

DOKUMENTASI SISTEM

Dashboard Audit MAINPP

Dokumentasi fungsi sistem, struktur database, ERD dan flow chart

Nama Sistem	Dashboard Audit MAINPP
Organisasi	Majlis Agama Islam Negeri Pulau Pinang
Platform	PHP, MySQL, XAMPP, HTML/CSS/JavaScript
Database	audit_system
Tarikh Dokumentasi	18/05/2026

Nota Keselamatan: Akaun lalai pembangunan perlu ditukar kata laluan sebelum sistem digunakan secara rasmi.

1. Pengenalan Sistem

Dashboard Audit MAINPP ialah sistem dalaman untuk mengurus pendaftaran maklumat audit, tugas kepada bahagian/unit, maklum balas audit, catatan audit, kelulusan status audit, notifikasi, capaian pengguna dan transaksi log pengguna.

- Memusatkan rekod audit dan tugas mengikut bahagian/unit.
- Membolehkan bahagian terlibat menghantar maklum balas dan lampiran.
- Membolehkan Admin Audit memberi catatan audit dan menilai status Selesai Audit.
- Menyediakan kawalan capaian berdasarkan bahagian dan pengguna individu.
- Merekod aktiviti utama pengguna untuk tujuan jejak audit.

2. Peranan Pengguna

Role	Skop Utama	Keterangan
Pentadbir Sistem	Kawalan sistem penuh	Mengurus capaian bahagian, capaian pengguna, pengguna, status akaun dan konfigurasi akses.
Admin Audit	Pengurusan audit	Mendaftarkan audit, menyemak maklum balas, memberi catatan audit dan mengemaskini kelulusan audit.
Pengguna Biasa	Maklum balas bahagian	Melihat audit yang ditugaskan kepada bahagian dan menghantar/kemaskini maklum balas dalam tempoh audit.

3. Modul Sistem

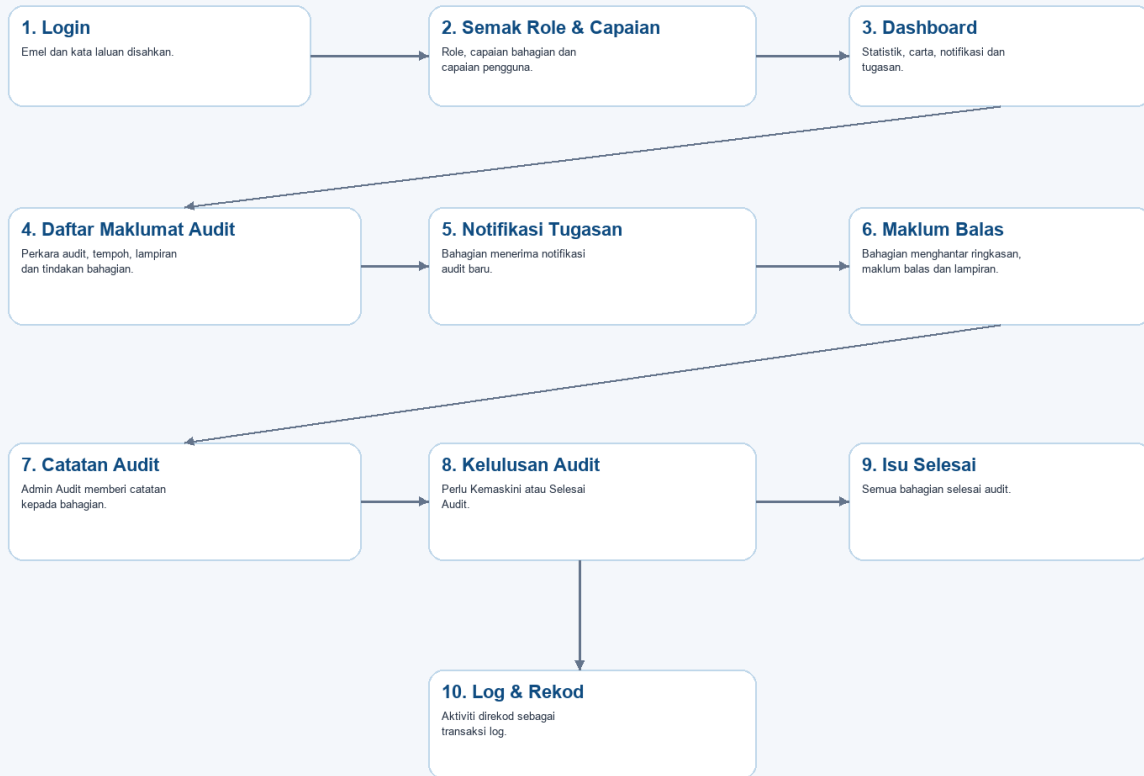
Modul	Fungsi
Dashboard	Statistik audit, isu selesai/belum selesai, carta dan tugas.
Daftar Maklumat Audit	Daftar/kemaskini perkara audit, tempoh, lampiran dan tindakan bahagian.
Senarai Maklumat Audit	Senarai audit dengan filter dan tindakan edit/view/delete.
Senarai Maklum Balas Audit	Senarai maklum balas, lampiran dan tarikh kemaskini.
Pengurusan Pendaftaran	Kelulusan atau penolakan akaun pengguna baharu.
Senarai Pengguna	Paparan pengguna, role, bahagian dan status akaun.
Capaian Pengguna/Bahagian	Tetapan CRUD dan rollback berdasarkan bahagian serta pengguna individu.
Transaksi Log Pengguna	Rekod aktiviti pengguna.
Notifikasi	Makluman tugas audit dan catatan audit.
Profile Pengguna	Kemaskini profil dan kata laluan.
Lupa Kata Laluan	Reset password menggunakan emel, IC dan kod verifikasi SMTP.

4. Flow Chart Sistem

Rajah berikut menunjukkan aliran utama operasi audit daripada login hingga rekod audit selesai dan direkodkan.

