BAB 3
PELAKSANAAN KERJA MAGANG

3.1 Kedudukan dan Koordinasi

Pelaksanaan kerja magang dilakukan pada posisi *Technical Consultant* di divisi *Operation*. Saat ini, divisi *Operation* beranggotakan Bapak Muhammad Fajar Pratama dan Robiul Musthofa selaku *Project Manager*, Bapak M. Ichsan Nur Iman sebagai ketua tim, serta Bapak Rei dan Bapak Rizki Gunawan sebagai rekan kerja. Seluruh pekerjaan tim *Operation* berada di bawah pengawasan Bapak Ahmad Rizki selaku VP *Operation*. Penugasan dan koordinasi dilaksanakan melalui aplikasi web KejarTugas yang disediakan PT GIT.

3.2 Tugas yang Dilakukan

Kerja magang yang berfokus pada implementasi dan konfigurasi *Identity and Access Management* (IAM) dilaksanakan melalui beberapa tahapan sebagai berikut:

1. *Explore*

   Pada tahap ini, pekerjaan difokuskan pada eksplorasi kebutuhan klien. Eksplorasi awal dilakukan melalui pengenalan terhadap sistem IAM yang telah ada serta penetapan target sistem yang akan diintegrasikan ke dalam IAM. Selanjutnya dilakukan perencanaan (*planning*) dari alur (*flow*) yang akan dijalankan beserta tata cara pelaksanaannya.

2. *Implementation*

   Setelah tahap eksplorasi, melakukan implementasi alur (*flow*) yang telah direncanakan. Tahap ini mencakup *upgrade* atau pembuatan skema, *form*, serta pekerjaan *coding*, misalnya pengembangan *connector* antara target sistem dan aplikasi Oracle IAM.

3. *Testing*

   Pada tahap ini, dilakukan *testing* untuk memverifikasi keberhasilan hasil pada tahap *development*. Ruang lingkupnya mencakup *testing* alur IAM, *edge case testing*, serta pengujian konektivitas antara IAM dan target sistem.

4. *Documentation*

   Setelah *testing* selesai, dilakukan penyusunan dokumentasi atas IAM yang telah dikembangkan. Tahap ini mencakup pembuatan panduan mengenai cara kerja IAM serta tindakan yang dilakukannya terhadap sistem target.

3.3 Uraian Pelaksanaan Magang

Berikut ringkasan aktivitas magang dari minggu 1 sampai 15. Detail kegiatannya bisa dilihat di Tabel 3.1.

Tabel 3.1. Pekerjaan yang dilakukan tiap minggu selama pelaksanaan kerja magang

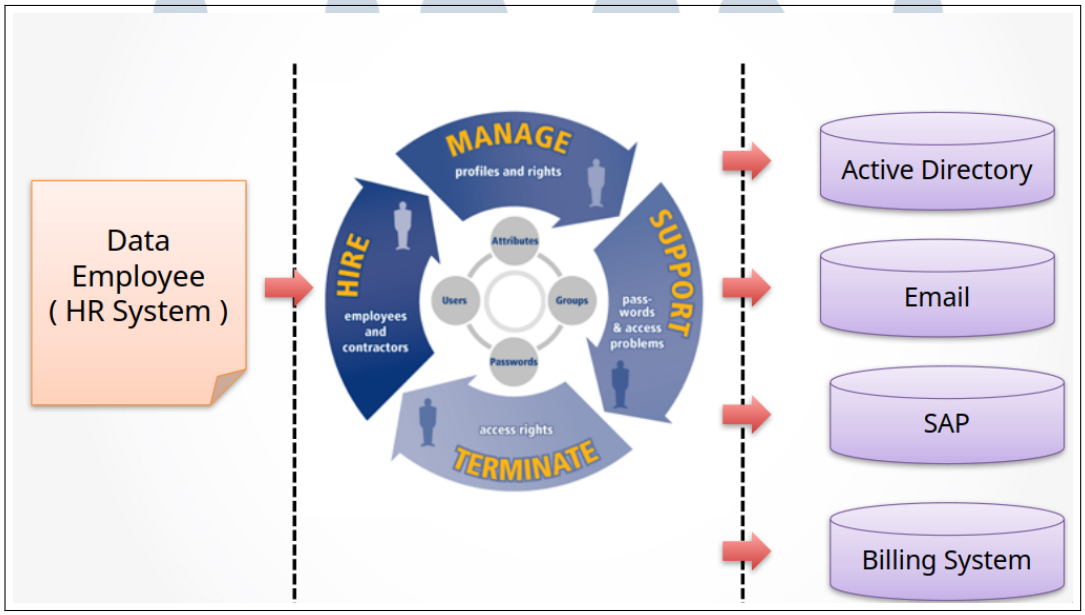
Minggu Ke -	Pekerjaan yang dilakukan
1	Menyusun dan merevisi dokumen IAM Panin serta menyiapkan dokumen target systems.
2	Melanjutkan revisi dokumen target systems dan mempelajari Reconciliation Panin.
3	Memperbaiki Design Console dan mengekspor Oracle 11g ke 12c.
4	Mengonfigurasi database 11g–12c dan melakukan prepopulate form Oracle IAM.
5	Menyelesaikan prepopulate Oracle IAM dan membuat Application Instance Active Directory.
6	Membuat flow *Create* ICBS dan menguji perbaikan prepopulate via adapter.
7	Merancang *Access Policy* ICBS dan memperbaiki bug database Oracle.
8	Menyusun dokumen ITS untuk sistem Active Directory dan ICBS.
9	Melakukan mutasi ICBS dan AD serta membuat *user guide*.
10	Menyelesaikan *user guide* ICBS dan membuat form Prudent.
11	Membuat *Process Definition* Prudent dan form e-SAR.

Tabel 3.2. Pekerjaan yang dilakukan tiap minggu selama pelaksanaan kerja magang (lanjutan)

12	Menyusun dokumentasi SIT dan membuat form Fingsys serta Red Hat.
13	Menyusun laporan dan melakukan *backup* sistem.
14	Memperbaiki SIT, melakukan *backup* sistem, dan merencanakan Prudent.
15	Menguji *workflow* dan menyusun *Access Policy* Prudent.

3.3.1 Oracle Identity and Access Management

Identity and Access Management (IAM) adalah sistem terpusat untuk mengelola siklus hidup identitas dan akses *user* pada beragam aplikasi atau sumber daya, mulai dari pembuatan akun, pemberian hak akses, sinkronisasi, hingga penonaktifan atau penghapusan akun. Dengan pendekatan ini, kebijakan akses menjadi konsisten, terukur, dan mudah diaudit lintas *target system*. Dalam konteks ini, Oracle menyediakan solusi bernama Oracle *Identity Management System* (OIM) yang mengelola akses *user* dari pembuatan hingga penghapusan akun [2], serta mendukung integrasi dan sinkronisasi akses ke seluruh *target system* melalui satu aplikasi *Identity Management* [4].



Gambar 3.1. Ilustrasi alur dasar IAM dari sumber data pegawai ke berbagai *target system*.

Gambar 3.1 memperlihatkan alur dasar IAM, dimana data pegawai dari sistem HR berfungsi sebagai rujukan utama untuk memicu siklus *hire*, *manage*, *support*, dan *terminate*. Pada inti proses terdapat objek identitas, meliputi atribut, *users*, *groups*, dan kata sandi, yang diatur menurut kebijakan akses. Perubahan profil maupun hak akses kemudian disalurkan dan disinkronisasi dengan berbagai *target system* (misalnya *Active Directory*, *email*, SAP, atau sistem penagihan), dan ketika masa kerja berakhir akses dicabut secara otomatis dan konsisten.

A Terminologi Dasar IAM

Berikut merupakan definisi singkat terminologi dasar IAM yang sering muncul pada uraian selanjutnya [5].

