BAB II
LANDASAN TEORI

2.1 Penelitian Terdahulu

Terdapat penelitian terdahulu yang digunakan sebagai sumber referensi untuk mendukung pengerjaan penelitian ini. Berikut pada Tabel 2.1 adalah penelitian terdahulu yang digunakan, antara lain:

Tabel 2. 1 Penelitian Terdahulu

Penelitian terdahulu 1 [12]	
Judul	*Integration of Identity Governance and Management Framework within Universities for Privileged Users*
Nama Penulis	Shadma Parveen, Sultan Ahmad dan Mohammad Ahmar Khan
Nama Jurnal/Tahun	(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 12, No. 6, (2021)
Permasalahan	Mengendalikan pencurian data dan juga hak akses yang tidak terotorisasi di dalam perusahaan. Tujuan penelitian ingin memperjelas bahwa manajemen dan tata kelola identitas adalah representasi keamanan siber yang baik.
Metode	*Identity Access Management* (IAM) dan *Priviledge Access Management* (PAM)
Pembahasan	Membahas fungsi manajemen identitas untuk melakukan pengelolaan identitas. Membahas fungsi SailPoint sebagai platform yang mampu menangani manajemen akses, manajemen identitas, dan permintaan akses.
Penelitian Terdahulu 2 [16]	
Judul	*Usability And Privacy in Academic Libraries: Regaining A Foothold Through Identity and Access Management*
Nama Penulis	Ishaq Azhar Mohammed
Nama Jurnal/Tahun	International Journal of Innovations in Engineering Research and Technology [IJIERT], Vol 7 (2020)

Permasalahan	Perpustakaan di suatu universitas ingin meningkatkan keamanan dalam hal pengelolaan identitas penggunanya karena sistem perpustakaan yang terhubung dengan banyak aplikasi *third-party.*
Metode	*Identity Access Management* (IAM).
Pembahasan	Ketika pengguna mengakses sistem perpustakaan terdapat potensi untuk informasi pengguna tersebut dimanfaatkan atau digunakan oleh pihak yang tidak terotorisasi. Dalam hal ini IAM digunakan untuk menyelesaikan akses yang tidak terotorisasi. Dalam rencana pengembangan IAM, terdapat 3 hal yang menjadi dasar yaitu, *provisionning*, *de-provisionning*, dan perubahan data pengguna.
Penelitian Terdahulu 3 [13]	
Judul	*SOA Approach - Identity and Access Management for the Risk Management Platform.*
Nama Penulis	Jovana Petrovska, Agon Memeti, Florinda Imeri
Nama Jurnal/Tahun	Mediterranean Conference on Embedded Computing (2019)
Permasalahan	Ingin meningkatkan sistem manajemen risiko yang ada dengan menggunakan pendekatan *Service-oriented architecture* dengan memanfaatkan solusi *Identity Accesss Management* (IAM).
Metode	Menggunakan *tools "Oracle Identity Manager* (OIM)" untuk mengembangkan solusi IAM, menggunakan pendekatan *Identity Management* untuk solusi IAM
Pembahasan	Dalam mengembangkan IAM, memperhatikan seluruh aspek *Identity Management* yaitu, autentikasi, otorisasi, kerahasiaan, akuntabilitas, dan keaslian. OIM digunakan untuk mengatur siklus identitas yang juga dapat memenuhi tata kelola identitas, manajemen akses, dan servis direktori. Hasil penelitian berupa konsep solusi dan rekomendasi untuk memenuhi syarat implementasi.
Penelitian Terdahulu 4 [17]	
Judul	Introduction to IAM Architecture (v2)
Nama Penulis	Andrew Cameron dan Graham Williamson
Nama Jurnal/Tahun	IDPro Body of Knowledge, Vol. 1 (2021)

Permasalahan	Menganalisa komponen IAM yang berguna untuk meningkatkan efisiensi dan keamanan pada bagian *IT Operation.*
Metode	IAM dan IGA dari sisi arsitektural desain.
Pembahasan	IGA merupakan bagian dari IAM yang berfokus pada *Identity Management* (IdM) yang dikombinasikan dengan tata kelola administrasi identitas. IGA menyediakan fungsi tambahan di luar IAM, yaitu dokumentasi pelaporan yang dapat membantu proses audit.
Penelitian Terdahulu 5 [18]	
Judul	Strategic Alignment and Access Governance
Nama Penulis	Andre Koot
Nama Jurnal/Tahun	IDPro Body of Knowledge, Vol. 1 (2022)
Permasalahan	Ketidaksesuaian antara manajemen akses dengan proses bisnis perusahaan menjadi penyebab terjadinya kegagalan implementasi IAM dan dapat menghambat pertumbuhan bisnis.
Metode	IAM
Pembahasan	Pada pengelolaan akses, HR bertanggung jawab untuk mengelola transaksi identitas sedangkan manajemen identitas dikelola oleh tim IT. Projek IAM akan sukses jika sejalan dengan proses bisnis perusahaan. *Segregation of Duites* (SoD) menjadi objek penting untuk proses bisnis perusahaan dalam hal tata kelola akses.
Penelitian Terdahulu 6 [19]	
Judul	Evaluasi Keamanan Informasi Data Center Berdasarkan Standar ISO 27001:2013 (Studi Kasus PT. Pupuk Kalimantan Timur)
Nama Penulis	Faza Ainun Nafisah, dkk.
Nama Jurnal/Tahun	Jurnal Teknologi Informasi dan Ilmu Komputer Vol. 4, No. 6, Juni (2020)
Permasalahan	Melakukan pengamanan terhadap *data center* milik PT Pupuk Kalimantan Timur yang akan melakukan sertifikasi ISO 27001
Metode	SSE-CMM, ISO 27001:2013

Pembahasan	Melakukan penilaian terhadap keamanan *data center*. Rekomendasi diberikan berdasarkan hasil penilaian kematangan yang dilakukan terhadap klausul ISO 27001:2013. Rekomendasi diberikan untuk memperbaiki kondisi perusahaan yang akan mengikuti sertifikasi ISO 27001:2013.
Penelitian Terdahulu 7 [20]	
Judul	*The Use of ISO 27001 Framework for Government's Online E-Monitoring System Implementation*
Nama Penulis	Pini Singgrit, Geraldi Catur Pamuji
Nama Jurnal/Tahun	International Journal of Education, Information Technology and Others (IJEIT), Vol. 3 (2020)
Permasalahan	Ingin mengetahui tingkat keamanan pada Sistem online monitoring pada pemerintahan di Karawang apakah sudah merepresentasikan manajemen keamanan informasi.
Metode	Menggunakan siklus PDCA dan menggunakan klausul Annex-A ISO 27001:2013 poin A 11.3 dan A 11.3 sebagai dasar penilaian.
Pembahasan	Kontrol A 11.2 dan 11.3 pada Annex-A ISO 27001:2013 dipilih karena berkaitan dengan keamanan tata kelola informasi, yaitu sesuai dengan tujuan penelitian. Berdasarkan kuesioner yang diisi oleh para pemimpin dan anggota, monitoring *online* pada pemerintah Karawang masih kurang aman karena penilaian evaluasi yang masih di bawah 64%.
Penelitian Terdahulu 8 [21]	
Judul	*Analysis of System Security Levels of Tax Payment and Regional Retribution Based on ISO / IEC27002:2013 Standard Using SSE-CCM*
Nama Penulis	Aburizal Rosadi, Bheta Agus Wardijono
Nama Jurnal/Tahun	International Research Journal of Advanced Engineering and Science, Vol. 6 (2021)
Permasalahan	Sistem pembayaran pajak yang memiliki aktivitas transaksional pajak di dalamnya sejauh ini belum pernah melakukan evaluasi kematangan keamanan sistem informasi.
Metode	ISO 27002, Annex-A *Control* 9, 10, 12, 16, metode perhitungan SSE-CMM.
Pembahasan	Peneliti memilih 4 kontrol Annex berdasarkan kebutuhan pembahasan pada penelitian, yaitu hanya yang berkaitan dengan keamanan akses, yaitu klausul 9, klausul 10, klausul 12, dan klausul 16. Dari penilaian yang sudah