Flow Chart Operasi Audit

Aliran utama daripada login hingga audit selesai

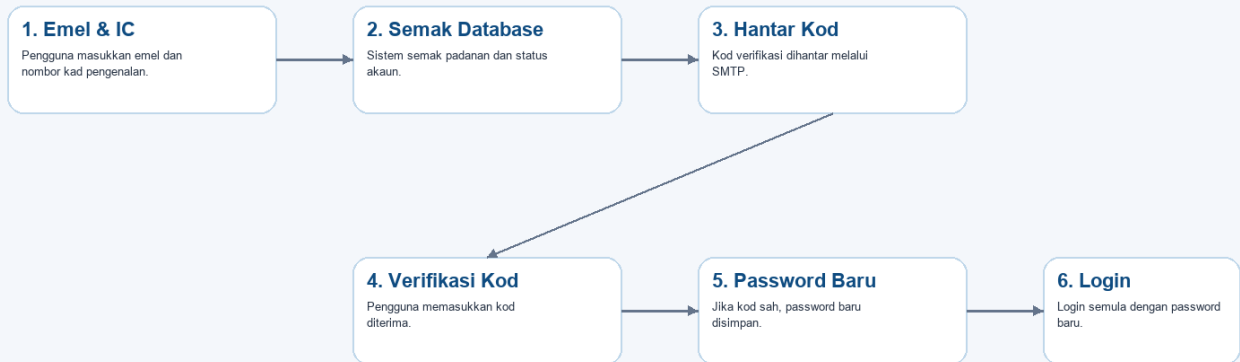


5. Flow Chart Lupa Kata Laluan

Flow ini digunakan apabila pengguna terlupa kata laluan dan perlu mengesahkan emel serta nombor kad pengenalan.

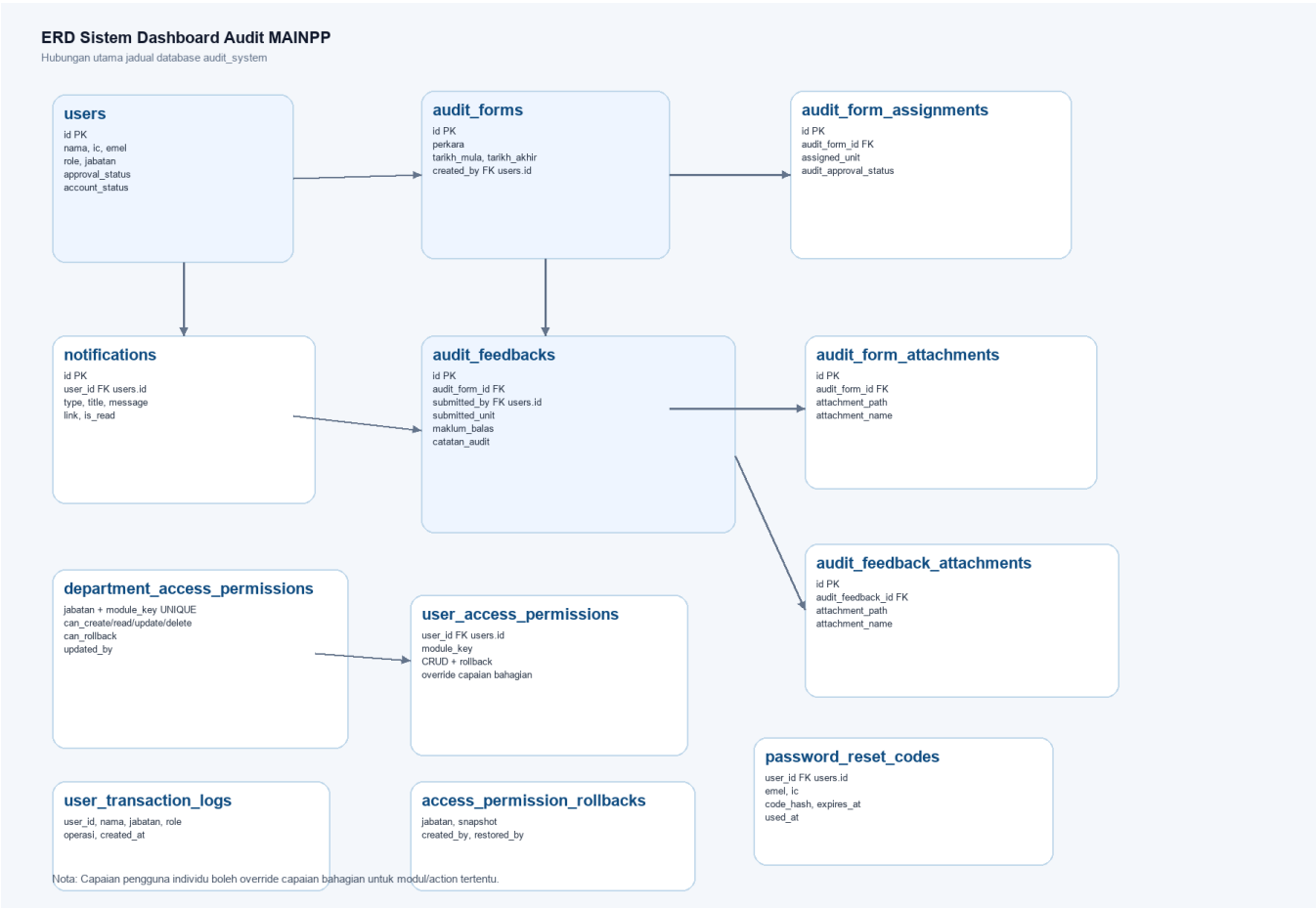
Flow Chart Lupa Kata Laluan

Reset kata laluan menggunakan emel, IC dan kod verifikasi



6. Entity Relationship Diagram (ERD)

ERD berikut memaparkan hubungan jadual utama dalam database audit_system.



7. Struktur Database

Jadual	Tujuan
users	Pengguna, role, bahagian, status akaun dan password hash.
audit_forms	Rekod utama maklumat audit.
audit_form_assignments	Bahagian/unit ditugaskan dan status audit setiap bahagian.
audit_form_attachments	Lampiran maklumat audit.
audit_feedbacks	Maklum balas, catatan audit dan metadata pengguna.
audit_feedback_attachments	Lampiran tambahan maklum balas.
notifications	Notifikasi sistem kepada pengguna.
department_access_permissions	Capaian modul/action berdasarkan bahagian.
user_access_permissions	Override capaian bagi pengguna individu.
department_access_permission_rollbacks	Snapshot capaian untuk rollback.
password_reset_codes	Kod reset kata laluan dan tempoh sah.
user_transaction_logs	Jejak transaksi pengguna.