- *Target system*: Sistem tujuan yang menerima atau menggunakan data akses.
- *Source of truth*: Sumber data utama yang dianggap paling terpercaya untuk identitas.
- *Flow*: Rangkaian langkah terstruktur dari masuknya data hingga penerapan akses.
- *Provisioning*: Proses pemberian atau pembaruan akses ke sistem tujuan.
- *Deprovisioning*: Proses pencabutan akses ketika masa kerja berakhir/berubah.
- *Connector*: Komponen penghubung antara IAM dan sistem tujuan.
- *RBAC*: Pendekatan pemberian akses berdasarkan peran.
- *Reconciliation*: Penyelarasan kondisi akses yang ada dengan kebijakan IAM.
- *Trusted reconciliation*: Penyelarasan yang memperbarui data IAM mengikuti kondisi pada sistem tujuan (sistem tujuan diperlakukan terpercaya).
- *Non-trusted reconciliation*: Penyelarasan yang tidak langsung mengubah data IAM, di mana perbedaan dicatat atau ditandai untuk peninjauan lebih lanjut.
- *Lookup*: Merupakan kolom *dropdown* yang berisikan atribut-atribut yang dapat dipilih oleh *user*.
- *Prepopulate*: Merupakan kolom yang diisi secara otomatis lewat sistem menggunakan data yang sudah didapatkan dari tempat lain.

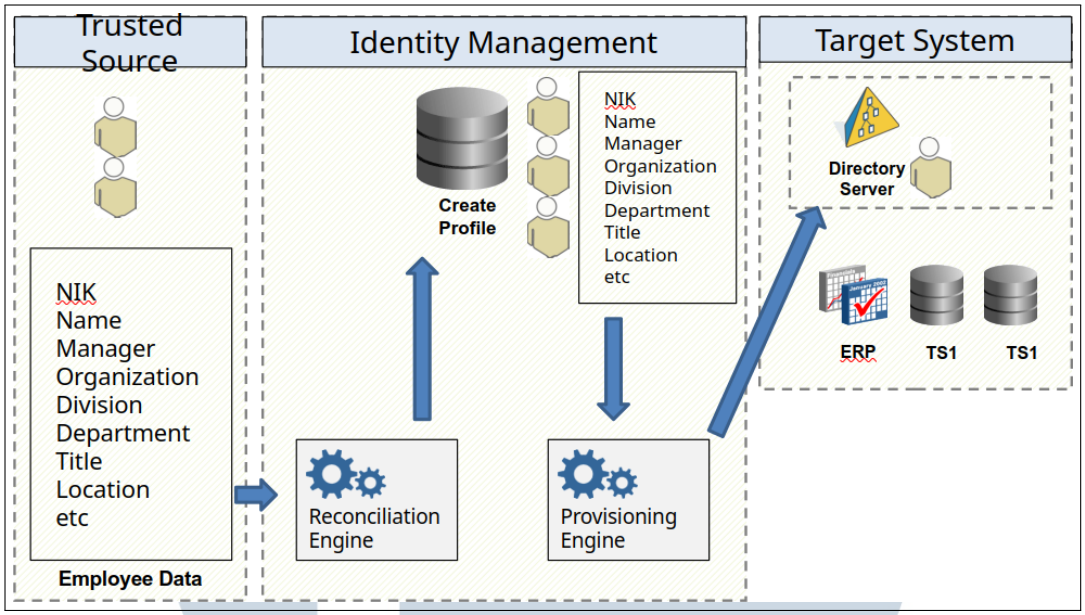
– *ERP*: Kelas aplikasi *enterprise* untuk mengelola proses bisnis inti, seperti keuangan, pengadaan, persediaan, produksi, SDM, yang sering menjadi salah satu sistem tujuan dalam integrasi IAM.

B Arsitektur dan Alur Kerja Identity Management

Dalam alur kerja sistem IAM, terdapat beberapa contoh arsitektur yang digunakan, yaitu: *On-Boarding, Transfer, Termination,* dan *Identification*.

B.1 On-Boarding

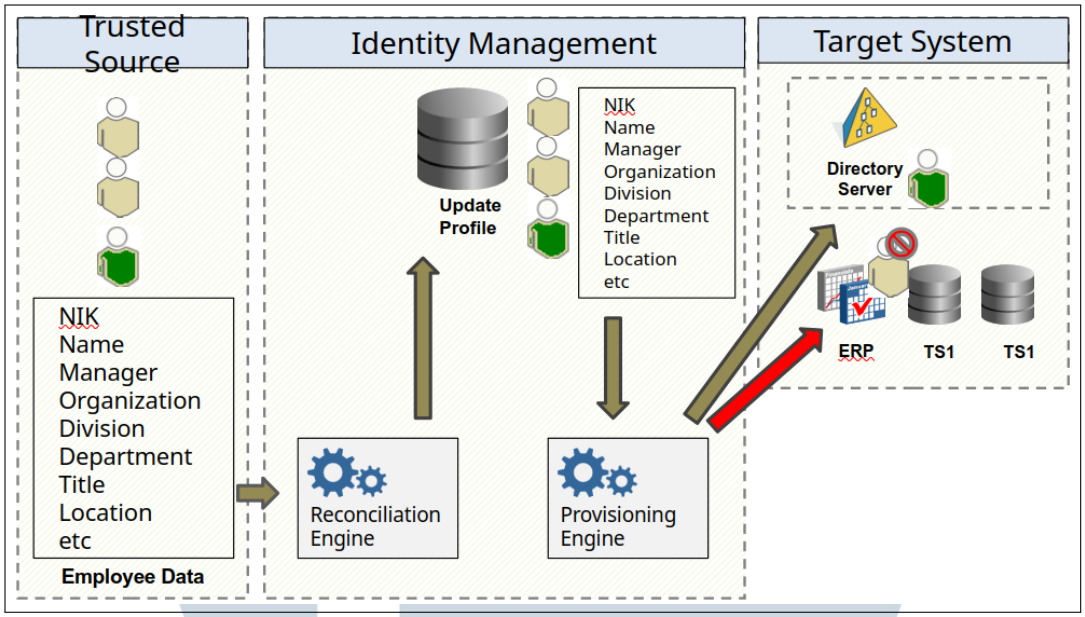
On-Boarding merupakan arsitektur IAM dimana akun pegawai baru akan dimasukkan ke dalam sistem. Data pegawai dari sumber terpercaya dikirim ke modul pengelolaan identitas, lalu sistem membuat profil pusat berisi atribut seperti NIK, nama, atasan, organisasi, jabatan, dan lokasi. IAM kemudian akan memberikan akses-akses dasar terhadap target sistem yang diperlukan, sesuai dengan kebijakan. Ketika terjadi perubahan status pada pegawai tersebut, seperti mutasi, promosi, ataupun jika pegawai keluar, maka perubahan ini akan juga disesuaikan berdasarkan kebijakan IAM. Contoh ini memperlihatkan bahwa IAM bertindak sebagai penghubung tunggal antara sumber data pegawai dan seluruh aplikasi tujuan, sehingga kebijakan akses dapat diterapkan secara terukur, konsisten, dan mudah diaudit. Gambar dari arsitektur *On-Boarding* dapat dilihat pada Gambar 3.2.



Gambar 3.2. Ilustrasi alur dasar IAM dari sumber data pegawai ke berbagai *target system*.

B.2 Transfer Employee

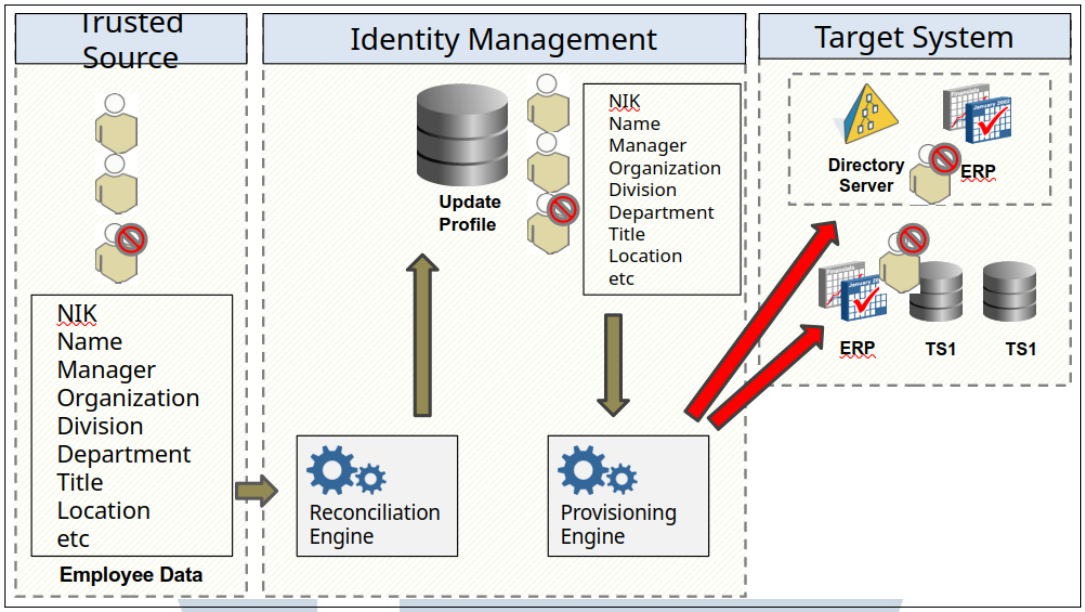
Setelah proses *on-boarding*, skenario umum berikutnya adalah mutasi pegawai. Gambar 3.3 memperlihatkan bahwa perubahan data dari sumber terpercaya seperti perpindahan organisasi, divisi, jabatan, atau lokasi akan memperbarui profil identitas di pusat. Berdasarkan kebijakan, IAM kemudian menata ulang akses dengan mempertahankan sumber daya dasar, mencabut akses yang tidak lagi relevan, dan memberikan akses yang sesuai dengan unit atau jabatan yang baru. Pembaruan ini disalurkan ke berbagai *target system* seperti direktori, ERP, dan aplikasi lain sehingga keanggotaan grup, peran, dan kewenangan di setiap sistem tetap selaras dengan kondisi terbaru. Dengan demikian, akses pegawai selalu sesuai kebutuhan terkini, resiko kelebihan hak dapat diminimalkan, dan proses penelusuran serta audit menjadi lebih mudah.