	dilakukan, kemudian terdapat *gap* penilaian dan *gap* tersebut digunakan sebagai dasar pemberian rekomendasi.
Penelitian Terdahulu 9 [22]	
Judul	Evaluasi Tata Kelola Keamanan Informasi Berdasarkan Standar ISO/IEC 27001:2013 dengan Menggunakan Model SSE-CMM *(System Security Engineering Capability Maturity Model)* pada Perusahaan Daerah Air Minum Surya Sembada Kota Surabaya
Nama Penulis	Dimas Pramudya Haqqi, Khakim Ghozali, dan Raden Venantius Hari Ginardi
Nama Jurnal/Tahun	Jurnal Teknik ITS, Vol. 11 (2022)
Permasalahan	Menganalisa kemampuan tata kelola keamanan informasi untuk objek yang diteliti.
Metode	SSE-CMM, ISO 27001:2013
Pembahasan	Melakukan penilaian kematangan dengan fokus terhadap 4 klausul, yaitu A.9 Kontrol Akses, A.11 Keamanan Fisik dan Lingkungan, A.12 Keamanan operasi, A.16 Pengelolaan Insiden Keamanan Informasi. Memberikan pertanyaan *assessment* dengan mengacu pada ISO 27001:2013. Mendapatkan *gap* berdasarkan perhitungan menggunakan SSE-CMM
Penelitian Terdahulu 10 [23]	
Judul	*Maturity Framework Analysis ISO 27001: 2013 on Indonesian Higher Education*
Nama Penulis	IGN Mantra, Aedah Abd. Rahman, Hoga Saragih
Nama Jurnal/Tahun	International Journal of Engineering & Technology, Vol. 9 (2020)
Permasalahan	Keamanan Sistem Informasi akademik yang cukup rawan pada masa Covid-19 karena seluruh kegiatan akademik yang dilakukan secara daring. *Gap* pada keamanan sistem informasi dapat menjadi celah kejahatan siber.
Metode	ISO 27001:2013, SSE-CMM
Pembahasan	Perhitungan kematangan dilakukan dari klausul A.5 hingga A.18. Hasil dari pembahasan adalah memberikan informasi *gap* dari hasil penilaian sebagai dasar pemberian rekomendasi.

Tabel 2.1 merupakan daftar penelitian terdahulu yang masing-masing memiliki hubungan dan juga menjadi dasar referensi utama dalam melakukan penelitian ini. IAM dan PAM dapat digunakan untuk mengendalikan pencurian data dan juga otorisasi hak akses. Melalui kedua solusi yang digunakan, diperoleh kesimpulan bahwa fungsi manajemen identitas dapat mewujudkan tata kelola kelola identitas yang efisien dan terautomasi. Kemudian salah satu referensi *tools* yang dapat digunakan untuk manajemen identitas adalah SailPoint [12]. Kemudian risiko pada keamanan akun pengguna juga dapat terancam apabila akun pengguna terhubung dengan beberapa aplikasi *third-party.* Dalam penelitian tersebut, IAM digunakan untuk menyelesaikan pengelolaan akses melalui 3 fitur dasar, yaitu *provisioning, de-provisioning,* dan perubahan data pengguna [16]. Pada penelitian terdahulu ketiga, membahas tentang pengembangan solusi IAM untuk *platform* manajemen risiko di perusahaan. Pengembangan solusi menggunakan *tools* Oracle Identity Manager (OIM). Hasil penelitian berupa syarat implementasi bagi perusahaan dan menunjukkan bahwa OIM dapat digunakan untuk mengatur siklus identitas yang juga dapat memenuhi tata kelola identitas, manajemen akses, dan servis direktori [13]. Terdapat keterkaitan antara IAM dan IGA, yaitu IGA merupakan bagian dari IAM yang berperan penting untuk mengelola identitas (IdM) dan juga tata kelola administrasi identitas pengguna [17]. Kemudian, untuk mewujudkan implementasi manajemen akses anggota perusahaan, maka diperlukan tugas tim HR untuk mengelola karyawan dan tim IT untuk menjalankan fungsi manajemen identitas. Kesesuaian manajemen akses dengan bisnis proses dapat dijalankan dengan baik apabila perusahaan menerapkan *Segregation of Duties* (SoD) [18].

Melalui kelima penelitian terdahulu yang berkaitan dengan IAM, penelitian tersebut digunakan sebagai dasar pengembangan solusi IGA pada penelitian ini. IGA merupakan bagian dari IAM yang berfokus pada tata kelola identitas manajemen akses, dan administrasi tata kelola identitas. Terdapat perbedaan antara lima penelitian terdahulu dengan penelitian yang saat ini sebagai kebaruan yang dilakukan yaitu, identitas karyawan yang terhubung dengan beberapa aplikasi

perusahaan akan diselesaikan menggunakan solusi IGA pada penelitian ini. Kemudian, *tools* yang akan digunakan pada untuk pengembangan solusi IGA pada penelitian ini akan menggunakan *SailPoint* dan berfokus pada fitur *provisioning* akses, *deprovisioning* akses, permintaan hak akses, dokumentasi pembuatan/pencabutan akses. Penelitian [17] akan digunakan sebagai dasar pemisahan antara fungsi IAM dan IGA.

Selanjutnya adalah penelitian terdahulu yang berkaitan dengan pengukuran tingkat kematangan organisasi yang berdaasarkan ISO 27001 menggunakan metode *Security System Engineering Capability Maturity Model* (SSE-CMM). Evaluasi Keamanan Informasi dapat dilakukan menggunakan metode SSE-CMM dengan ISO 27001:2013 sebagai dasar. Metode SSE-CMM membantu peneliti untuk mengevaluasi keadaan *data center* sehingga mempermudah proses pemberian rekomendasi [19]. Pada penelitian [19], evaluasi kematangan dilakukan dengan menetapkan 2-3 pertanyaan untuk masing-masing sub klausul ISO 27001:2013 dan kemudian skor diberikan berdasarkan indeks SSE-CMM. Kemudian, untuk memilih fokus evaluasi menjadi lebih terarah sesuai dengan tujuan penelitian, evaluasi pada sistem monitoring pemerintahan Karawang hanya difokuskan pada 2 poin yaitu Annex-A poin 11.2 dan 11.3 [20]. Penelitian tersebut menjadi bukti pertama bahwa kontrol ISO dapat dipilih beberapa saja untuk menjadi fokus evaluasi kematangan. Selanjutnya pada yang melakukan evaluasi akses tentang sistem perpajakan hanya dipilih 4 kontrol yang relevan yaitu, A.9, A10, A.12, dan A.16 [21]. Kemudian, pemilihan objek kontrol untuk melakukan evaluasi kematangan juga dapat difokuskan pada kontrol keamanan informasi yang ingin diimplementasikan saja, yaitu seperti klausul A.9. A.11, A.12, dan A.16 [22].