8. Kawalan Capaian

Kawalan capaian menggunakan gabungan role, capaian bahagian dan capaian pengguna individu. Jika tetapan pengguna individu wujud, ia akan override capaian bahagian untuk modul/action tersebut.

- Pentadbir Sistem mempunyai capaian penuh.
- Admin Audit dan Pengguna Biasa tertakluk kepada permission modul.
- Action yang digunakan ialah Create, Read, Update, Delete dan Rollback.
- Modul Daftar Pengguna menggunakan Create dan Read; Pengurusan Pendaftaran menggunakan Read dan Update.

9. Peraturan Perniagaan Utama

- Maklum balas belum boleh diisi sebelum tarikh mula audit.
- Maklum balas tidak boleh diisi atau dikemaskini selepas tarikh akhir audit tamat.
- Kelulusan audit setiap bahagian boleh ditetapkan kepada Perlu Kemaskini atau Selesai Audit.
- Isu selesai dikira apabila status bahagian ialah Selesai Audit.
- Admin Audit tidak dibenarkan mengubah role Pentadbir Sistem.
- Notifikasi dihantar apabila audit ditugaskan dan apabila catatan audit diberikan.

10. Keselamatan dan Sesi

Komponen	Keterangan
Password Hash	Password disimpan menggunakan hash PHP.
SMTP Reset Password	Kod verifikasi dihantar melalui email.
Session Timeout	Amaran sesi tamat dipaparkan dan pengguna boleh sambung sesi.
Account Status	Akaun pending/rejected/inactive tidak boleh login.
Transaction Log	Aktiviti penting direkod untuk audit trail.

11. Akaun Lalai Pembangunan

Role	Emel	Nota
Admin Audit	admin@mainpp.gov.my	Tukar kata laluan sebelum production.
Pentadbir Sistem	superadmin@mainpp.gov.my	Tukar kata laluan sebelum production.

12. Cadangan Penambahbaikan

- Aktifkan HTTPS apabila sistem ditempatkan pada server rasmi.
- Hadkan cubaan login dan reset password.
- Tambah backup berkala database audit_system dan folder uploads.
- Sediakan SOP pentadbiran capaian pengguna dan semakan permission berkala.

13. Objektif Sistem

Objektif utama Dashboard Audit MAINPP adalah untuk menyediakan satu platform berpusat yang memudahkan proses pengurusan audit, pemantauan tindakan bahagian dan rekod transaksi pengguna secara lebih sistematik.

- Mengurangkan kebergantungan kepada rekod manual atau fail berasingan.
- Memastikan tugas audit boleh dijejaki mengikut bahagian/unit yang bertanggungjawab.
- Mempercepat proses semakan maklum balas dan catatan audit oleh Admin Audit.
- Meningkatkan kawalan capaian melalui permission berdasarkan bahagian dan pengguna individu.
- Menyediakan laporan ringkas melalui dashboard, carta dan bilangan isu selesai/belum selesai.
- Mewujudkan jejak audit melalui transaksi log pengguna.

14. Skop Sistem

Skop	Termasuk	Tidak Termasuk / Cadangan Masa Hadapan
Pengurusan Audit	Daftar audit, kemaskini audit, tugas bahagian, lampiran dan senarai audit.	Integrasi terus dengan sistem pengurusan dokumen rasmi.
Maklum Balas Bahagian	Isi ringkasan, maklum balas, lampiran dan kemaskini dalam tempoh audit.	Workflow kelulusan bertingkat lebih daripada satu peringkat.
Catatan Audit	Admin Audit memberi catatan kepada maklum balas bahagian.	E-signature atau pengesahan digital rasmi.
Capaian Pengguna	CRUD dan rollback mengikut bahagian serta override pengguna individu.	Integrasi SSO/LDAP/Active Directory.
Notifikasi	Notifikasi tugas audit dan catatan audit dalam sistem.	Push notification mobile atau WhatsApp rasmi.
Reset Kata Laluan	SMTP email dengan kod verifikasi.	MFA/OTP aplikasi authenticator.

15. Spesifikasi Modul Terperinci

Modul	Spesifikasi
Dashboard	Memaparkan kad statistik, carta palang isu mengikut bahagian, carta pai status isu dan carta bar isu belum selesai. Untuk pengguna biasa, statistik difokuskan kepada bahagian sendiri.
Daftar Maklumat Audit	Merekod perkara audit, tarikh mula, tarikh akhir, ringkasan audit, lampiran fail dan tindakan bahagian/unit. Sistem menghantar notifikasi kepada bahagian yang ditugaskan.
Senarai Maklumat Audit	Menyediakan filter berdasarkan perkara, bahagian/unit, tempoh audit, status tindakan dan tarikh. Menyokong view, edit dan delete bergantung kepada capaian.
Maklum Balas Audit	Bahagian yang ditugaskan boleh mengisi ringkasan, maklum balas dan lampiran. Sistem menghalang input sebelum tarikh mula dan selepas tarikh akhir.
Detail Maklum Balas Audit	Admin Audit boleh melihat detail maklum balas dan memberi catatan audit. Edit/delete telah dibuang daripada detail mengikut keperluan semasa.
Capaian Bahagian	Pentadbir Sistem menetapkan permission modul kepada semua pengguna dalam bahagian yang dipilih.
Capaian Pengguna	Pentadbir Sistem menetapkan permission individu yang

	boleh override permission bahagian.
Profile Pengguna	Pengguna boleh mengemaskini nama, emel, bahagian/unit dan kata laluan.

16. SOP Operasi Harian

16.1 SOP Admin Audit

1. Login sebagai Admin Audit.
2. Daftar maklumat audit dan pilih tindakan bahagian.
3. Semak senarai maklum balas audit yang diterima.
4. Buka detail maklum balas untuk menyemak ringkasan, lampiran dan maklum balas.
5. Masukkan catatan audit jika perlu pembetulan atau pengesahan.
6. Tukar kelulusan audit bahagian kepada Selesai Audit apabila tindakan lengkap.
7. Pantau bilangan isu belum selesai dan selesai di dashboard.