Gambar 3.3. Ilustrasi alur IAM saat mutasi pegawai (*transfer*).

B.3 Termination Employee

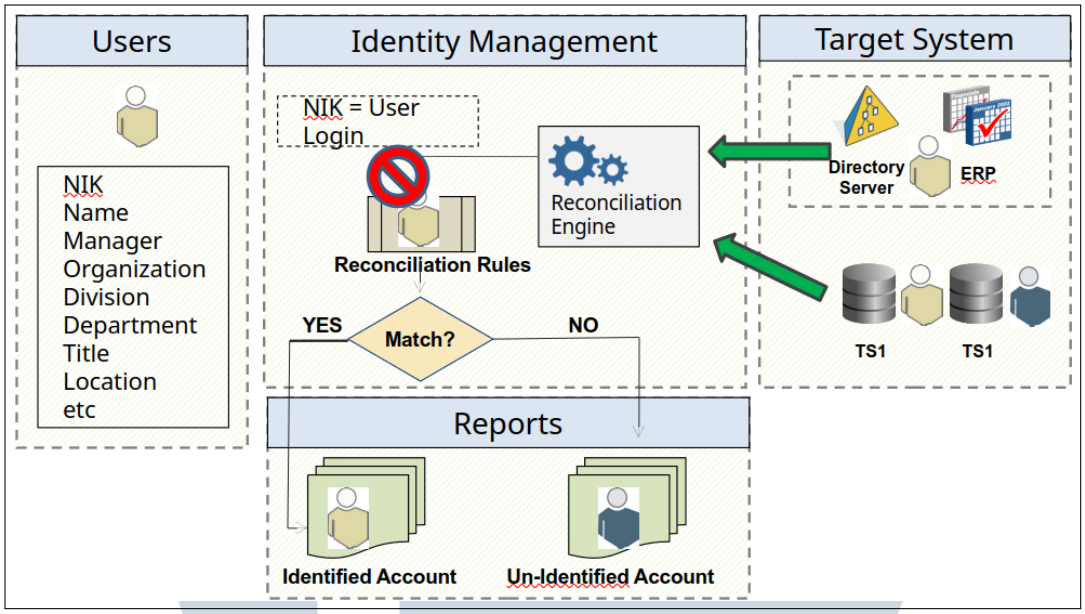
Gambar 3.4 memperlihatkan proses ketika pegawai berhenti bekerja. Perubahan status dari sumber terpercaya diterima oleh modul pengelolaan identitas, kemudian profil pusat diperbarui agar mencerminkan kondisi terakhir. Sesuai dengan kebijakan yang ditetapkan pada sistem, IAM akan menghapus atau akan menonaktifkan semua hak akses pegawai tersebut pada semua target sistem untuk menjaga keamanan sistem pada perusahaan.



Gambar 3.4. Ilustrasi alur IAM saat pemutusan hubungan kerja (*termination*).

B.4 Identification Users

Gambar 3.5 menunjukkan proses ketika akun yang sudah ada pada berbagai *target system* diinventarisasi lalu dibandingkan dengan data identitas di IAM. Pencocokan dilakukan berdasarkan aturan yang disepakati, misalnya menyamakan NIK dengan nama pengguna atau menggunakan kombinasi atribut lain yang relevan. Jika ditemukan kecocokan, akun ditandai sebagai *identified account* dan dihubungkan ke identitas pusat sehingga riwayat dan hak aksesnya dapat dikelola secara terpadu. Jika tidak ada pasangan yang sesuai, akun masuk ke laporan *un-identified account* untuk ditinjau lebih lanjut apakah perlu digabungkan, dinonaktifkan, atau dibersihkan. Proses ini membantu menemukan akun yang tertinggal (akun yatim), menutup kesenjangan data, dan meningkatkan kepatuhan audit.



Gambar 3.5. Ilustrasi pencocokan akun di sistem tujuan dengan identitas pada IAM.

3.3.2 Target System

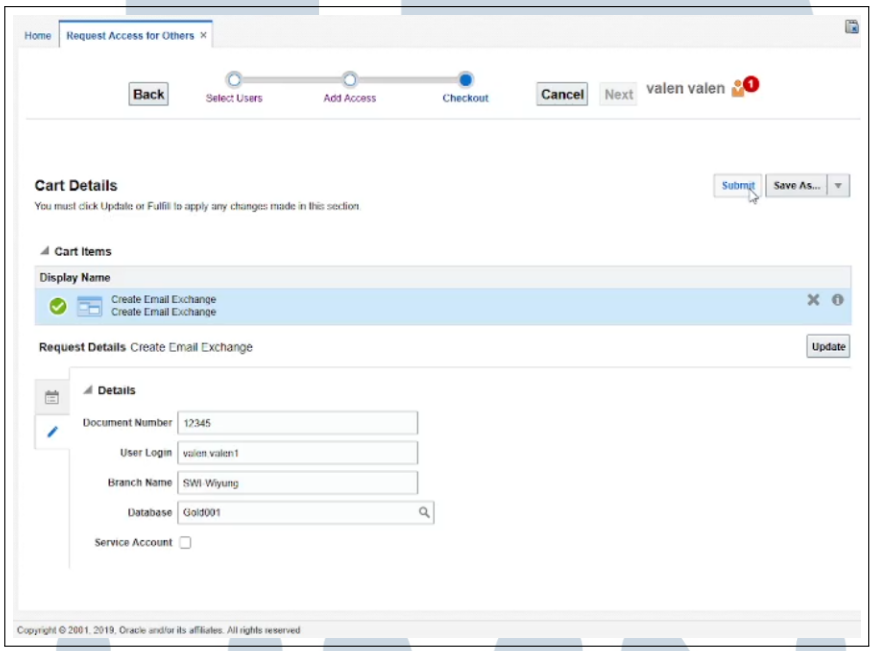
Dalam melaksanakan proyek IAM untuk Bank Panin, tim diminta mengintegrasikan sejumlah aplikasi dan layanan ke dalam sistem *Identity and Access Management* (IAM). Tabel 3.3 merangkum *target system* yang ditetapkan untuk dimasukkan, dikonfigurasi, serta diselaraskan kebijakan aksesnya di IAM.