Penelitian [21], [22] menggunakan metode *System Security Engineering Capability Maturity Model* (SSE-CMM) dalam melakukan perhitungan kematangan untuk setiap kontrol yang dipilih. Perhitungan *gap* yang didapatkan berasal dari sejumlah pertanyaan berdasarkan kontrol ISO 27001, kemudian dihitung rata-ratanya dan dikelompokkan berdasarkan indeks kematangan SSE-CMM. *Gap* dihasilkan dari nilai maksimal, yaitu 5 dengan nilai rata-rata yang saat

itu didapatkan. Kemudian, rekomendasi perbaikan perlu diberikan agar perusahaan dapat mengisi *gap* yang ditemukan saat penilaian kematangan dilakukan [23]. Melalui seluruh penelitian terdahulu tentang evaluasi tingkat kematangan, terdapat perbedaan yang juga menjadi kebaruan dalam penelitian ini, yaitu perbedaan pada klausul yang dianalisa dan hasil rekomendasi yang akan diberikan.

Pada penelitian ini, metode SSE-CMM digunakan untuk menilai apakah perusahaan sudah melakukan praktek tata kelola identitas dengan baik. Berdasarkan *gap* yang diperoleh, maka akan lebih mudah untuk memberikan rekomendasi solusi IGA dengan fitur-fitur yang dapat mengisi *gap* tersebut. Kontrol ISO 27001:2022 yang dipilih pada penelitian ini hanya yang berfokus pada *Identity Governance Administration* (IGA).

2.2 Keamanan Informasi

Keamanan informasi merupakan usaha untuk melindungi perangkat komputer maupun bukan komputer seperti fasilitas pengelolaan data serta informasi perusahaan agar tidak tidak disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab [24]. Keamanan informasi Memiliki 3 tujuan utama yang perlu dicapai oleh organisasi, yaitu:

Gambar 2. 1 Konsep CIA-Triad
Sumber: [25]

Pada Gambar 2.1 merupakan 3 pilar utama dalam keamanan informasi yang meliputi kerahasiaan *(Confidentiality)* yaitu tentang suatu sumber yang hanya dapat diakses oleh pengguna yang diizinkan, kemudian terdapat nilai Integritas *(Integrity)* yaitu jaminan keaslian penggunaan data, dan Ketersediaan *(Availability)* tentang sumber informasi yang selalu dapat digunakan oleh anggota organisasi [25].

Keamanan informasi yang digunakan pada umumnya mencakup beberapa bagian penting. Berikut adalah jenis-jenis keamanan informasi [26]:

1. Keamanan fisik

   Mencakup strategi organisasi untuk melakukan pengamanan aset fisik dari berbagai kejahatan seperti spionase, pencurian data, dan kerusakan data.
2. Keamanan jaringan

   Merupakan persyaratan kritikal yang perlu diperhatikan agar meminimalisir dan mencegah adanya serangan siber dari akses yang tidak terotorisasi ke data-data sensitif organisasi. Hal ini dapat direalisasikan melalui implementasi *firewall* atau *Virtual Private Network* (VPN) [27].
3. Keamanan pribadi

   Berhubungan dengan anggota organisasi atau karyawan yang mengakses informasi perusahaan secara langsung. Perlu dipastikan bahwa akses anggota terhadap suatu sumber tidak digunakan oleh piihak yang tidak bertanggung jawab. Hal ini dapat direalisasikan melalui adanya *Non-Disclosure Agreement* (NDA) yang mengikat pada setiap anggota dan juga pengamanan perangkat yang digunakan.
4. Keamanan operasional

   Merupakan strategi pengamanan yang berhubungan dengan kegiatan operasional sehari-hari dari anggota organisasi. Hal ini dapat direalisasikan dengan pengolahan informasi hanya dapat digunakan melalui perangkat yang disediakan oleh perusahaan dan pembatasan pada instalasi *software.*

5. Keamanan Identitas dan Akses

   Pada keamanan identitas, organisasi perlu memastikan bahwa setiap sumber informasi atau aplikasi hanya dapat diakses oleh anggota yang memiliki akun. Kemudian akun tersebut adalah yang terdaftar dan memiliki pemilik serta dapat diverifikasi [28].

Upaya mengedepankan keamanan informasi juga telah direalisasikan melalui peraturan untuk kontrol akses pada pemegang dan pemeberi hak akses. Di Indonesia terdapat peraturan manajamen akses yang juga menjadi standar bagi perusahaan yaitu, Peraturan Otoritas Jasa Keuangan Nomor 4/POJK.05/2021 Tahun 2021 Tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi Oleh Lembaga Jasa Keuangan Nonbank. Pada pasal 26 huruf a dan b, yang mengharuskan instansi untuk mengendalikan hak akses dan aplikasi yang digunakan dalam rangka penyelenggaraan Teknologi Informasi di dalam instansi. Selain itu instansi juga perlu memastikan bahwa Teknologi Informasi yang rahasia hanya dapat diakses oleh pihak yang telah terotorisasi.

Selain itu, terdapat Peraturan Menteri Badan Usaha Milik Negara Nomor Per-03/MBU/02/2018 pasal 5. Pada Tahapan Layanan Operasi poin 6, menyatakan kewajiban instansi untuk melakukan manajemen akses yaitu dengan membatasi akses antar pengguna. Untuk dapat mewujudkan hal ini, maka instansi perlu mengimplementasikan sistem untuk melakukan identifikasi pengguna yang berwenang dan yang tidak berwenang.

2.3 *Employee Lifecycle* (ELC)

Setiap organisasi atau perusahaan pasti memiliki alur masuk dan keluarnya anggota, hal ini akan dialami baik oleh perusahaan kecil maupun besar. Adapun proses tersebut mencakup rekrutmen karyawan baru *(hiring),* perubahan status atau pekerjaan pada karyawan, dan berakhirnya masa kerja karyawan tersebut di dalam perusahaan [29]. Seluruh proses yang berkaitan dengan masuk dan keluarnya karyawan disebut sebagai *Employee Lifecycle* atau siklus hidup karyawan.