16.2 SOP Pengguna Bahagian

8. Login sebagai Pengguna Biasa.
9. Semak dashboard untuk melihat audit yang ditugaskan kepada bahagian.
10. Buka audit yang memerlukan maklum balas.
11. Isi ringkasan, maklum balas dan lampiran dalam tempoh audit.
12. Kemaskini maklum balas jika menerima catatan audit daripada Admin Audit.
13. Pantau status sehingga audit disahkan selesai.

16.3 SOP Pentadbir Sistem

14. Semak pendaftaran pengguna baharu dan aktifkan akaun yang sah.
15. Tetapkan capaian bahagian mengikut modul dan action.
16. Tetapkan capaian individu jika terdapat pengecualian khas.
17. Semak transaksi log pengguna secara berkala.
18. Urus role dan status akaun pengguna, kecuali perlindungan role Pentadbir Sistem.
19. Semak backup database dan folder uploads.

17. Jadual Permission Modul

Modul	Create	Read	Update	Delete	Rollback	Catatan
Senarai Maklum Balas Audit	Ya	Ya	Ya	Ya	Ya	Kawalan kepada senarai, detail dan catatan audit.
Senarai Maklumat Audit	Ya	Ya	Ya	Ya	Ya	Termasuk daftar, edit, view dan padam maklumat audit.
Daftar Pengguna	Ya	Ya	Tidak	Tidak	Tidak	Hanya create dan read sesuai untuk borang daftar pengguna.
Pengurusan	Tidak	Ya	Ya	Tidak	Tidak	Kelulusan

Pendaftaran						atau penolakan akaun pengguna baharu.
Senarai Pengguna	Ya	Ya	Ya	Ya	Ya	Pengurusan role dan status akaun bergantung capaian.
Transaksi Log Pengguna	Ya	Ya	Ya	Ya	Ya	Biasanya read sahaja diberi kepada pihak tertentu.

18. Kamus Data Ringkas

18.1 users

Field	Jenis	Keterangan
id	INT UNSIGNED PK	ID unik pengguna.
nama	VARCHAR(150)	Nama penuh pengguna.
ic	VARCHAR(20)	Nombor kad pengenalan unik.
emel	VARCHAR(150)	Emel unik untuk login dan reset password.
role	ENUM	Pengguna Biasa, Admin Audit atau Pentadbir Sistem.
jabatan	VARCHAR(150)	Bahagian/unit pengguna.
approval_status	ENUM	pending, active atau rejected.
account_status	ENUM	active atau inactive.
password	VARCHAR(255)	Hash kata laluan.

18.2 audit_forms

Field	Jenis	Keterangan
id	INT UNSIGNED PK	ID rekod audit.
perkara	VARCHAR(255)	Tajuk/perkara audit.
tarikh_mula	DATE	Tarikh mula tempoh maklum balas.
tarikh_akhir	DATE	Tarikh akhir tempoh maklum balas.
remarks	TEXT	Ringkasan perkara audit.
audit_approval_status	ENUM	Status umum audit.
created_by	FK users.id	Pengguna yang mendaftarkan audit.

18.3 audit_feedbacks

Field	Jenis	Keterangan
audit_form_id	FK audit_forms.id	Audit berkaitan.
submitted_by	FK users.id	Pengguna yang menghantar maklum balas.
submitted_unit	VARCHAR(150)	Bahagian/unit penghantar.
ringkasan	VARCHAR(255)	Ringkasan maklum balas.
maklum_balas	TEXT	Maklum balas penuh.
catatan_audit	TEXT	Catatan daripada Admin Audit.
attachment_path	VARCHAR(255)	Lokasi lampiran.
updated_at	TIMESTAMP	Tarikh hantar/kemaskini terkini.

19. Validasi dan Peraturan Sistem

Kawasan	Validasi / Peraturan
Login	Emel dan password mesti sepadan; akaun pending, rejected atau inactive tidak dibenarkan login.
Daftar Audit	Tarikh akhir mesti sama atau selepas tarikh mula.
Lampiran	Format dibenarkan: PDF, Word, Excel, JPG, JPEG dan PNG.
Maklum Balas	Hanya bahagian ditugaskan boleh mencipta maklum balas.
Tempoh Audit	Maklum balas disekat sebelum tarikh mula dan selepas tarikh akhir.
Reset Password	Emel dan IC mesti wujud; kod verifikasi sah selama 15 minit.
Role	Admin Audit tidak boleh mengubah role Pentadbir Sistem.

20. Notifikasi Sistem

Jenis Notifikasi	Penerima	Pencetus	Keterangan
audit_assigned	Pengguna dalam bahagian ditugaskan	Audit baru didaftarkan atau ditugaskan	Memaklumkan terdapat perkara audit yang memerlukan tindakan.
catatan_audit	Bahagian yang menghantar maklum balas	Admin Audit menyimpan catatan audit	Memaklumkan bahagian bahawa terdapat catatan audit baharu.
header notification	Pengguna berkaitan	Rekod notification belum dibaca	Dipaparkan di ikon loceng header.

21. Backup dan Penyelenggaraan

- Backup database audit_system sekurang-kurangnya sekali sehari atau mengikut polisi ICT organisasi.
- Backup folder uploads/audit dan uploads/maklum_balas kerana lampiran tidak disimpan terus dalam database.
- Simpan salinan SQL dan uploads di lokasi berasingan daripada server aplikasi.
- Uji proses restore secara berkala supaya backup benar-benar boleh digunakan.
- Semak saiz folder uploads dan arkib lampiran lama jika polisi organisasi membenarkan.

22. Deployment Ringkas

Langkah	Keterangan
1. Sediakan Server	Pasang Apache/PHP/MySQL atau gunakan XAMPP untuk persekitaran tempatan.
2. Salin Kod	Letakkan folder audit di htdocs atau document root server.
3. Import Database	Import audit_system.sql atau biarkan includes/app.php bootstrap schema.
4. Konfigurasi SMTP	Pastikan konfigurasi email reset password berfungsi.
5. Semak Permission Folder	Pastikan folder uploads boleh ditulis oleh web server.
6. Tukar Password Lalai	Tukar password akaun admin dan superadmin selepas

	deployment.
7. Ujian Akhir	Uji login, daftar audit, maklum balas, notifikasi, reset password dan capaian pengguna.