Tabel 3.3. Daftar *target system*

No.	*Target System*
1	Active Directory
2	ICBS
3	Email Exchange
4	LOSS Panin
5	Prudent
6	Fingsys
7	e-SAR
8	Ascend
9	PSAK71
10	Red Hat

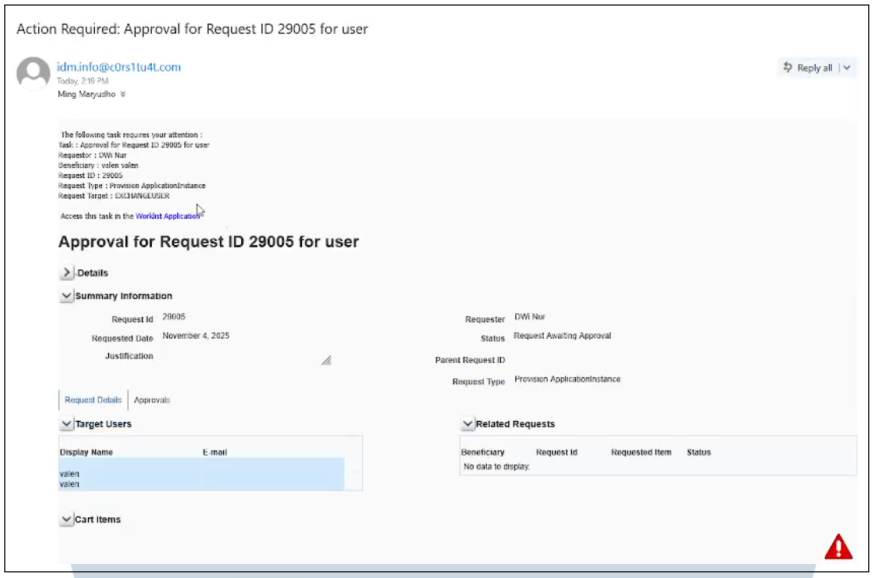
Untuk saat ini, tim IAM GIT diprioritaskan untuk menyelesaikan intergrasi

terhadap 3 target sistem, yaitu *Active Directory*, ICBS, dan *Email Exchange*. Setiap target sistem pada Tabel 3.3 mengikuti alur persetujuan yang sama. Sesuai permintaan Bank Panin, pengguna tidak dapat melakukan permintaan *request* atas nama sendiri, namun semua pengajuan harus dilakukan atas nama *user* yang memiliki peran sebagai *Maker*. Pengguna dengan peran *Maker* akan mengajukan permintaan melalui *form request* yang sesuai pada IAM. Contoh dari *form* ini dapat dilihat pada Gambar 3.6.



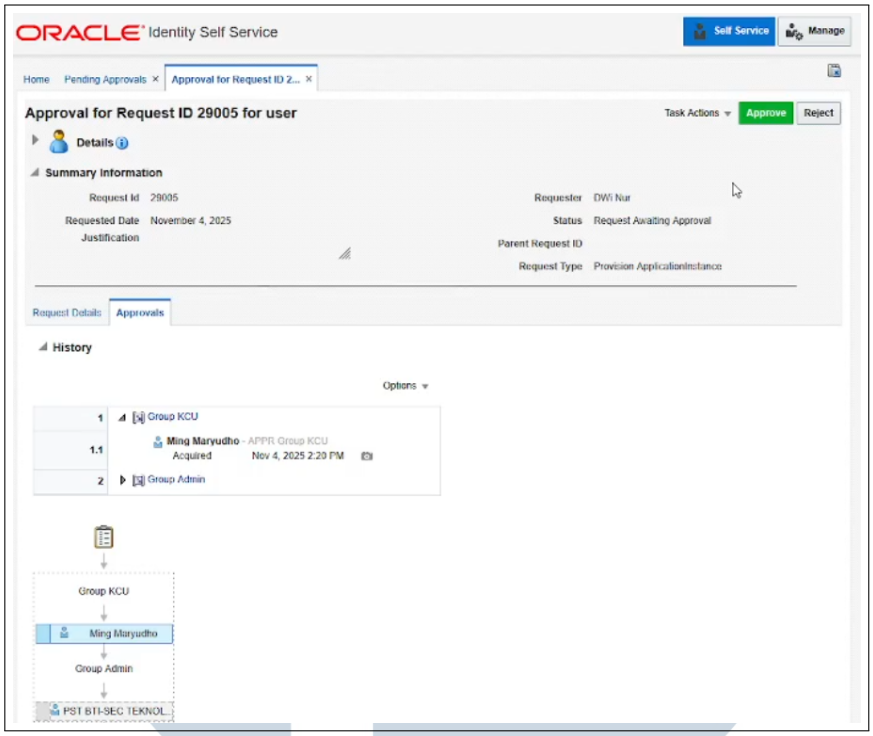
Gambar 3.6. Contoh pengisian *Form Request* oleh *Maker*.

Setelah *Maker* melakukan pengajuan *request*, sistem akan memberikan pemberitahuan kepada *user* yang memiliki peran sebagai *checker*. Untuk sistem IAM ini, notifikasi dari *request* tersebut akan dilakukan dalam bentuk *email*. Hal ini dapat dilihat pada Gambar 3.7.



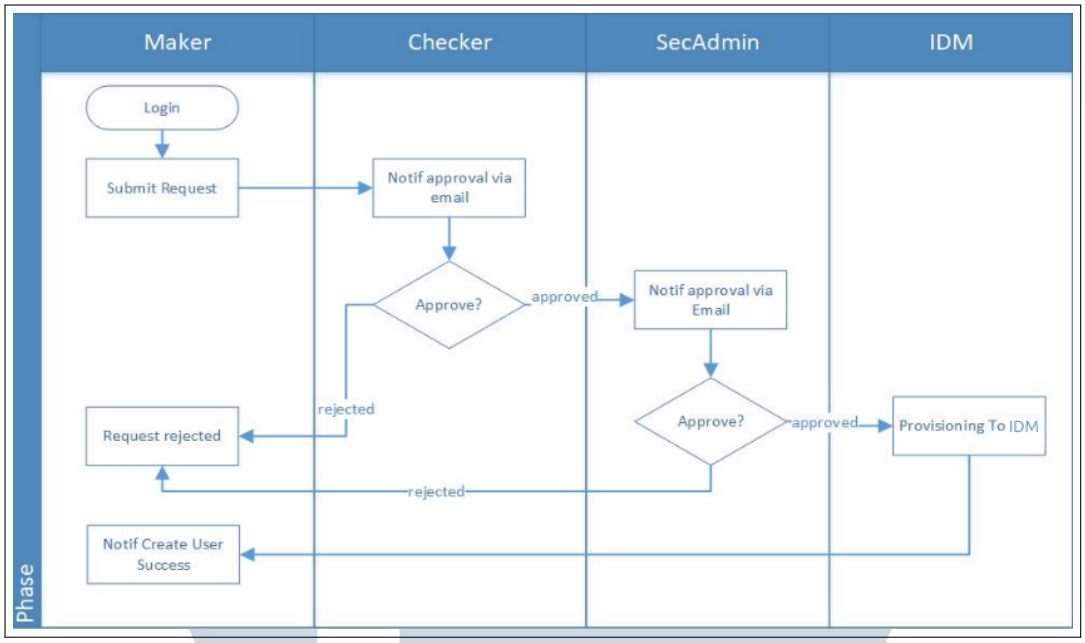
Gambar 3.7. Contoh notifikasi email yang didapatkan oleh *Checker*.

Kemudian, *checker* dapat meninjau request tersebut lebih lanjut dalam aplikasi IAM. jika diterima, maka *request* tersebut akan dilanjutkan kepada *SecAdmin* yang akan melakukan persetujuan akhir, dimana alur notifikasi dan persetujuan akan sama dengan *checker*. Contoh dari halaman persetujuan pada Oracle IAM dapat dilihat pada Gambar 3.8.



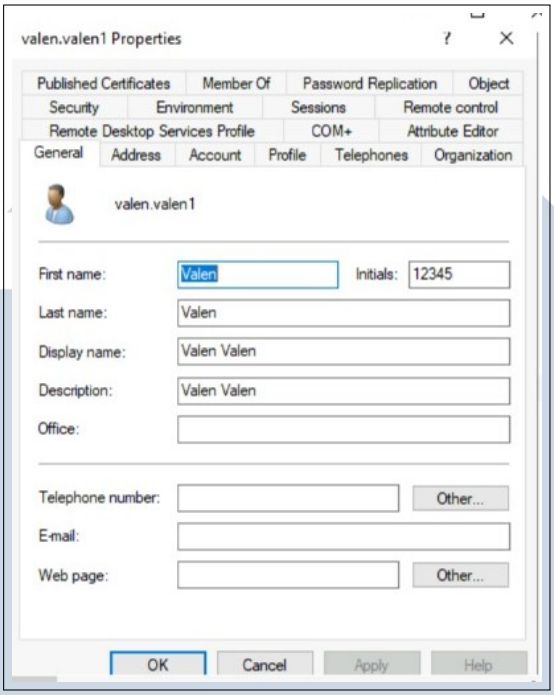
Gambar 3.8. Contoh halaman persetujuan pada Oracle IAM.