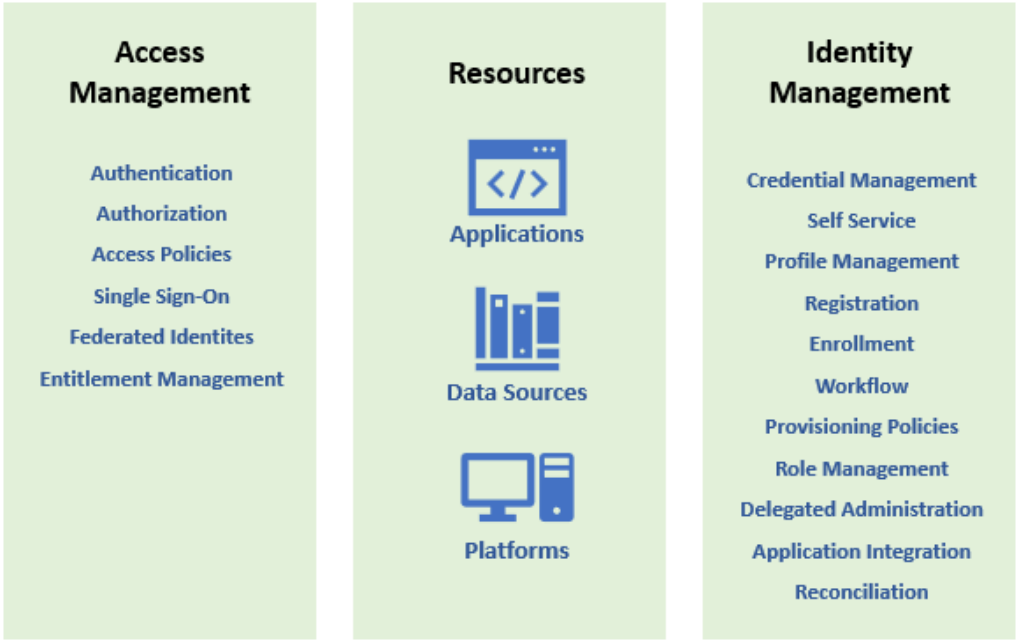
Siklus hidup karyawan pertama-tama akan di mulai dari proses rekrutmen yaitu, divisi *Human Resource* (HR) akan memasukkan informasi karyawan yang baru masuk ke dalam *database* karyawan atau yang biasa di sebut sebagai *trusted source.* Kemudian setelah karyawan itu masuk ke dalam perusahaan, maka akan diberikan akses terhadap informasi dan aplikasi perusahaan untuk menunjang tugas dan tanggung jawab sebagai karyawan di dalam perusahaan [30].

Siklus hidup karyawan selanjutnya adalah ketika karyawan itu mengalami perubahan status di dalam perusahaan. Perubahan status itu dapat disebabkan oleh promosi jabatan, perpindahan lokasi kerja, dan perpindahan divisi. Pada siklus ini HR bertanggung jawab untuk memperbarui informasi karyawan pada *trusted source* untuk menjaga keabsahan informasi karyawan.

Kemudian siklus hidup karyawan akan berakhir saat karyawan tersebut keluar dari perusahaan. Hal ini terjadi ketika karyawan *resign* atau pensiun. Pada tahap ini, HR bertanggung jawab untuk menghapus data karyawan dari *trusted source* karena karyawan tersebut sudah tidak menjadi bagian dari perusahaan.

2.4 *Identity and Access Management* (IAM)

Identity and Access Management (IAM) merupakan serangkaian proses yang terdiri dari verifikasi identitas seseorang untuk mengakses suatu sumber informasi. IAM didefinisikan sebagai sebuah kerangka kerja atau *framework* karena di dalamnya mencakup prosedur, kebijakan, sera teknologi untuk melakukan pengelolaan terhadap identitas [31]. Sistem IAM digunakan untuk memastikan bahwa setiap orang hanya dapat mengakses apa yang menjadi haknya saja. IAM terdiri dari 2 fungsi utama yaitu, *Identity Management* (IdM) dan *Access Management* (AM) [17] [31] seperti pada Gambar 2.2 berikut,



Gambar 2. 2 Komponen IAM
Sumber: [32]

IdM memiliki tugas utama untuk memberikan izin akses kepada pengguna sedangkan AM bertugas untuk melakukan autentikasi dan otorisasi informasi pengguna agar diberikan akses.

Terdapat 4 fitur utama yang yang disediakan oleh IAM, yaitu otorisasi pengguna (pemberian izin untuk mengakses suatu sumber), autentikasi (melakukan validasi identitas), dan manajemen pengguna yang mencakup pengelolaan akses pengguna berdasarkan *role* atau kedudukannya [33]. Fitur tersebut kemudian didukung oleh 4 pilar utama pada *framework* IAM yang membuat organisasi dapat menggunakan fitur-fitur IAM secara terpisah sesuai dengan kebutuhan. Berikut adalah 4 pilar utama pada IAM [34] [35]:

1. *Identity Governance Administration* (IGA) yang berfokus pada sinkronisasi identitas pengguna dengan akses yang diberikan terhadap pengguna tersebut. IGA membantu organisasi untuk memiliki visibilitas yang tersentralisasi tentang akses apa saja yang dimiliki oleh seluruh anggotanya. Fitur utama dari IGA adalah melakukan *"Provisioning"* dan *"Deprovisioning"* akses. Di mana *provisioning* adalah proses

memberikan hak akses sedangkan *deprovisioning* adalah mencabut atau menghilangkan akses yang dimiliki.

2. *Access Management* (AM) merupakan komponen IAM yang berfokus pada manajemen akses anggota organisasi terhadap aplikasi, data, dan sistem. AM berisi sekumpulan peraturan untuk pengaturan akses pemberian akses.
3. *Privileged Access Management* (PAM) yang mengatur akun-akun khusus pada sebuah organisasi karena akun tersebut memiliki akses istimewa terhadap data yang sangat sensitif. PAM biasanya diimplementasikan ketika organisasi memiliki banyak jenis *"role"* sensitif
4. *Customer Identity and Access Management* (CIAM), merupakan solusi tambahan pada IAM yang berfokus pada identitas eksternal perusahaan. Perusahaan yang ingin melakukan manajemen akses dan identitas untuk anggota eksternal dapat menggunakan solusi CIAM. Contoh, perusahaan menggunakan solusi CIAM untuk mengatur akses kustomer perusahaan sedangkan menggunakan solusi IAM untuk mengatur akses karyawan perusahaan.

Berikut pada Gambar 2.3 menggambarkan pengelompokkan komponen-komponen antara IAM dan IGA. berdasarkan fiturnya masing-masing. IAM bertanggung jawab pada sisi manajemen pemberian akses melalui fungsi yang dimilikinya yaitu, autentikasi, *Single Sign-On, Multifactor Authentication,* dan otorisasi akses. Alur kerja IAM tergolong kompleks karena membutuhkan konfigurasi pada sistem keamanan *login* pengguna, sehingga lebih berfokus untuk memastikan bahwa pengguna mengakses suatu sumber dengan melewati tahapan-tahapan *login* yang sesuai dengan standar keamanan. Fitur-fitur tersebut juga tidak berhadapan dengan *user* secara langsung, akan tetapi berjalan secara *back-end.* Berbeda dengan IGA yang lebih berfokus pada alur kerja manajemen identitas.