23. Senarai Ujian Penerimaan Pengguna (UAT)

No.	Senario Ujian	Jangkaan Keputusan
1	Login menggunakan akaun aktif.	Pengguna berjaya masuk ke dashboard.
2	Login akaun inactive/pending.	Sistem menolak login dengan mesej sesuai.
3	Daftar audit baru dan pilih beberapa bahagian.	Audit disimpan dan notifikasi dihantar kepada bahagian.
4	Bahagian isi maklum balas dalam tempoh audit.	Maklum balas disimpan dan tarikh hantar dikemaskini.
5	Bahagian cuba isi maklum balas selepas tarikh akhir.	Sistem menyekat proses.
6	Admin Audit beri catatan audit.	Catatan disimpan dan notifikasi dipaparkan kepada bahagian.
7	Pentadbir Sistem ubah capaian bahagian.	Permission bahagian dikemaskini.
8	Pentadbir Sistem ubah capaian pengguna individu.	Permission individu override permission bahagian.
9	Reset password dengan emel dan IC sah.	Kod verifikasi dihantar dan password baru boleh disimpan.
10	Semak transaksi log.	Aktiviti penting pengguna direkod.

24. Risiko dan Kawalan

Risiko	Kesan	Kawalan Dicadangkan
Password lalai tidak ditukar	Akaun admin boleh diakses pihak tidak dibenarkan.	Wajib tukar password selepas deployment.
Tiada HTTPS	Data login boleh terdedah dalam rangkaian tidak selamat.	Gunakan SSL/TLS di server production.
Backup tidak konsisten	Data audit dan lampiran boleh hilang.	Jadual backup automatik dan ujian restore.
Permission terlalu luas	Pengguna boleh mengakses modul tidak berkaitan.	Semakan capaian berkala oleh Pentadbir Sistem.
Lampiran terlalu besar	Storage server cepat penuh.	Had saiz fail dan polisi arkib.

25. Penutup

Dokumentasi ini menerangkan fungsi utama, struktur data, aliran proses dan kawalan keselamatan bagi Dashboard Audit MAINPP. Dokumen ini boleh dijadikan rujukan pembangunan, latihan pengguna, UAT dan penyelenggaraan sistem pada masa hadapan.

Carta alir ini disediakan dalam bentuk menegak seperti carta proses rasmi. Ia menunjukkan peranan Admin Audit, Bahagian/Unit, Pentadbir Sistem dan Sistem dari mula login sehingga audit selesai. Simbol berlian menunjukkan keputusan sistem seperti semakan tarikh mula, tarikh akhir dan status maklum balas.



27. Penerangan Terperinci Aliran Login dan Kawalan Sesi

Semasa pengguna membuka sistem, proses login menjadi pintu kawalan pertama sebelum sebarang modul boleh dicapai. Sistem menerima emel dan kata laluan, kemudian membuat semakan ke atas jadual users. Semakan bukan hanya tertumpu kepada padanan kata laluan, tetapi turut mengambil kira status kelulusan dan status akaun. Ini penting kerana pengguna yang masih pending, ditolak atau dinyahaktifkan tidak sepatutnya boleh masuk ke dashboard walaupun emel dan kata laluan adalah betul.

Selepas login berjaya, sistem menyimpan maklumat penting di dalam session seperti user_id, nama, emel, role dan jabatan. Maklumat session ini digunakan oleh hampir semua modul untuk menentukan paparan, filter data, capaian modul dan log transaksi. Session juga mempunyai mekanisme amaran tamat sesi supaya akaun tidak dibiarkan aktif terlalu lama tanpa kawalan.

Kawalan sesi turut disambung dengan fungsi keepalive. Apabila amaran sesi tamat dipaparkan, pengguna boleh memilih untuk meneruskan sesi atau log keluar. Jika sesi diteruskan, sistem mengemaskini masa aktiviti terakhir dan memuat semula halaman. Ini membantu mengurangkan risiko pengguna kehilangan kerja kerana sesi tamat secara mengejut.

28. Penerangan Terperinci Dashboard Mengikut Role

Dashboard bukan sekadar halaman utama, tetapi menjadi pusat pemantauan status audit. Untuk Pentadbir Sistem dan Admin Audit, dashboard memaparkan statistik keseluruhan seperti jumlah audit, bilangan isu belum selesai, bilangan isu selesai dan tugas semasa. Carta palang memaparkan perbandingan isu selesai dan belum selesai mengikut bahagian/unit.

Untuk Pengguna Biasa, dashboard difokuskan kepada bahagian pengguna tersebut sahaja. Kad jumlah audit memaparkan audit yang ditugaskan kepada bahagian pengguna, manakala kad isu belum selesai dan isu selesai hanya mengambil kira status audit_assignment bahagian tersebut. Pendekatan ini menjadikan dashboard lebih relevan dan mengelakkan pengguna biasa melihat statistik yang tidak berkaitan dengan tanggungjawab bahagian mereka.

Carta pai digunakan untuk memberi gambaran ringkas nisbah isu selesai dan belum selesai. Carta bar pula membantu pentadbir mengenal pasti bahagian yang mempunyai isu belum selesai paling banyak. Gabungan kad statistik dan carta menjadikan dashboard sesuai untuk pemantauan harian serta mesyuarat ringkas status audit.

29. Penerangan Terperinci Daftar Maklumat Audit

Modul daftar maklumat audit digunakan untuk mencipta rekod audit baharu. Admin Audit atau pengguna yang mempunyai capaian create akan memasukkan perkara audit, tarikh mula, tarikh akhir, ringkasan perkara audit, lampiran dan tindakan bahagian. Bahagian yang dipilih akan direkodkan dalam jadual `audit_form_assignments`.

