapatkan informasi mendalam terkait permasalahan yang dialami oleh PT XYZ. Hal ini dilakukan karena informasi yang diperoleh lebih deskriptif dan

pemilik aplikasi bisa saling melengkapi informasi satu sama lain. Pemilihan narasumber berdasarkan keterlibatannya dalam pengelolaan akses karyawan.

Wawancara dilakukan bersama dengan 6 orang narasumber yang terdiri dari 1 orang staff divisi HR, 2 orang divisi IT *Operation*, 2 orang pemilik aplikasi target, dan *Project Manager* PT XYZ. Pertanyaan yang diberikan seputar dengan proses pengelolaan karyawan sehari-hari untuk mengetahui alur keseluruhan dan melengkapi analisa penilaian kematangan nantinya. Hasil wawancara akan digunakan sebagai dasar pengembangan solusi IGA yang akan tetap mengikuti beberapa proses yang masih dilakukan oleh perusahaan saat ini. Tim HR dilibatkan sebagai narasumber untuk menjelaskan prosedur perekrutan, tim IT *Operation* untuk menjelaskan bagaimana sistem pemberian akses dan pembuatan akun yang ada saat ini, dan pemilik aplikasi berkontribusi untuk menyediakan informasi syarat integrasi sistem IGA ke aplikasi yang dituju.

Pengumpulan data juga dilakukan dengan melakukan wawancara lanjutan kepada manajer IT *Operation* untuk menjawab pertanyaan pada *maturity assessment* untuk mengukur tingkat kematangan perusahaan saat ini terhadap klausul ISO 27001 yang berhubungan dengan IGA. Manajer IT *Operation* memiliki visibilitas terhadap pengelolaan karyawan oleh HR dan penyediaan akses oleh anggota timnya, dan juga memiliki wewenang sebagai *decision maker* sehinggga beliau dipilih sebagai narasumber utama dalam pengisian *assessment*.

3.4 Periode Pengambilan Data

Pengambilan data dilakukan di pertengahan bulan Agustus 2023 karena sejalan dengan kebutuhan PT XYZ untuk melakukan implementasi IGA di tahun tersebut untuk memenuhi kebutuhan audit dan sertifikasi ISO 27001 mendatang.

3.5 Teknik Analisis Data

Tingkat kematangan keamanan informasi suatu organisasi dapat dihitung menggunakan skala pada *maturity model.* Dalam melakukan evaluasi nilai

kematangan tata kelola identitas pada PT XYZ menggunakan metode SSE-CMM, di mana metode tersebut merupakan metode yang pada umumnya dipakai ketika akan melakukan penilaian atas suatu standar keamanan seperti ISO 27001 [57].

Hasil wawancara yang dilakukan dengan memperhatikan klausul pada Annex-A ISO 27001:2022 untuk kemudian jawaban dari narasumber dimasukkan ke dalam skala penilaian SSE-CMM yang terdiri 6 tingkat kematangan. Adapun klausul Annex-A yang dijadikan sebagai bahan evaluasi adalah klausul yang berkaitan dengan kontrol identitas dan kontrol akses yang menjadi dasar untuk memberikan rekomendasi dalam bentuk alur sistem solusi IGA.

Setiap pertanyaan *assessment* yang diajukan akan diberikan nilai berdasarkan penjelasan dari narasumber terkait dan kemudian dicocokan berdasarkan kriteria penilaian indeks kematangan dari level 0-6. Kemudian seluruh penilaian yang sudah diberikan pada setiap pertanyaan akan dijumlahkan dan didapatkan nilai rata-rata [19]. Kemudian nilai rata-rata tersebut akan kembali dicocokan dengan indeks kematangan untuk mengetahui tingkat kematangan perusahaan dan menentukan langkah perbaikan solusi IGA selanjutnya.