Gambar 2. 3 Pengelompokan IAM dan IGA
Sumber: [36]

2.4.1 *Identity Governance Administration* (IGA)

Berdasarkan Gambar 2.3, *Identity Governance Administration* (IGA) merupakan bagian dari IAM yang berfokus pada pengelolaan akses seperti, manajemen siklus hidup identitas, *access review*, memberi hak akses, menarik hak akses, dan bertanggung jawab untuk memberikan dokumentasi sebagai keperluan audit. Sistem IGA merupakan kombinasi antara IdM dan tata kelola administrasi identitas *(identity governance)*. Tata kelola identitas berfokus pada sekumpulan standar proses yang terdiri dari pemisahan tanggung jawab, manajemen peran, peninjauan akses, dan pelaporan akses, sedangkan administrasi identitas berfokus pada manajemen akun beserta kredensialnya, pemberian dan pencabutan hak akses secara otomatis [37]. IGA memiliki karakteristik utama yang kemudian digunakan oleh perusahaan

saat ini sebagai bentuk ketaatan terhadap peraturan keamanan informasi. Adapun karakteristik IGA adalah sebagai berikut:

1. Alur kerja yang terautomasi untuk memberikan akses kepada pihak yang membutuhkan untuk menunjang pekerjaannya.
2. Dapat melakukan kustomisasi alur kerja otomatis untuk penyediaan dan pembatalan pada tingkat pengguna dan aplikasi.
3. Dapat diintegrasikan dengan aplikasi perusahaan yang beragam sehingga pemberian dan penarikan tersentralisasi.
4. Melakukan manajemen hak akses guna menentukan dan memverifikasi pengguna yang melakukan permintaan hak akses.

Saat ini IGA disebut sebagai salah "solusi" untuk menyelesaikan permasalahan keamanan khususnya pada manajemen identitas. Bagi perusahaan berskala besar yang memiliki ribuan anggota, sangat penting untuk memiliki solusi IGA dalam rangka meningkatkan efisiensi proses bisnis dan meningkatkan keamanan. Berikut adalah manfaat yang didapatkan ketika suatu perusahaan mengimplementasikan solusi IGA:

1. Mengurangi biaya operasional.

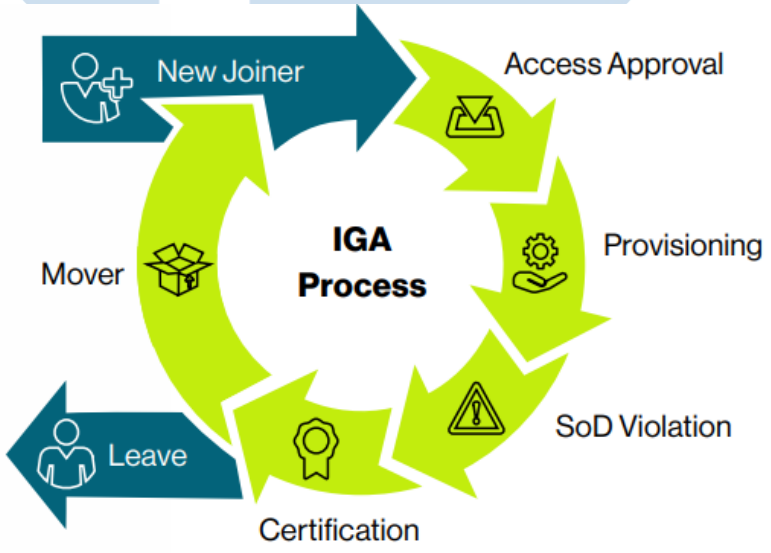
   IGA memiliki *workflow* yang terautomasi sehingga membantu perusahaan dalam mengurangi aktivitas-aktivitas manual. Hal ini tentunya membuat waktu kerja menjadi lebih efisien karena pekerjaan administratif seperti memberi akses, memberikan notifikasi akses, serta mencatat hak akses telah dilakukan melalui sistem.
2. Mengurangi risiko keamanan.

   Melalui IGA maka perusahaan dapat memiliki tampilan yang tersentralisasi untuk meninjau akses karyawannya. Melalui tampilan yang tersentralisasi maka akan lebih mudah dalam mendeteksi akses-akses yang tidak sesuai.
3. Meningkatkan ketaatan perusahaan terhadap peraturan audit.

IGA membuat proses bisnis, khususnya dalam hal pengelolaan akses menjadi lebih konsisten. Kemudian, IGA juga dapat memberikan laporan yang menyeluruh untuk keperluan auditor ketika melakukan audit terhadap perusahaan.

2.4.2 Hubungan IGA dengan Manajemen Siklus Hidup Karyawan

Pada umumnya implementasi solusi IGA pada perusahaan ditujukan untuk menyelesaikan masalah yang berkaitan dengan administrasi karyawan. IGA digunakan untuk melakukan automasi untuk pemberian, pembaruan, dan penghapusan akses pada setiap tahap *Employee Lifecycle* (ELC) agar dapat membantu tim HR dan tim IT dalam menjalankan tugas dan tanggung jawabnya. Berikut pada Gambar 2.4 menjelaskan tentang keterkaitan antata pengelolaan siklus hidup karyawan dengan sistem IGA.



Gambar 2. 4 Alur Siklus Identitas pada IGA
Sumber: [38]

Seperti sistem lainnya, IGA memulai pekerjaannya melalui data. Adapun data tersebut diperoleh dari data yang dimasukkan oleh tim HR ke dalam *database* atau yang disebut sebagai sumber terpercaya *(trusted source)*. Data yang dimasukkan oleh tim HR sendiri berupa informasi karyawan yang baru bergabung *(Joiner)*. Selanjutnya permintaan pembuatan akun untuk *new*

joiner akan diteruskan ke tahap *approval* agar proses pemberian akses dapat dilakukan. Pada siklus identitas, terdapat siklus *policy violation*, yaitu tahapan yang berfungsi untuk memastikan bahwa akses yang diberikan kepada karyawan sesuai dengan tugas dan tanggung jawabnya.

Pada siklus identitas juga terdapat proses *certification*, yaitu untuk memastikan akses yang dimiliki oleh karyawan pada periode tersebut masih relevan dengan status atau tugasnya. Kemudian, siklus selanjutnya adalah *movement*, yaitu karyawan yang berpindah divisi, lokasi, mengalami perubahan status, ataupun peran. Pada karyawan *movement* maka hak akses dan identitas karyawan perlu diperbarui dan tugas IGA adalah melakukan *provisioning* identitas karyawan yang baru ke seluruh target aplikasi nantinya. Tahapan terakhir pada siklus hidup karyawan adalah proses *resign*. Seluruh akses karyawan akan dicabut oleh sistem IGA sehingga mempermudah tim HR dan IT agar tidak perlu lagi melakukan pembersihan dan penarikan akses karyawan secara manual.