Tarikh mula dan tarikh akhir memainkan peranan penting kerana ia mengawal bila bahagian boleh menghantar maklum balas. Jika tarikh mula belum tiba, sistem menghalang maklum balas daripada dihantar. Jika tarikh akhir telah tamat, sistem juga menghalang kemaskini maklum balas. Ini memastikan semua tindakan mematuhi tempoh audit yang ditetapkan.

Selepas audit didaftarkan, sistem menghantar notifikasi kepada pengguna dalam bahagian yang ditugaskan. Notifikasi ini membantu memastikan bahagian menyedari terdapat tindakan baharu tanpa perlu menyemak dashboard secara manual setiap masa.

30. Penerangan Terperinci Maklum Balas Audit

Maklum balas audit merupakan komponen utama yang menghubungkan bahagian terlibat dengan Admin Audit. Pengguna dalam bahagian yang ditugaskan boleh menghantar ringkasan, maklum balas lengkap dan lampiran sokongan. Rekod ini disimpan dalam jadual `audit_feedbacks` dan dikaitkan dengan `audit_forms` melalui `audit_form_id`.

Sistem memastikan hanya bahagian yang terlibat boleh mencipta maklum balas bagi audit tersebut. Jika maklum balas telah wujud, sistem akan mengemaskini rekod sedia ada dan tarikh `updated_at` akan menjadi tarikh hantar terkini. Ini membolehkan senarai maklum balas audit memaparkan tarikh kemaskini sebenar, bukan hanya tarikh pertama kali diisi.

Jika Admin Audit memberi catatan audit, bahagian boleh menggunakan catatan tersebut sebagai panduan untuk membuat pembetulan. Proses ini mewujudkan kitaran komunikasi antara audit dan bahagian sehingga maklum balas diterima sebagai memuaskan.

31. Penerangan Terperinci Catatan Audit dan Kelulusan Audit

Catatan audit digunakan oleh Admin Audit untuk memberi komen, arahan pembetulan atau pengesahan terhadap maklum balas bahagian. Catatan ini disimpan bersama maklumat siapa yang memberi catatan dan masa catatan diberikan. Apabila catatan disimpan, sistem menghantar notifikasi kepada pengguna dalam bahagian berkaitan.

Kelulusan audit dibuat mengikut bahagian, bukan secara umum sahaja. Ini bermaksud setiap bahagian yang ditugaskan boleh mempunyai status berbeza. Status Perlu Kemaskini menunjukkan isu masih belum selesai, manakala status Selesai Audit menunjukkan bahagian tersebut telah memenuhi keperluan audit.

Pengiraan bilangan isu selesai dan belum selesai bergantung kepada status `audit_approval_status` di `audit_form_assignments`. Jika semua bahagian untuk sesuatu audit telah selesai, audit tersebut boleh dianggap selesai dari sudut operasi. Jika masih ada sekurang-kurangnya satu bahagian belum selesai, audit tersebut masih dikira mempunyai isu belum selesai.

32. Penerangan Terperinci Notifikasi

Notifikasi membantu pengguna mengetahui tindakan yang perlu dibuat tanpa bergantung sepenuhnya kepada semakan manual. Sistem menyimpan notifikasi dalam jadual notifications dengan maklumat `user_id`, `type`, `title`, `message`, `link`, `status` dibaca dan masa dicipta.

Notifikasi tugas audit dihantar apabila audit didaftarkan kepada bahagian tertentu. Notifikasi catatan audit dihantar apabila Admin Audit memberikan catatan kepada maklum balas bahagian. Notifikasi ini dipaparkan pada ikon loceng di header dan juga boleh dilihat dalam halaman Notifikasi.

Halaman Notifikasi menyediakan ringkasan jumlah notifikasi, notifikasi belum dibaca dan notifikasi sudah dibaca. Pengguna boleh memilih notifikasi untuk ditandakan sebagai dibaca atau dipadam. Reka bentuk ini membantu pengguna mengurus maklumat tindakan dengan lebih teratur.

33. Penerangan Terperinci Capaian Bahagian dan Capaian Pengguna

Capaian bahagian membolehkan Pentadbir Sistem menetapkan permission kepada semua pengguna dalam satu bahagian. Tetapan ini sesuai apabila semua pengguna dalam bahagian mempunyai tugas yang sama. Permission yang disediakan ialah Create, Read, Update, Delete dan Rollback, bergantung kepada modul.

Capaian pengguna pula digunakan apabila terdapat pengecualian khas untuk seorang pengguna. Jika rekod capaian pengguna wujud bagi modul dan action tertentu, sistem akan menggunakan tetapan pengguna tersebut dan mengatasi tetapan bahagian. Ini memberi fleksibiliti tanpa perlu mencipta role baharu untuk kes kecil.

Rollback disediakan supaya perubahan capaian bahagian boleh dikembalikan kepada snapshot sebelumnya. Ciri ini penting kerana tetapan permission yang salah boleh menyebabkan pengguna tidak dapat mengakses modul penting atau mendapat akses yang terlalu luas.

34. Penerangan Terperinci Pengurusan Pengguna

Modul pengurusan pengguna meliputi daftar pengguna, pengurusan pendaftaran, senarai pengguna, kemaskini role dan status akaun. Pengguna baharu yang mendaftar perlu melalui status kelulusan sebelum boleh login. Pentadbir boleh meluluskan atau menolak pendaftaran melalui modul Pengurusan Pendaftaran.

Senarai Pengguna memaparkan maklumat seperti nama, IC, emel, role, bahagian, status akaun dan status kelulusan. Admin Audit tidak dibenarkan mengubah role Pentadbir Sistem sebagai perlindungan struktur pentadbiran. Ini memastikan role tertinggi tidak boleh diubah oleh pihak yang tidak sepatutnya.

Status akaun active atau inactive digunakan untuk membenarkan atau menyekat login tanpa perlu memadam rekod pengguna. Pendekatan ini lebih baik kerana sejarah transaksi dan rekod berkaitan pengguna masih kekal dalam sistem.

35. Penerangan Terperinci Reset Kata Laluan

Fungsi lupa kata laluan bermula dengan pengguna memasukkan emel dan nombor kad pengenalan. Sistem akan menyemak sama ada padanan tersebut wujud dalam jadual users dan akaun berada dalam keadaan aktif. Jika semakan gagal, proses reset tidak diteruskan.