Dalam alur tersebut, *Checker* dan *SecAdmin* juga berhak untuk melakukan penolakan pada *request* yang didapatkan, namun diperlukannya komentar tambahan sebagai alasan mengapa permintaan tersebut ditolak. Jika ditolak, *Maker* akan mendapatkan notifikasi *email* penolakan tersebut. Alur kerja persetujuan ini secara keseluruhan dapat dilihat pada Gambar 3.9



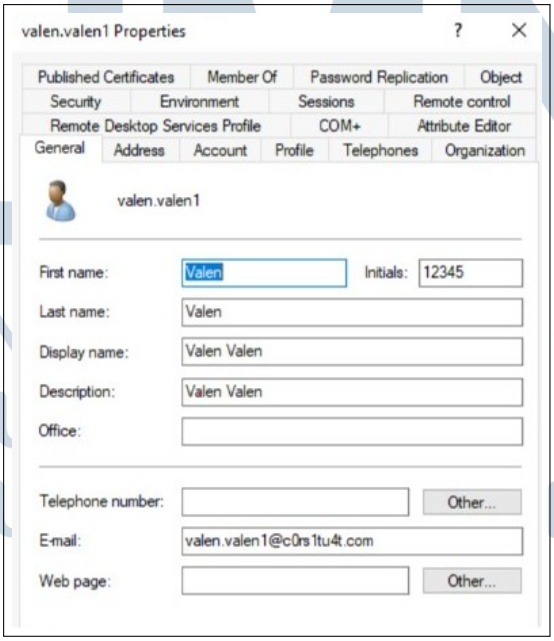
Gambar 3.9. Ilustrasi *workflow* yang diimplementasikan pada sistem IAM.

Setelah *workflow* tersebut sudah dilalui, maka pembuatan atau perubahan terhadap akun yang telah dilakukan *request* akan ditambahkan kepada *target system* yang dituju. Sebagai contohnya, Gambar 3.10 merupakan sebuah akun dalam sistem *Active Directory* yang belum mendapatkan *email*, dapat dilihat dengan kolom *E-Mail* kosong.



Gambar 3.10. Contoh akun *Active Directory* sebelum mendapatkan *E-Mail*

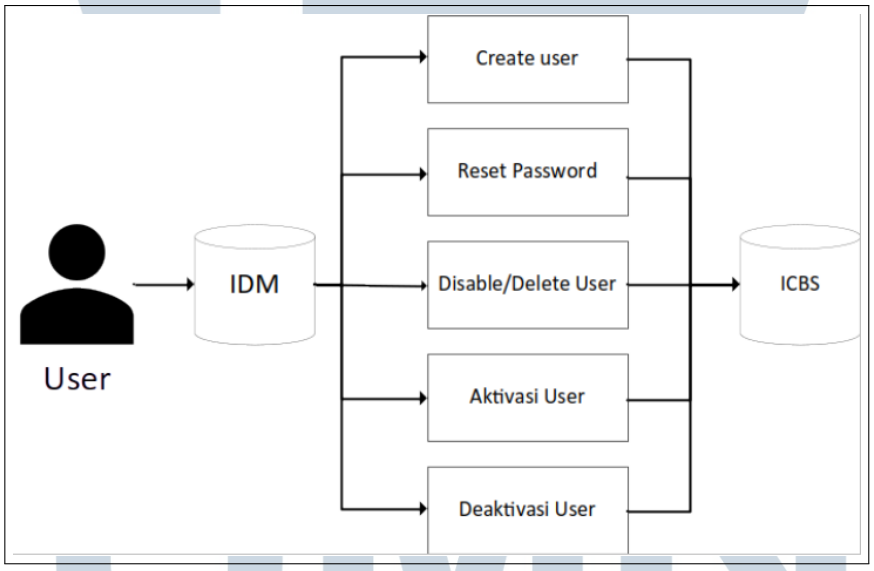
Setelah melakukan pembuatan form, dan semua alurnya dilalui dan disetujui, maka akun yang telah dilakukan *request* akan dibuatkan *email*, dan kolom *E-Mail* tersebut akan terisi secara otomatis. Hasil dari ini dapat dilihat pada Gambar 3.11



Gambar 3.11. Contoh akun *Active Directory* setelah mendapatkan *E-Mail*

A ICBS

Gambar 3.12 memperlihatkan proses-proses *provisioning* pada ICBS, seperti *Create User, Reset Password, Disable atau Dellete User, Aktivasi User, serta Deaktivasi User*. *Create user* membuat akun baru berdasarkan atribut yang tersimpan di IAM. *Reset password* hanya mengganti kata sandi tanpa mengubah profil pengguna. *Disable/Delete user* menonaktifkan sementara atau menghapus akun sesuai kebijakan yang berlaku. *Aktivasi user* mengubah status menjadi aktif agar akun dapat digunakan. *Deaktivasi user* menonaktifkan akun tanpa menghapus data sehingga dapat diaktifkan kembali bila diperlukan. Panah dari IAM ke ICBS menunjukkan eksekusi perintah, sedangkan panah kembali menggambarkan konfirmasi hasil yang kemudian dicatat di IAM.



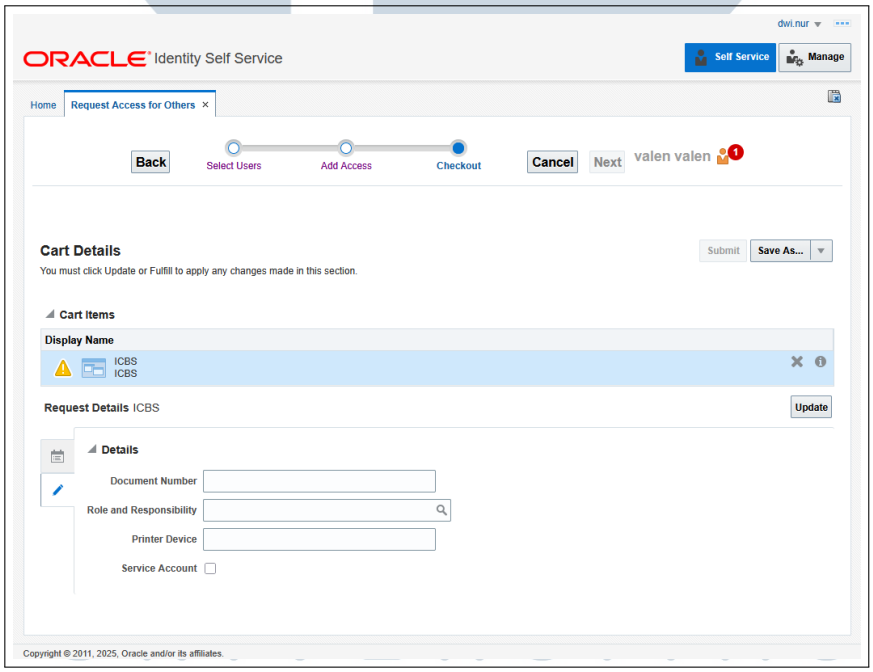
Gambar 3.12. Ilustrasi proses *provisioning* pada target sistem ICBS.

ICBS menerima masukan melalui sebuah formulir yang memadukan data otomatis dari IAM dan isian pengguna. Rangkuman bidang yang digunakan tersaji pada Tabel 3.4.

Tabel 3.4. Bidang masukan untuk proses ICBS

Field Label	Variant Type	Field Type	Editable	Required
Document Number	String (100)	Output Value	Y	Y
First Name	String (100)	Output Value	N	Y
Last Name	String (100)	Output Value	N	Y
Role and Responsibilities	String (100)	Lookup Field	Y	Y
Printer Device	String (100)	Output Value	Y	N

Document Number diisi pengguna sebagai penanda proses, *First Name* dan *Last Name* terisi otomatis dari profil IAM sehingga tidak memerlukan kolom pada *form Create User ICBS*, *Role and Responsibilities* dipilih dari daftar acuan peran yang berlaku, sedangkan *Printer Device* bersifat opsional dan diisi sesuai kebutuhan unit kerja. Contoh dari *form* untuk melakukan pembuatan user ICBS dapat dilihat pada Gambar 3.13.



Gambar 3.13. Form Create User ICBS dalam Oracle IAM.