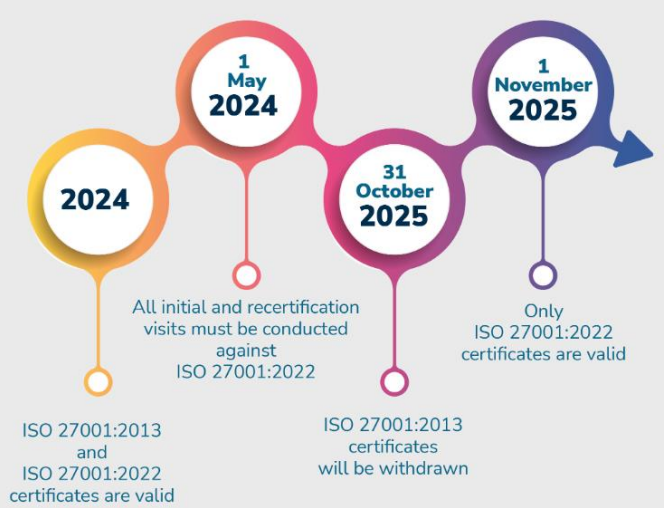
2.5 ISO 27001

ISO 27001 merupakan suatu standar keamanan sistem informasi yang digunakan untuk menilai serta mengembangkan keamanan informasi dari sebuah organisasi. Standar ISO 27001 memuat klausa-klausa yang menjadi persyaratan utama dalam melakukan pengelolaan informasi di dalam organisasi. Adapun klausa tersebut memuat hal-hal yang berkaitan dengan manajemen keamanan informasi, pihak yang bertanggung jawab dalam melakukan manajemen informasi, audit internal untuk Sistem Manajemen Keamanan Informasi (SMKI), serta berkaitan dengan perbaikan berkelanjutan yang perlu dicapai oleh organisasi [39]. ISO 27001 berfokus untuk mewujudkan *Confidentiality* (kerahasiaan), *Integrity* (Integritas), dan *Availability* (ketersediaan). ISO 27001 merupakan standar yang baik untuk digunakan dalam praktik manajemen keamanan informasi, pengelolaan risiko, dan skala perhitungan keamanan. Standar ISO 27001 berfokus untuk mengurangi risiko

dalam keamanan pengelolaan informasi dengan cara membuat manajemen sistem informasi yang dapat diperbarui secara terus menerus [40]

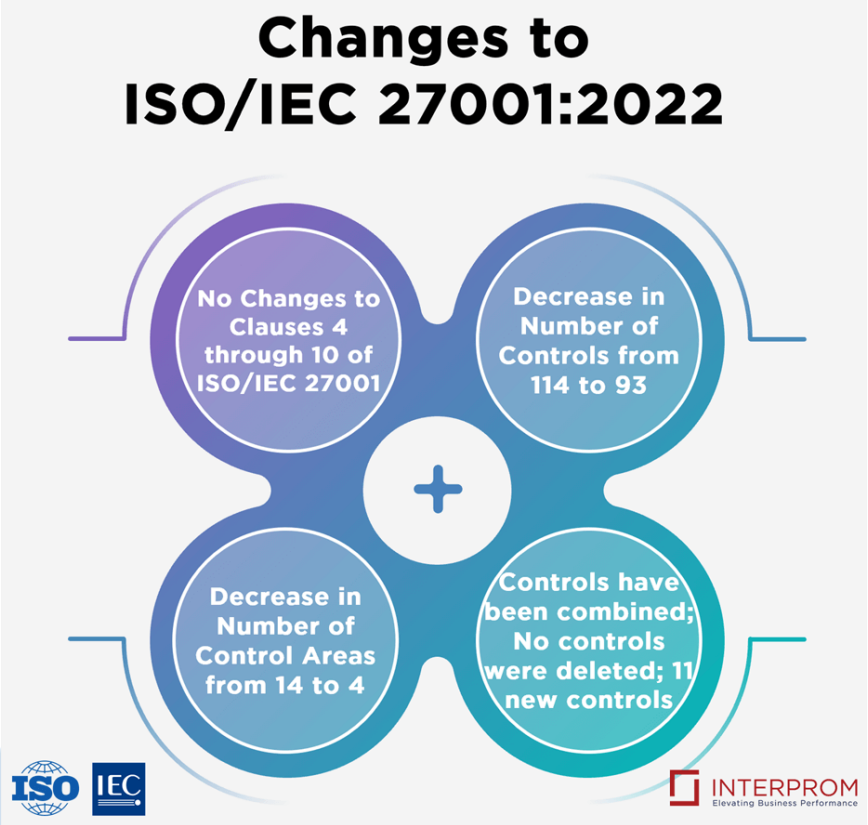
Dokumen ISO 27001 memuat sejumlah kontrol yang dapat digunakan oleh organisasi secara umum terlepas dari besarnya organisasi, tipe, ataupun sifatnya. Kontrol yang digunakan dalam ISO adalah Annex A, di mana kontrol tersebut dijelaskan secara terperinci dan terbagi sesuai dengan kategorinya dan dapat digunakan sebagai panduan untuk menganalisa kondisi keamanan informasi perusahaan. Klausa yang terdapat pada kontrol Annex A dirancang agar dapat menjadi organisasi untuk memastikan apakah aset informasi pada organisasi tersebut sudah dikelola dengan baik dalam rangka mewujudkan SMKI yang efektif [41], [42].

Sertifikasi ISO 27001:2013 masih banyak digunakan pada perusahaan saat ini, akan tetapi Pada Oktober tahun 2022 lalu, ISO/IEC 27001:2022 telah resmi dirilis dan akan menggantikan standar ISO/IEC 27001:2013. Setiap perusahaan yang sudah tersertifikasi ISO/IEC 27001:2013 dihimbau untuk memperbarui standar ISO yang digunakan hingga Oktober 2025, maka perusahaan perlu mempersiapkan diri untuk melakukan seritifikasi ISO 27001:2022 [43], [44]. Berikut pada Gambar 2.5 merupakan *timeline* untuk transisi sertifikasi ISO 27001,



Gambar 2. 5 *Timeline* Sertifikasi ISO 27001
Sumber: [45]

Adapun pada penelitian ini digunakan standar ISO 27001:2022 agar dapat memberikan rekomendasi solusi IGA yang relevan saat perusahaan hendak melakukan sertifikasi ISO 27001:2022 di waktu yang akan datang. Berikut pada Gambar 2.6 merupakan kebaruan yang ada pada ISO 27001:2022 sekaligus menunjukkan perbedaan antara ISO 27001:2013 dengan ISO 27001:2022,



Gambar 2. 6 Perubahan pada ISO 27001:2022
Sumber: [46]

Berdasarkan Gambar 2.8, pembaruan yang terdapat di ISO 27001 terletak pada jumlah kontrol Annex-A yang semula berjumlah 114 menjadi 93, jumlah kontrol yang semula berjumlah 14 menjadi berkurang menjadi 4 bagian utama. Pengurangan terhadap jumlah kontrol dikarenakan terdapat beberapa kontrol yang digabungkan menjadi satu kesatuan. Berikut pada Tabel 2.2 merupakan klausa Annex-A yang terdapat di dalam ISO 27001:2022,

Tabel 2. 2 Klausul Annex-A ISO 27001:2022

Annex	Kontrol Domain	Jumlah Kontrol
5	Kontrol Organisasi	37
6	Kontrol Sumber Daya Manusia	8
7	Kontrol Fisik	14
8	Kontrol Teknologi	34
TOTAL		**93**

Setiap klausa kontrol domain yang ada pada ISO 27001 berkaitan dengan kelompok kontrol yang ada pada ISO 27002. Pengelompokan yang digunakan dapat membantu proses evaluasi menjadi lebih terarah karena evaluasi dapat difokuskan dengan kelompok yang dipilih. Berikut pada Gambar 2.7 merupakan pengelompokan kontrol ISO 27002 berdasarkan kapabilitas operasionalnya,

Gambar 2. 7 Klausul A.5 Berdasarkan Kapabilitas Operasional

Berdasarkan Gambar 2.7 dapat diambil diambil informasi bahwa setiap kontrol memiliki kategori berdasarkan kapabilitas operasionalnya. Hal ini berfungsi untuk melihat suatu kontrol dari sisi praktik keamanan informasi. Dalam melakukan penelitian ini, diambil kontrol yang hanya berkaitan dengan *Identity Governance Administration* (IGA). Adanya keterkaitan antara IAM dan IGA, maka dalam hal evaluasi ISO 27001, digunakan kontrol area domain IAM sebagai acuan penilaian.