Jika semakan berjaya, sistem menjana kod verifikasi dan menyimpan hash kod tersebut dalam jadual password_reset_codes. Kod asal dihantar melalui email SMTP kepada pengguna. Kod mempunyai tempoh sah tertentu supaya tidak boleh digunakan selepas tamat masa.

Pengguna perlu memasukkan kod verifikasi yang betul sebelum dibenarkan menetapkan kata laluan baharu. Selepas kata laluan baharu disimpan, kod ditanda sebagai telah digunakan. Ini mengurangkan risiko kod lama digunakan semula oleh pihak lain.

36. Penerangan Terperinci Transaksi Log Pengguna

Transaksi log pengguna berfungsi sebagai audit trail kepada aktiviti penting sistem. Setiap aktiviti seperti login, daftar audit, kemaskini audit, simpan maklum balas, perubahan capaian dan tindakan pentadbiran boleh direkodkan bersama nama, jabatan, role dan masa aktiviti.

Log ini membantu pentadbir membuat semakan apabila berlaku isu seperti perubahan data yang tidak dijangka, akses tidak sah atau pertikaian berkaitan siapa yang melakukan tindakan tertentu. Walaupun log bukan pengganti kawalan keselamatan, ia adalah lapisan penting untuk pemantauan dan akauntabiliti.

Dalam persekitaran production, log perlu disimpan dengan polisi retention yang jelas. Contohnya, log boleh disimpan sekurang-kurangnya satu tahun atau mengikut keperluan organisasi. Jika saiz log meningkat, arkib berkala boleh dibuat tanpa menghapuskan rekod penting.

37. Penerangan Terperinci Struktur Fail Sistem

Struktur fail sistem dibina menggunakan PHP biasa dengan fail proses yang berasingan daripada fail paparan. Fail `includes/app.php` mengandungi sambungan database, bootstrap schema, fungsi semakan role, fungsi notifikasi, fungsi capaian dan fungsi umum lain. Fail `includes/layout.php` pula mengurus header, sidebar, modal sesi dan skrip layout.

Fail seperti `dashboard.php`, `senarai_maklumat_audit.php` dan `capaian_pengguna.php` bertindak sebagai halaman paparan utama. Fail proses seperti `proses_daftar_maklumat_audit.php`, `proses_maklum_balas_audit.php` dan `proses_capaian_pengguna.php` bertanggungjawab memproses data POST dan mengemaskini database.

Folder `uploads` digunakan untuk menyimpan lampiran audit dan maklum balas. Oleh sebab lampiran disimpan sebagai fail, backup sistem mesti merangkumi database dan folder `uploads`. Jika hanya database dibackup, pautan lampiran akan wujud tetapi fail sebenar mungkin hilang.

38. Penerangan Terperinci Database dan Relasi

Database audit_system menggunakan jadual users sebagai pusat identiti pengguna. Jadual audit_forms menyimpan rekod audit, manakala audit_form_assignments menyimpan bahagian yang ditugaskan kepada audit. Struktur ini membolehkan satu audit ditugaskan kepada banyak bahagian.

Jadual audit_feedbacks menyimpan maklum balas daripada pengguna atau bahagian yang berkaitan. Jadual audit_form_attachments dan audit_feedback_attachments menyimpan metadata lampiran seperti path dan nama fail. Fail sebenar berada dalam folder uploads.

Jadual department_access_permissions dan user_access_permissions membentuk lapisan authorization. Jadual notifications menyimpan notifikasi, password_reset_codes menyimpan kod reset kata laluan, dan user_transaction_logs menyimpan rekod aktiviti sistem.

39. Penerangan Terperinci Keselamatan

Keselamatan sistem bermula daripada kawalan login dan password hash. Password tidak disimpan dalam bentuk asal, sebaliknya disimpan sebagai hash. Semakan login dilakukan menggunakan password_verify supaya password asal tidak perlu didedahkan.

Kawalan role dan permission memastikan pengguna hanya boleh mencapai fungsi yang dibenarkan. Pentadbir Sistem mempunyai capaian penuh, manakala Admin Audit dan Pengguna Biasa tertakluk kepada capaian modul. Capaian individu boleh digunakan untuk kes pengecualian.

Sistem juga perlu dilindungi pada peringkat deployment. Penggunaan HTTPS, password yang kuat, backup berkala, kawalan akses server dan permission folder uploads adalah langkah penting sebelum sistem digunakan secara rasmi.

40. Penerangan Terperinci Deployment Production

Sebelum sistem dipindahkan ke production, pentadbir perlu memastikan versi PHP dan MySQL serasi dengan kod sistem. Folder audit perlu diletakkan dalam document root server dan konfigurasi database perlu disemak supaya sambungan berjaya.

Fail `audit_system.sql` boleh digunakan untuk menyediakan database awal. Sistem juga mempunyai bootstrap schema dalam `includes/app.php` yang membantu mencipta atau mengemaskini jadual. Walau bagaimanapun, untuk production, import SQL yang terkawal lebih disarankan supaya perubahan schema boleh direkodkan.

Selepas deployment, pentadbir perlu menukar password lalai admin dan superadmin, menguji SMTP, memastikan folder uploads boleh ditulis, dan menguji fungsi utama seperti login, daftar audit, maklum balas, notifikasi, reset password dan capaian pengguna.

41. Penerangan Terperinci UAT

Ujian penerimaan pengguna atau UAT perlu dilakukan sebelum sistem digunakan secara rasmi. UAT bertujuan memastikan fungsi sistem memenuhi keperluan pengguna sebenar dan bukan hanya lulus dari sudut teknikal. Setiap modul utama perlu diuji menggunakan akaun yang berbeza mengikut role.

Contoh ujian termasuk login akaun aktif, semakan akaun inactive, daftar audit baharu, isi maklum balas dalam tempoh, cuba isi maklum balas selepas tarikh akhir, beri catatan audit, tukar status Selesai Audit, ubah capaian bahagian dan reset kata laluan.

Keputusan UAT perlu direkodkan. Jika terdapat isu, pembetulan perlu dibuat dan ujian diulang. UAT dianggap selesai apabila fungsi kritikal berjalan dengan baik dan pengguna utama bersetuju sistem boleh digunakan.