A.1 Business Rule ICBS

Dalam memproses data pada target sistem ICBS, terdapat beberapa *Business Rule* yang perlu diikuti. Berikut merupakan aturan-aturan yang mesti diikuti saat memproses data *User* ICBS:

A.1.1 User Login

Dalam melakukan *user login* pada target sistem ICBS, *username* pada ICBS terdiri dari maksimum 10 digit. 3 digit pertama dalam *username* merupakan kode inisial untuk cabang *user* tersebut. Kemudian 1 digit berikutnya merupakan *role* atau peran *user* dalam ICBS (0-9), dan yang terakhir, 6 digit berikutnya merupakan nama user yang dapat diambil dari *first name* dan *last name user* tersebut. Contoh dari *username* ini akan berbentuk seperti ”JAS4FAJARP”.

A.1.2 Request Create User

Pada skenario *request create user* untuk ICBS, *maker* mengisi formulir yang sudah terhubung ke IAM. Beberapa atribut kunci akan menjadi penanda unik, yaitu *ICBS User ID* dan, khusus untuk peran PDW, *PDW User ID*, dimana dalam konteks ini, PDW merupakan sebuah server lain yang terikat dengan ICBS. Pada formulir *Create User*, *Requestor Branch* akan secara otomatis terisi dari data cabang dan bisa dipilih lewat *lookup*. Kolom yang wajib diisi antara lain merupakan *Document Number*, *Employee Number*, *First Name*, *Last Name*, serta *Role and Responsibilities* yang juga dapat dipilih lewat *lookup*. Terdapat juga kolom *Printer Device* yang secara *default* bernilai ”*WRKSTN” dan kolom *Comment* bila butuh catatan tambahan. Setelah proses berjalan dan akses dibuat di ICBS, IAM menyimpan hasilnya sesuai jenis peran. Kalau perannya bukan PDW, maka *Role and Responsibilities* dan *ICBS User ID* akan tercatat di atribut IAM. Kalau perannya sebagai PDW, yang disimpan pada IAM adalah atribut PDW yang terkait.

A.1.3 Aktivasi User ICBS

Pada skenario aktivasi *user*, tujuannya adalah untuk mengisi *initial program* dan *library* pada profil *user* ICBS yang sebelumnya masih bernilai *default*. Pada formulir, kolom *Requestor Branch* akan secara otomatis terisi dari data cabang karyawan tersebut, sedangkan kolom *User* ICBS atau PDW juga akan terisi secara otomatis, menggunakan *ICBS User ID* untuk peran non-PDW atau *PDW User ID* bila perannya PDW. Setelah permintaan dikirim dan disetujui, IAM menerapkan perubahan ke ICBS sehingga akun siap digunakan.

A.1.4 Perubahan atau Modifikasi Akun

Pada skenario perubahan akun, *maker* mengisi formulir yang memuat *Document Number* sebagai isian wajib, *User IAM* yang terisi otomatis dan wajib, *User ICBS* yang juga diambil dari data yang ada, *Current Role* sebagai peran saat ini, serta *New Role* yang wajib dipilih melalui pencarian *lookup*. Kolom *Printer Device* dapat diisi sesuai kebutuhan dan tersedia ruang *Comment* untuk catatan tambahan. Setelah disetujui dan dieksekusi, mekanisme di ICBS akan menghapus akun ICBS tersebut beserta seluruh perannya, kemudian membuat ulang akun baru dengan *user ID* dan peran yang sesuai.

A.1.5 Penghapusan Akun

Pada skenario penghapusan akun ketika karyawan *resign* atau kontrak berakhir, *maker* mengisi formulir dengan *Document Number* sebagai isian wajib dan *User ID* yang terisi otomatis. Setelah disetujui dan dieksekusi, ICBS akan menghapus akun beserta seluruh perannya agar tidak ada akses yang tersisa. Jika penghapusan dipicu dari IAM untuk Kantor Pusat, sistem juga akan mencabut sumber daya terkait seperti *Active Directory* dan ICBS sehingga status akses konsisten di semua sistem. Penghapusan juga bisa diajukan dari KCP atau KCU melalui *e-submission* dan hasilnya tetap tersinkron dengan IAM.

A.1.6 Karyawan Mutasi

Pada skenario mutasi, perubahan cabang atau peran diajukan lewat formulir yang terhubung ke IAM dan ICBS. Di ICBS, akun lama beserta seluruh perannya dihapus, lalu dibuat akun baru dengan *user ID* dan peran yang sesuai kondisi terbaru. Cara ini mencegah sisa akses dari cabang atau fungsi sebelumnya. Untuk mutasi di Kantor Cabang Utama (KCU) yang sama, *maker* mengisi *Document Number* sebagai isian wajib. Kolom *User IAM*, *User ICBS*, *Current Branch*, dan *Current Role* otomatis terisi dari data yang ada. Kolom *New Branch* dan *New Role* dipilih melalui *lookup*. Kolom *Printer Device* bersifat opsional dan tersedia kolom *Comment* untuk catatan tambahan. Untuk mutasi antar KCU, alurnya mirip, tetapi *New Branch* dapat dipilih dari seluruh organisasi, baik KCU maupun KCP, dan *New Role* juga dipilih melalui *lookup*. Pada profil pengguna di IAM, nama organisasi pada tab atribut akan berubah mengikuti cabang terbaru.

A.1.7 Reset Password

Pada skenario *reset password*, *maker* mengisi *Document Number* sebagai isian wajib. Pada kolom *user ICBS*, kolom tersebut akan secara otomatis terisi berdasarkan akun *user ICBS* yang ingin dilakukannya *reset password*. Setelah permintaan diproses di ICBS, nilai verifikasi kata sandi yang tidak valid akan di-*set* menjadi 0, status akun diubah menjadi ”*ENABLED”, dan riwayat *previous sign-on* akan dikosongkan agar akun dapat kembali digunakan.

A.1.8 Password Policy

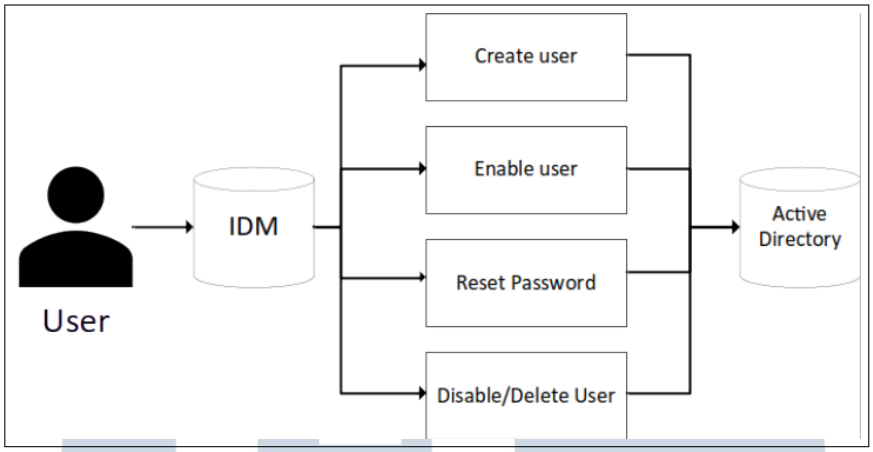
Kata sandi di ICBS mengikuti aturan sederhana, yaitu menggunakan maksimum 10 karakter yang terdiri dari angka dan huruf kecil. Aturan ini berlaku saat membuat akun baru maupun saat mengganti kata sandi, sehingga kombinasi yang dipakai harus memenuhi ketentuan tersebut.

A.1.9 Enable Account ICBS

Pada saat akun terkunci karena salah memasukkan kata sandi tiga kali atau dinonaktifkan atas permintaan *SecAdmin*, proses aktifkan kembali dilakukan melalui permintaan di IAM. Kolom *User ICBS* sudah terisi otomatis dan wajib sesuai akun yang akan dipulihkan. Setelah disetujui dan dieksekusi di ICBS, nilai *password verification not valid* diatur menjadi 0 dan status akun diubah menjadi ”*ENABLED” agar pengguna bisa masuk kembali.

B Active Directory

Gambar 3.14 memperlihatkan proses *provisioning* untuk *Active Directory*, yang meliputi *Create user*, *Enable user*, *Reset Password*, serta *Disable/Delete User*. *Create user* merupakan membuat akun AD baru berdasarkan atribut yang tersimpan di IAM, seperti nama, identitas pegawai, dan penempatan *Organization Unit* (OU) awal. *Enable user* mengaktifkan akun agar bisa digunakan, termasuk membuka akses jika sebelumnya terkunci. *Reset Password* mengganti kata sandi tanpa mengubah profil atau struktur keanggotaan grup. *Disable* atau *Delete User* menonaktifkan sementara atau menghapus akun sesuai kebijakan yang berlaku, misalnya ketika pegawai keluar atau akses harus dihentikan.