Kontrol organisasi dengan kabailitas operasional IAM terdiri dari beberapa klausa yang memuat panduan untuk memenuhi standar pada kontrol tersebut. Berikut pada Gambar 2.8 merupakan klausa IAM yang berhubungan dengan IGA,

Gambar 2. 8 Klausul IAM yang berkaitan dengan IGA

Berikut pada Tabel 2.3 merupakan uraian panduan dari setiap klausul yang dipilih berdasarkan Gambar 2.8 sebagai panduan melakukan evaluasi kematangan perusahaan terhadap *Identity Governance Administration* (IGA):

Tabel 2. 3 Uraian Klausul Annex-A ISO 27001:2022 yang Berhubungan dengan IGA

A.5 Kontrol Organisasi		
A.5.3	Pemisahan Tugas	• Menerapkan praktik pemisahan tugas dan tanggung jawab.
A.5.15	Kontrol Akses	• Sistem informasi harus memenuhi kebutuhan pemisahan tugas. • Menjaga keamanan kredensial karyawan *(username* dan *password)*. • Membatasi akses karyawan menggunakan prosedur "manajemen akses" agar karyawan hanya dapat mengakses sumber atau aplikasi yang relevan dengan tugas dan tanggung jawabnya. • Melakukan monitoring akses karyawan secara berkala untuk memastikan bahwa akses yang dimiliki oleh karyawan saat ini sudah sesuai dengan tanggung jawabnya.
A.5.16	Manajemen Identitas	• Implementasi siklus manajemen identitas yang terdiri dari proses *request* akun/akses, penyediaan akun/akses, *user self-service* untuk menunjang penggantian informasi secara mandiri oleh karyawan, autentikasi akun karyawan, dan penghapusan akun karyawan ketika karyawan tersebut sudah tidak tergabung di dalam perusahaan [47]

A.5 Kontrol Organisasi		
A.5.18	Hak Akses	• Penyediaan hak akses harus dilakukan bersamaan dengan peninjauan hak akses secara berkala, pembaruan hak akses, serta penghapusan hak akses berdasarkan kebijakan perusahaan.

2.6 *Systems Security Engineering Capability Maturity Model* (SSE-CMM)

National Security Agency (NSA) merupakan agensi pemerintah Amerika Serikat yang berfokus untuk mewujudkan keamanan pada teknologi informasi. Pada tahun 1995 NSA membentuk sebuah tim untuk mengembangkan metode SSE-CMM yang dapat digunakan dalam membantu proyek rekayasa keamanan informasi. Penelitian ini kemudian dikembangkan oleh Carnegie Mellon University [22]

Sejak awal keberadaanya, metode SSE-CMM banyak digunakan oleh organisasi di Amerika Serikat untuk mengevaluasi serta menilai kemampuan rekayasa keamanan informasi pada saat itu. Dengan adanya metode SSE-CMM yang merupakan sebuah model perhitungan komprehensif, maka dapat diketahui tingkat keamanan informasi dari sebuah organisasi. Metode ini dapat membantu mengidentifikasi sistem atau tata kelola yang perlu diperbaiki untuk mencapai tingkat kepatuhan keamanan data berdasarkan framework yang dipilih. Berikut adalah ruang lingkup metode SSE-CMM,

1. Melakukan rekayasa keamanan *(security engineering)* terhadap suatu produk atau siklus hidup sistem, yang terdiri dari konsep dari sistem tersebut, kebutuhan organisasi, integrasi, penggunaan sistem, serta pengawasan atas penggunaan sistem.
2. Diterapkan dalam rangka mengamankan sistem informasi perusahaan, integrasi sistem informasi dengan organisasi yang menyediakan jasa pengembangan keamanan sistem atau rekayasa keamanan.
3. Metode dapat digunakan untuk pengukuran rekayasa keamanan untuk berbagai organisasi seperti, bidang komersial, pemerintahan, dan pendidikan.

2.7 *Tools* Implementasi *Identity Governance Administration* (IGA)

Terdapat banyak perusahaan penyedia *software* untuk mengimplementasikan IGA. Software ini diperlukan sebagai wadah bagi pengembang nantinya untuk melakukan integrasi sumber data dengan akses aplikasi yang diinginkan. Berikut pada gambar 2.9 merupakan *magic quadrant* untuk *tools* yang tersedia di pasar implementasi IGA.

Gambar 2. 9 *Magic Quadrant Tools* Implementasi IGA
Sumber: [48]

Gambar 2.9 menunjukan beberapa perusahaan yang menyediakan *software* yang dapat digunakan oleh perusahaan dalam mengintegrasikan sistemnya dengan IGA. Dapat diambil kesimpulan bahwa SailPoint merupakan salah satu perusahaan pemimpin penyedia layaan implementasi IGA. Berdasarkan riset yang dilakukan oleh Gartner, SailPoint dapat menjadi pemimpin pasar untuk *tools* pengelolaan

keamanan identitas. Hal ini diraih oleh SailPoint berdasarkan *feedback* yang diberikan oleh 82 pengguna SailPoint. Adapun kepuasan penggunanya adalah kemudahan mengintegrasikan SailPoint dengan aplikasi-aplikasi *third party* perusahaan dan kelengkapan fitur IGA yang disediakan [49].

2.7.1 SailPoint

SailPoint merupakan perusahaan asal Texas yang berdiri pada tahun 2005 untuk memberikan solusi yang inovatif dalam rangka menghadapi permasalahan keamanan identitas global yang terjadi secara dinamis.

Gambar 2. 10 Logo SailPoint
Sumber: [50]

Perusahaan ini berfokus pada integritas identitas melalui automasi dan penyederhanaan kompleksitas memberikan akses yang tepat kepada identitas yang tepat pada waktu yang tepat. Didukung oleh *platform* yang cerdas dan terpadu yang mengelola serta mengamankan akses *real-time* ke data dan aplikasi penting untuk setiap identitas perusahaan [51] .

Perusahaan ini berfokus pada integritas identitas melalui automasi dan penyederhanaan kompleksitas memberikan akses yang tepat kepada identitas yang tepat pada waktu yang tepat. Didukung oleh *platform* yang cerdas dan terpadu yang mengelola serta mengamankan akses *real-time* ke data dan aplikasi penting untuk setiap identitas perusahaan [51]. SailPoint membuat sistem yang ada di perusahaan saat ini menjadi lebih efisien dan hemat biaya untuk menemukan, mengelola, dan mengamankan semua akses identitas. SailPoint dapat memberikan visibilitas yang lebih mendalam untuk perlindungan identitas. Berikut adalah fitur-fitur yang tersedia pada SailPoint [52]:

a) Mengelola akses saat pengguna bergabung, berpindah, atau meninggalkan perusahaan.
b) Mengendalikan akses karyawan ke aplikasi dan sumber daya informasi perusahaan yang penting.
c) Mendeteksi dan memperbaiki hak akses yang diberikan oleh pemilik aplikasi walaupun di luar modul SailPoint.
d) Menyediakan laporan audit yang rinci tentang kepemilikan akses dan aktivitas pemberian serta penggunaan akses di dalam perusahaan.
e) Menyederhanakan proses sertifikasi hak akses dengan meningkatkan visibilitas terhadap kepemilikan akses dan akun karyawan.
f) Memberikan kepemilikan hak akses yang terinci, persetujuan, dan tata kelola pemberian hak akses.