Perkara penting yang perlu dipastikan:

- Semua tindakan kritikal perlu mempunyai rekod atau bukti yang boleh disemak semula.
- Pengguna perlu mengikut role dan capaian yang telah ditetapkan.
- Sebarang isu operasi perlu direkodkan supaya pembetulan boleh dibuat secara sistematik.

42. Penerangan Terperinci Backup dan Disaster Recovery

Backup sistem perlu merangkumi dua komponen utama iaitu database audit_system dan folder uploads. Database menyimpan rekod audit, pengguna, capaian dan log, manakala folder uploads menyimpan lampiran audit dan maklum balas. Kedua-duanya saling bergantung.

Backup boleh dibuat secara harian untuk database dan berkala untuk folder uploads bergantung kepada kadar penggunaan sistem. Salinan backup perlu disimpan di lokasi berasingan daripada server utama supaya masih boleh digunakan jika server mengalami kerosakan.

Disaster recovery perlu diuji dengan melakukan proses restore ke persekitaran ujian. Ujian restore memastikan backup bukan sahaja wujud, tetapi benar-benar boleh digunakan untuk mengembalikan sistem kepada keadaan operasi.

Perkara penting yang perlu dipastikan:

- Semua tindakan kritikal perlu mempunyai rekod atau bukti yang boleh disemak semula.
- Pengguna perlu mengikut role dan capaian yang telah ditetapkan.
- Sebarang isu operasi perlu direkodkan supaya pembetulan boleh dibuat secara sistematik.

43. Penerangan Terperinci Penyelenggaraan Berkala

Penyelenggaraan berkala perlu melibatkan semakan akaun pengguna, status akaun, role, permission bahagian dan permission individu. Akaun yang tidak lagi digunakan perlu dinyahaktifkan supaya tidak menjadi risiko keselamatan.

Pentadbir juga perlu menyemak transaksi log untuk mengenal pasti aktiviti luar biasa. Jika terdapat aktiviti yang mencurigakan, tindakan seperti menukar password, menyemak permission dan menyemak log server perlu dibuat.

Selain itu, folder uploads perlu dipantau supaya saiz storage tidak membesar tanpa kawalan. Jika organisasi mempunyai polisi arkib, lampiran lama boleh dipindahkan ke storan arkib dengan rekod yang jelas.

Perkara penting yang perlu dipastikan:

- Semua tindakan kritikal perlu mempunyai rekod atau bukti yang boleh disemak semula.
- Pengguna perlu mengikut role dan capaian yang telah ditetapkan.
- Sebarang isu operasi perlu direkodkan supaya pembetulan boleh dibuat secara sistematik.

44. Penerangan Terperinci Risiko Operasi

Risiko operasi utama sistem audit termasuk kehilangan data, permission yang salah, penggunaan password lemah, kegagalan SMTP dan folder uploads tidak boleh ditulis. Setiap risiko ini boleh memberi kesan langsung kepada operasi pengguna.

Permission yang terlalu luas boleh menyebabkan pengguna mengubah data yang bukan tanggungjawab mereka. Permission yang terlalu ketat pula boleh menyebabkan kerja audit terganggu kerana pengguna tidak boleh membuka modul yang diperlukan. Oleh itu, semakan permission berkala sangat penting.

Kegagalan SMTP akan memberi kesan kepada fungsi lupa kata laluan. Jika email tidak dihantar, pengguna tidak dapat reset password sendiri dan pentadbir perlu membantu secara manual. Oleh itu, konfigurasi SMTP perlu diuji selepas sebarang perubahan server.

45. Penerangan Terperinci Cadangan Penambahbaikan Masa Hadapan

Antara penambahbaikan yang boleh dipertimbangkan ialah integrasi Single Sign-On atau LDAP supaya pengguna boleh login menggunakan akaun organisasi. Ini mengurangkan keperluan mengurus password berasingan dalam sistem audit.

Sistem juga boleh ditambah fungsi laporan PDF atau Excel untuk memudahkan pelaporan kepada pihak pengurusan. Laporan boleh merangkumi bilangan audit mengikut tempoh, status isu mengikut bahagian, tempoh maklum balas dan audit yang lewat tindakan.

Penambahbaikan lain termasuk notifikasi email untuk tugas audit, had saiz lampiran, audit trail lebih terperinci untuk perubahan status, dan dashboard trend bulanan bagi memantau prestasi penyelesaian isu audit.

46. Kesimpulan Dokumentasi

Dokumentasi yang lebih terperinci ini menerangkan aspek fungsi, proses, kawalan, database, keselamatan, deployment dan penyelenggaraan Dashboard Audit MAINPP. Ia boleh digunakan sebagai rujukan pembangunan, latihan pengguna, UAT dan penyelenggaraan sistem.

Dengan adanya carta alir terperinci, pentadbir dan pengguna boleh memahami proses audit secara visual. Dengan adanya penerangan panjang bagi setiap modul, pasukan teknikal dan pengguna operasi mempunyai rujukan yang lebih jelas untuk mengendalikan sistem dengan konsisten.

Dokumen ini juga boleh dikemaskini dari semasa ke semasa apabila terdapat perubahan proses kerja, penambahan modul atau pindaan dasar keselamatan organisasi.

47. Checklist Operasi Sistem

Kategori	Semakan	Status Cadangan
Login	Akaun aktif boleh login dan akaun inactive ditolak.	Wajib diuji
Audit	Daftar audit, edit audit dan tugas bahagian berfungsi.	Wajib diuji
Maklum Balas	Bahagian boleh isi maklum balas dalam tempoh audit.	Wajib diuji
Tarikh	Maklum balas disekat sebelum mula dan selepas tamat.	Wajib diuji
Notifikasi	Notifikasi tugas dan catatan audit muncul di header.	Wajib diuji
Capaian	Permission bahagian dan pengguna individu berfungsi.	Wajib diuji
Reset Password	Kod verifikasi dihantar dan password baru boleh disimpan.	Wajib diuji
Backup	Database dan uploads mempunyai salinan backup.	Wajib disediakan
Keselamatan	Password lalai ditukar dan HTTPS diaktifkan.	Wajib production