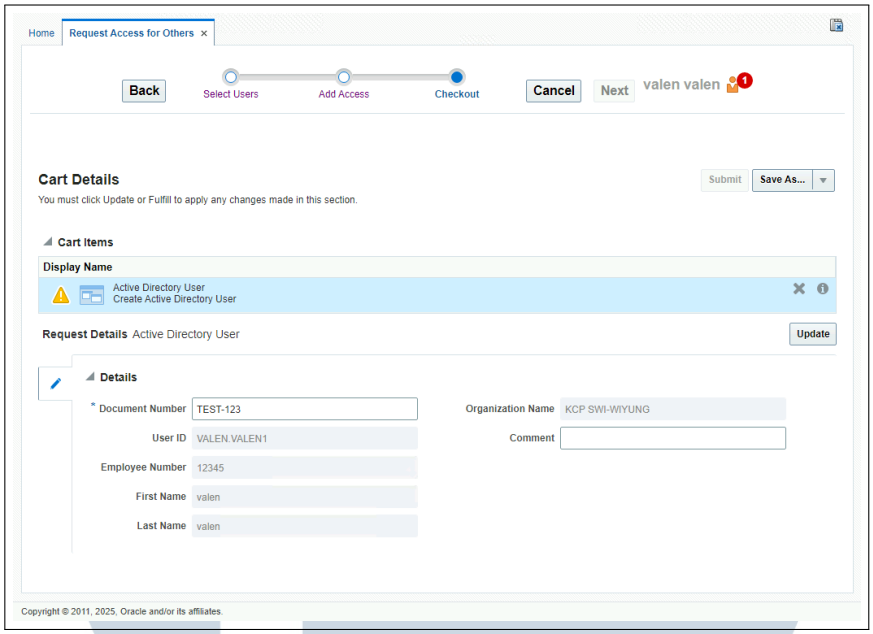
Gambar 3.14. Ilustrasi proses *provisioning* pada target sistem *Active Directory*.

Active Directory menerima masukan melalui formulir yang menggabungkan data otomatis dari IAM dengan isian pengguna. Rangkuman bidang yang digunakan ditunjukkan pada Tabel 3.5.

Tabel 3.5. Bidang masukan untuk proses Active Directory

Field Label	**Variant Type**	**Field Type**	**Editable**	**Required**
Document Number	String (100)	Output Value	Y	Y
Employee Number	String (100)	Output Value	N	Y
First Name	String (100)	Output Value	N	Y
Last Name	String (100)	Output Value	N	N
Organization Name	String (100)	Lookup Field	Y	Y
Comment	String (100)	Output Value	Y	N

Kolom *Document Number* berfungsi sebagai penanda proses, *Employee Number, First Name,* dan *Last Name* akan terisi secara otomatis berdasarkan akun yang dilakukannya *request*, *Organization Name* dapat dipilih berdasarkan organisasi karyawan tersebut, sementara *Comment* ditambahkan jika diperlukannya informasi tambahan dalam pembuatan akun AD tersebut. Contoh dari *form* untuk melakukan *create Active Directory* dalam IAM Oracle dapat dilihat pada Gambar 3.15.



Gambar 3.15. Form Create User Active Directory dalam Oracle IAM.

B.1 Business Rule Active Directory

Dalam memproses data pada *Active Directory*, aturan berikut dipakai agar penamaan akun, alur persetujuan, dan hasil penerapan di IAM dan AD tetap selaras.

B.1.1 Penamaan User Login dan Kebijakan Password

Format *user login* adalah ”*firstname.lastname*”. Jika nama hanya satu kata maka gunakan ”*firstname.firstname*”, contohnya ”daniel.daniel”. Jika sudah ada nama yang sama maka tambahkan angka urut di belakang *lastname*, misalnya ”daniel.daniel”, ”daniel.daniel1”, ”daniel.daniel2”. Panjang maksimal *user login* adalah 20 karakter termasuk tanda titik. *UserID* di IAM dan AD harus sama. *Password* harus memenuhi syarat minimal delapan karakter, memiliki setidaknya satu huruf besar, satu huruf kecil, satu angka, dan satu karakter spesial.

B.1.2 Pembuatan Akun Baru

Dalam melakukan pembuatan akun baru AD, alur kerja di-inisiasikan oleh *maker* dalam melakukan pembuatan *request*. Persetujuan kemudian dilakukan dengan urut *Checker* dan *SecAdmin*. Pada *form* ini, kolom *Document Number,*

Employee Number, First Name, Last Name dan *comment* berupa isian teks. Kolom *Organization Name* dapat dipilih dari daftar organisasi yang tersedia.

B.1.3 Reset Password

Alur persetujuan mengikuti urutan *Maker*, *Checker*, lalu *SecAdmin*. *Form* berisi *Document Number* yang berisi nomor eCSA, *User Login IAM* yang terisi otomatis, serta *Comment* sebagai *input* opsional. Hasil penerapan di AD adalah *password* pengguna di-*reset* dan status akun menjadi *enabled*.

B.1.4 Mutasi User dalam Satu KCU

Alur persetujuan mengikuti urutan *Maker*, *Checker*, lalu *SecAdmin*. *Form* berisi *Document Number*, *User IAM*, *User ICBS*, *Current Branch*, dan *Current Role* yang diisi dari data yang ada. *New Branch* dan *New Role* wajib dipilih dari *Organization* dengan induk yang sama menggunakan *lookup*. Kolom *Printer Device* dan *Comment* bersifat opsional. Dampaknya, pada tab *Attributes* di IAM, nilai *Organization* berubah dan pada objek AD, posisi OU pengguna juga berpindah ke cabang baru.

B.1.5 Mutasi User Antar KCU

Alur persetujuan mengikuti urutan *Maker*, *Checker* cabang asal, *Checker* cabang baru, lalu *SecAdmin*. Kolom pada *form* akan memiliki atribut yang sama seperti mutasi *user* dalam satu KCU, namun *New Branch* dapat dipilih dari seluruh *Organization* baik KCU maupun KCP menggunakan *lookup*. Dampaknya sama, yaitu perubahan *Organization* pada tab *Attributes* IAM dan perpindahan OU pada objek AD.

B.1.6 Hapus Akun

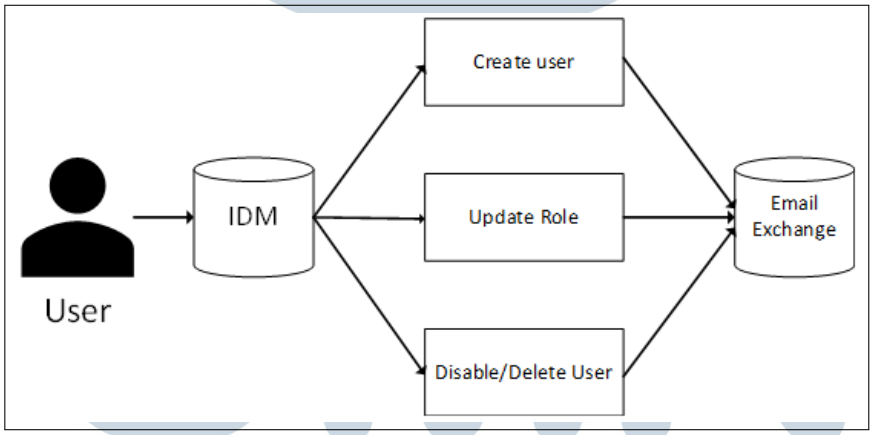
Alur persetujuan mengikuti urutan *Maker*, *Checker*, lalu *SecAdmin*. *Form* berisi kolom *User Domain* yang terisi secara otomatis, serta kolom *Document Number*. Setelah disetujui, akun di AD langsung dihapus tanpa proses *disable* terlebih dahulu.

B.1.7 Enable Account

Alur persetujuan berjalan dari *Maker* ke *SecAdmin*. Tujuannya mengaktifkan kembali akun AD, yaitu mengubah status dari *disabled* ke *enabled*. *Form* hanya meminta *User Domain* yang terisi secara otomatis.