Dalam melakukan identifikasi kematangan sistem dari suatu organisasi, SSE-CMM memiliki 6 level kapabilitas yang dapat digunakan untuk melakukan evaluasi kematangan sistem pada organisasi. Berikut pada Tabel 3.2 merupakan kriteria indeks kematangan SSE-CMM yang menjadi standar pengelompokan penilaian:

Tabel 3. 2 Indeks Kematangan SSE-CMM

Range	Keterangan
0.00 – 0.50	Non-Existent
0.51 – 1.50	Initial/Ad Hoc
1.51 – 2.50	Repeatable but Intuitive
2.51 – 3.50	Define Process
3.51 – 4.50	Managed and Measurable
4.51 – 5.00	Optimized

Setiap *range* penilaian kematangan yang ada pada Tabel 3.2 merupakan tingkatan atau level yang digunakan pada metode SSE-CMM. Berikut adalah kriteria penilaian dari setiap tingkatan:

1. Tingkat 0 – *Non-Existent*

   Ketika organisasi tidak melakukan praktek dasar yang telah ditentukan dari standar kamanan. Hal ini dapat dilihat ketika organisasi tersebut tidak mengimplementasikan suatu standar keamanan baik itu secara formal maupun informal, serta belum memiliki rencana untuk mengimplementasikannya. Perusahaan juga belum merasa bahwa hal tersebut merupakan permasalahan yang perlu diselesaikan.
2. Tingkat 1 – *Initial / Ad Hoc*

   Organisasi telah melakukan praktek dasar dari standar keamanan, akan tetapi masih dilakukan secara informal karena belum memiliki dokumentasi yang resmi, tidak memiliki standar operasi resmi, dan dilakukan masing-masing secara terpisah.
3. Tingkat 2 – *Repeatable but Intuitive*

   Organisasi telah memiliki langkah dalam melakukan proses, akan tetapi aturan dalam melakukan proses masih belum terdokumentasi dan proses masih dilakukan secara informal. Tanggung jawab bagi individu belum terdefinisi karena masih bergantung dengan kesadaran satu sama lain saja.
4. Tingkat 3 – *Define Process*

   Organisasi telah menjalankan proses keamanan yang sesuai dengan standar keamanan yang digunakan. Peraturan sudah ada secara formal dan sudah dilakukan pelatihan juga bagi seluruh anggota organisasi, akan tetapi dalam tahap ini organisasi tidak dapat mendeteksi penyimpangan pada proses yang dilakukan karena prosedur hanya merupakan formalitas.
5. Tingkat 4 – *Managed and Measurable*

Telah memiliki sistem monitoring untuk proses yang dilakukan sehingga semuanya dapat dikendalikan akan tetapi masih dalam keterbatasan perangkat pendukung. Perusahaan sudah dapat mengukur aktivitas pada proses secara kuantitatif untuk dapat memperoleh informasi apakah proses dilakukan secara efektif.

6. Tingkat 5 – *Optimized*

   Standar keamanan sudah diimplementasikan dengan adanya proses yang otomatis. Pada tingkatan ini kemudian juga dilakukan penilaian apakah organisasi sudah memiliki dokumentasi yang lengkap, standar operasi yang formal dan sudah diketahui oleh seluruh anggota. Pada tahap ini organisasi juga sudah siap untuk perbaikan secara terus menerus. Sudah memiliki teknologi informasi yang dapat mengautomasi alur kerja agar pekerjaan lebih efektif dan efisien.

Perhitungan kematangan akan berdasarkan kuesioner yang diberikan kepada responden, yaitu masing-masing pertanyaan akan diberikan penilaian berdasarkan kriteria yang ada pada metode SSE-CMM seperti pada Tabel 2.4. Kemudian dari seluruh penilaian yang diberikan untuk masing-masing pertanyaan akan diambil nilai rata-rata dengan menjumlahkan seluruh nilai yang didapat dengan jumlah pertanyaan yang diberikan. Penilaian yang diberikan pada setiap pertanyaan untuk evaluasi kematangan diberikan oleh *interviewer* berdasarkan informasi lapangan yang dijelaskan oleh narasumber. Jawaban yang diberikan oleh narasumber perlu dianalisa berdasarkan indeks kematangan SSE-CMM sehingga dapat dicocokan antara kondisi perusahaan saat ini dengan indeks.