Platform SailPoint memiliki tampilan *default* produk yang dapat disesuaikan dengan kebutuhan penggunanya. Berikut adalah tampilan *default platform* Sailpoint untuk halaman utama yang kemudian dapat dikustomisasi lagi berdasarkan modul-modul yang ingin digunakan. Tampilan *default* pada Sailpoint kemudian akan digunakan sebagai acuan dalam merancang protopie di penelitian ini.

2.8. *Unified Modeling Language* (UML)

UML merupakan sebuah pemodelan visual yang digunakan untuk menggambarkan model dari sistem yang akan dirancang. UML menggunakan sekumpulan istilah dan objek yang secara umum digunakan untuk mengembangkan sistem yan terdiri dari aktivitas sistem, struktur, interaksi di dalam sistem, dan siapa saja aktor yang dapat menggunakan sistem. UML memiliki *behavioural diagram* yang digunakan untuk menggambarkan bagaimana komponen di dalam suatu sistem saling beinteraksi yang terdiri dari beberapa jenis diagram seperti *Activity*

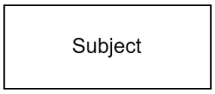
Diagram dan *Use Case Diagram.* Terdapat beberapa langkah yang perlu dilakukan sebelum melakuakan perancangan UML yaitu sebagai berikut [53],

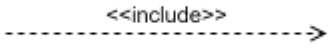
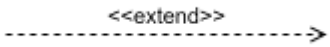
1. Melakukan pengumpulan informasi terkait proses yang diinginkan dan pihak yang terlibat di dalamnya untuk kemudian divisualisasikan menggunakan *use case diagram*.
2. Kemudian setelah mengetahui proses yang dibutuhkan, maka dilanjutkan dengan mendesain *activity diagram* untuk menggambarkan aliran aktivitas di dalam sistem.
3. Langkah terakhir adalah memastikan keterhubungan antara *use case diagram, activity diagram,* dan penjelasan masing-masing diagram sudah sesuai.

2.8.1 *Use Case Diagram*

Use Case diagram dapat memudahkan komunikasi pada saat merancang apa yang aka dilakukan oleh pengguna nantinya di dalam sistem. Diagram ini menggambarkan secara high level fugsi utama dari sistem dan hubungannya dengan tipe-tipe pengguna sistem. Berikut pada Tabel 2.4 merupakan simbol-simbol yang digunakan dalam membuat use case diagram [53],

Tabel 2. 4 Simbol Use Case Diagram

Simbol	Nama
	*Actor*
	*Use Case*
	Subject
	*Association Relationship*

Simbol	Nama
	*Include Relationship*
	*Extend Relationship*
	*Generalization Relationship*

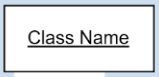
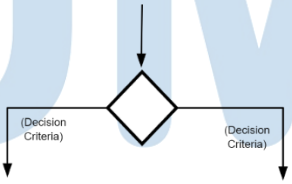
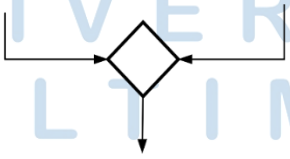
Berdasarkan Tabel 2.4, terdapat beberapa simbol yang digunakan dalam pembuatan *use case diagram.* Masing-masing simbol memiliki fungsinya tersendiri dalam menggambarkan fungsi dari sebuah sistem. Berikut adalah uraian penjelasan untuk setiap simbol pada *use case diagram:*

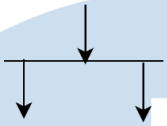
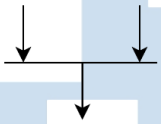
a) *Actor*: merupakan orang maupun sistem yang memperoleh manfaat. Dilambangkan dengan simbol *stick man* serta diberikan keterangan nama peran aktor di bagian bawah simbol.
b) *Use case*: mendiskripsikan poin utama dari fungsi sebuah sistem. Diberi label dengan kata kerja, dapat diperluas serta digabungkan dengan *use case* yang lain.
c) *Subject:* merupakan ruang lingkup seperti sistem atau proses bisnis.
d) *Association relationship:* penghubung antara *actor* dan *use case* yang saling berinteraksi.
e) *Include relationship:* penghubung antara satu *use case* dengan yang lainnya. Arah panah digambarkan dari *base use case* menuju *used use case*.
f) Extend relationship: untuk menghubungkan *use case* dengan perilaku tambahan. Arah panah digambarkan dari *extension* menuju *base use case*.
g) *Generalization relationship:* digunakan untuk menghubungkan *specialized use case* dengan *base use case*.

2.8.2 *Activity Diagram*

Activity Diargam merupakan lanjutan dari *use case diagram* yang menggambarkan alur proses pada suatu sistem [53]. *Activity diagram* digunakan untuk menggambarkan secara detail aktivitas apa saja yang terjadi pada sebuah sistem. Berikut pada Tabel 2.5 merupakan simbol yang digunakan dalam membuat *activity diagram:*

Tabel 2. 5 Simbol *Activity Diagram*

Simbol	Nama
	*Action*
	*Activity*
	Object node
	Control flow
	Object flow
	*Initial node*
	*Final-activity node*
	*Final-flow node*
	*Decision node*
	*Merge node*

Simbol	Nama
	*Fork node*
	*Join node*
	*Swimlane*

Tabel 2.6 merupakan simbol-simbol yang digunakan pada saat merancang *activity diagram* yang terdiri dari 13 simbol yang masing-masingnya memiliki fungsi sebagai berikut:

a) *Action:* berupa perilaku sederhana. Penamaannya berdasarkan perilaku yang dilakukan.
b) *Activity:* berupa tindakan yang dilakukan.
c) *Object node:* untuk merepresentasikan objek yang terhubung dengan *object flow*.
d) *Control flow:* untuk menggambarkan urutan sebuah *sequence*.
e) *Object flow:* berupa aliran sebuah objek dari satu aktivitas menuju aktivitas yang lain.
f) *Initial node*: merepresentasikan awal sebuah tindakan.
g) *Final-activity node*: untuk menunjukkan akhir sebuah tindakan.
h) *Decision node*: representasi *test condition* agar bergerak dalam satu jalur.
i) *Merge node:* mengembalikan berbagai keputusan ke dalam keputusan yang sama.
j) *Fork node*: membagi *behavior* menjadi berbagai aktivitas yang paralel.
k) *Join node*: mengembalikan aktivitas paralel menjadi satu aktivitas.

l) *Swimlane*: membagi *activity diagram* ke dalam baris dan kolom sebuah objek untuk diberikan aktivitas.