C Email Exchange

Gambar 3.16 memperlihatkan proses *provisioning* untuk Email Exchange, yang mencakup *Create user*, *Update Role*, serta *Disable/Delete User*. *Create user* merupakan proses untuk membuat akun surel baru berdasarkan penempatan cabang akun karyawan tersebut. *Update Role* merupakan proses untuk mengubah informasi akun surel yang telah dibuat berdasarkan *role* baru yang dimiliki oleh akun karyawan tersebut. *Disable/Delete User* akan menonaktifkan sementara atau menghapus akun email sesuai kebijakan, misalnya saat karyawan keluar. Perlu diketahui bahwa untuk melakukan *request* terhadap pembuatan *Email Exchange*, akun karyawan yang didaftarkan memerlukan akun *Active Directory*.



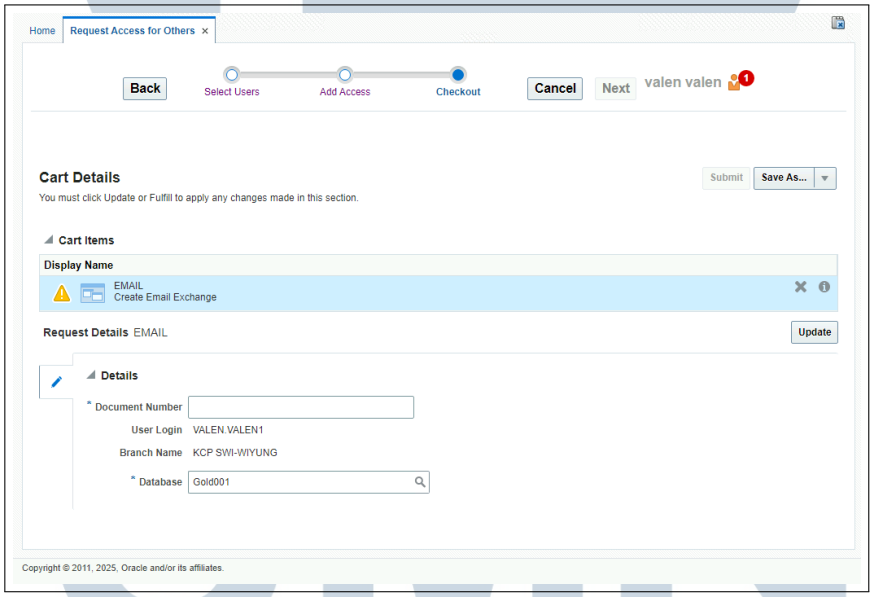
Gambar 3.16. Ilustrasi proses *provisioning* pada target sistem *Email Exchange*.

Formulir ini menggabungkan isian pengguna dengan acuan dari IAM. Rangkuman bidang yang dipakai ditunjukkan pada Tabel 3.6.

Tabel 3.6. Bidang masukan formulir

Field Label	Variant Type	Field Type	Editable	Required
Document Number	String (100)	Output Value	Y	Y
User Login	String (100)	Output Value	Y	Y
Database	String (100)	Lookup Field	Y	Y
Branch Name	String (100)	Output Value	Y	N

Secara singkat, *Document Number* dipakai sebagai nomor referensi pengajuan, *User Login* diisi sesuai nama akun yang akan diproses, *Database* dipilih lewat *lookup* agar sesuai daftar yang tersedia, sedangkan *Branch Name* dapat diisi bila diperlukan untuk menandai cabang terkait. *Form* IAM pembuatan akun *Email Exchange* dapat dilihat pada Gambar 3.17.



Gambar 3.17. Form Create Email Exchange dalam Oracle IAM.

C.1 Business Rule Email Exchange

Aturan berikut dipakai agar pembuatan dan pengelolaan akun email tetap rapi dan selaras dengan IAM.

C.1.1 User Login Email

Format alamat email adalah ”*firstname.lastname@panin.co.id*”. Jika nama hanya satu kata, gunakan ”*firstname.firstname@panin.co.id*”, misalnya

”daniel.daniel@panin.co.id”. Kalau sudah ada nama yang sama, tambahkan angka urut di belakang bagian *lastname*, contohnya ”daniel.daniel@panin.co.id”, ”daniel.daniel1@panin.co.id”, ”daniel.daniel2@panin.co.id”. Alias email mengikuti format yang sama. Penempatan *storage* atau database disesuaikan dengan jabatan: paket ”*Gold*” untuk staf, ”*Platinum*” untuk kepala divisi, dan ”*Infinity*” untuk direktur.

C.1.2 Form Request Create Email

Dalam form *Create Email*, kolom *Branch Number* wajib diisi 16 digit, kolom *Login* wajib diisi sesuai nama akun yang akan dibuat, dan kolom *Database* wajib dipilih agar penyimpanan *mailbox* sesuai paket yang berlaku.

C.1.3 Penghapusan Akun / Terminate

Saat pengguna *resign* atau kontrak berakhir, data *Email Exchange* akan dicabut. Dari sisi *Email Exchange*, akun akan di-*disable* atau *soft delete* sesuai kebijakan, sehingga akses email berhenti namun tetap tercatat untuk keperluan audit atau pemulihan bila diperlukan.

C.1.4 Karyawan Mutasi

Jika karyawan berganti cabang atau melakukan perubahan peran, maka akun *email* karyawan tersebut akan juga mengikuti perubahan berdasarkan cabang atau peran baru yang dimiliki. Perubahan ini akan mengikuti perubahan pada akun *Active Directory*, maka tidak diperlukannya *form* khusus untuk melakukan perubahan ini.

C.1.5 Reset Password

Untuk *reset password* email, *form* hanya akan meminta *Document Number* sebagai nomor rujukan. Prosesnya mengikuti aturan *reset* yang berlaku di Active Directory agar status akun dan kredensial tetap sinkron antara IAM, AD, dan *Email Exchange*.

3.4 Kendala dan Solusi yang Ditemukan

Selama proses pengerjaan proyek di PT Global Innovation Technology untuk Bank Panin, ada beberapa hal yang menjadi tantangan. Kendala-kendala yang ditemukan adalah sebagai berikut:

- IAM merupakan konsep yang baru, dimana terdapat banyak istilah dan komponen yang belum diketahui, seperti alur persetujuan, cara bekerjanya IAM secara umum, cara melakukan koneksi antara IAM dan target sistem, serta pola rekonsiliasi. Dampaknya, waktu pengerjaan untuk beberapa tugas lebih lama dari yang diperkirakan, dikarenakan diperlukannya untuk membaca dokumentasi serta melakukan *testing* pada IAM tersebut.
- Ketersediaan sumber daya manusia terbatas dibandingkan jumlah *target system* dan pekerjaan pendukungnya. Saat ada prioritas mendadak dari klien, sebagian pekerjaan lain tertunda dan terpaksa dilakukannya pembagian tugas kepada tim yang tidak terlibat secara langsung dengan proyek IAM Panin Bank.
- Terdapat beberapa permintaan khusus (*foreign case*) dari Bank Panin, sehingga tidak dapat langsung dikerjakan. Untuk permintaan dengan kasus ini, diperlukannya validasi dari pihak Oracle jika permintaan tersebut dapat dilakukan, dan jika tidak memungkinkan, maka diperlukannya diskusi ulang dengan Bank Panin jika terdapat solusi lain yang dapat dilakukan untuk mengatasi permintaan tersebut.

Untuk mengurangi hambatan di atas, solusi yang dilakukan adalah:

- Menerapkan pola belajar sambil praktik di *development environment* kantor dan *development server* Bank Panin. Setiap fitur dicoba *end-to-end*, dicatat langkahnya, dan dibuat *checklist* agar saat mengulang di lingkungan lain prosesnya lebih cepat dan minim salah.
- Mengatur kerja per *target system* dengan pasangan dua orang untuk mengurangi *workload* pada *target system* tersebut. Dengan pola ini, dua *target system* bisa berjalan paralel, sementara pekerjaan non-teknis seperti dokumentasi dan administrasi dibantu rekan GIT lain supaya progres teknis tidak terhambat.

– Membuka tiket ke *Oracle Support* untuk tiap *foreign case* yang membutuhkan konfirmasi resmi, lalu menindaklanjuti lewat *weekly meeting* bersama pihak terkait. Hasil dari diskusi tersebut kemudian akan dicoba pada *development server* Bank Panin, dan jika tidak dapat dilakukan, dilakukannya laporan kepada pihak terkait untuk mencari solusi baru terhadap permintaan tersebut.