

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

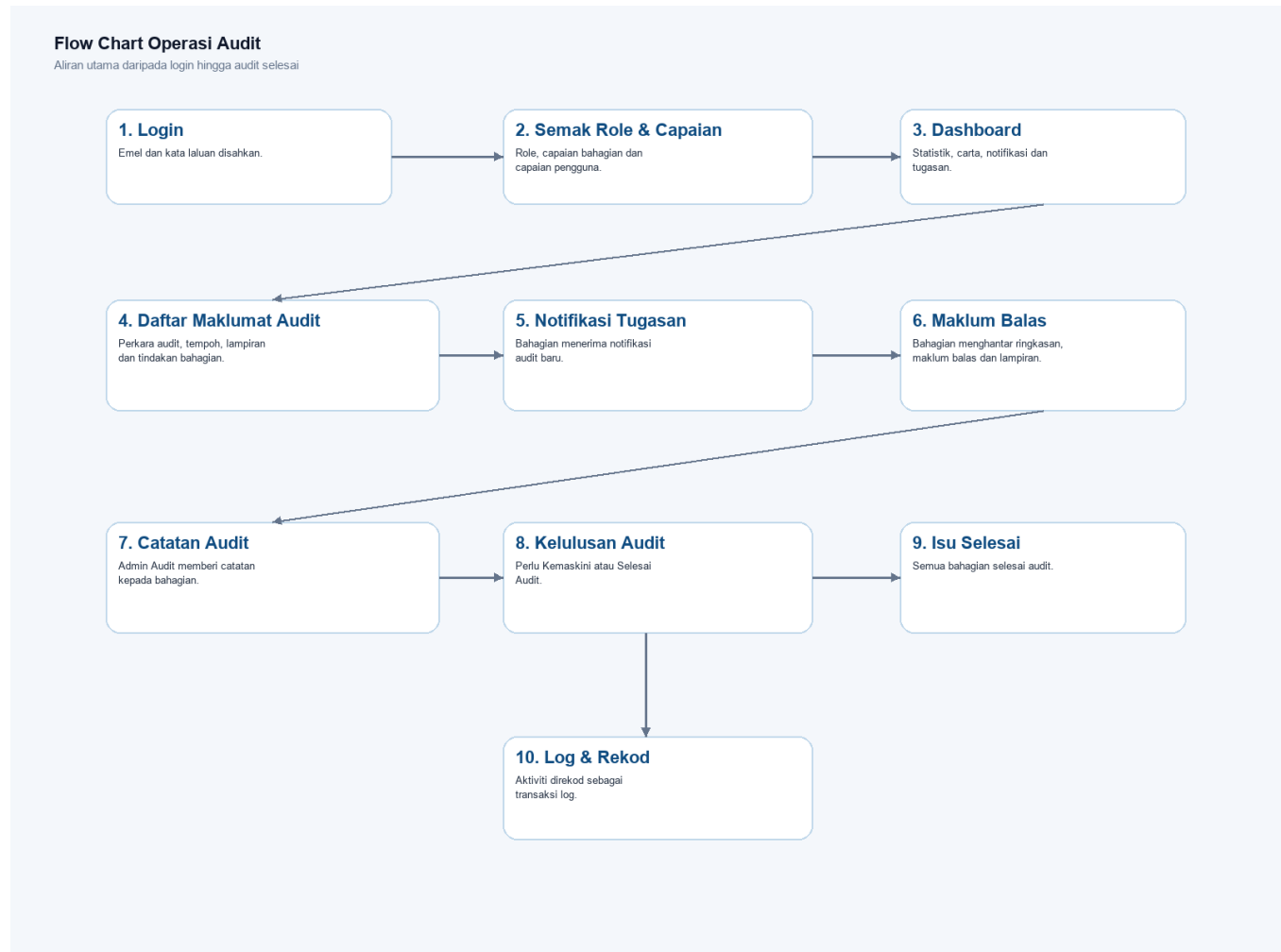
Role	Skop Utama	Keterangan
Pentadbir Sistem	Kawalan sistem penuh	Mengurus capaian bahagian, capaian pengguna, pengguna, status akaun dan konfigurasi akses.
Admin Audit	Pengurusan audit	Mendaftarkan audit, menyemak maklum balas, memberi catatan audit dan mengemaskini kelulusan audit.
Pengguna Biasa	Maklum 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.

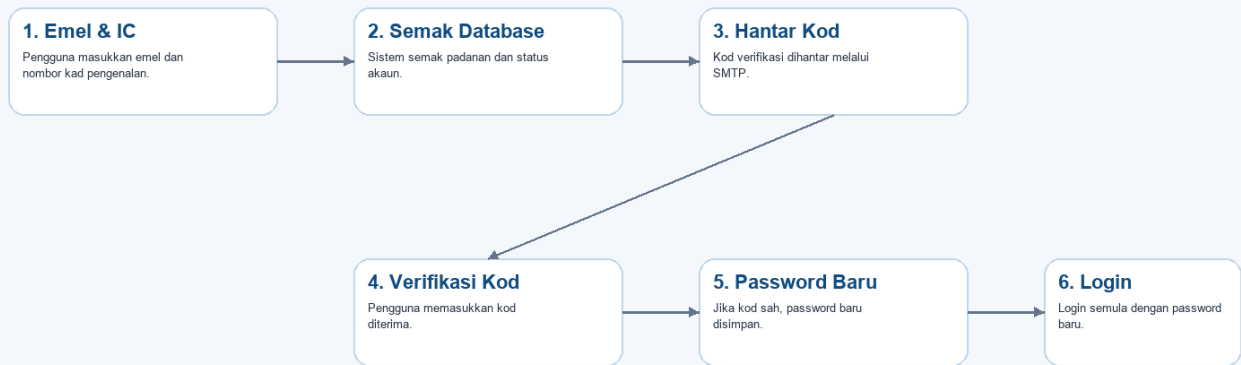


5. Flow Chart Lupa Kata Laluan

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

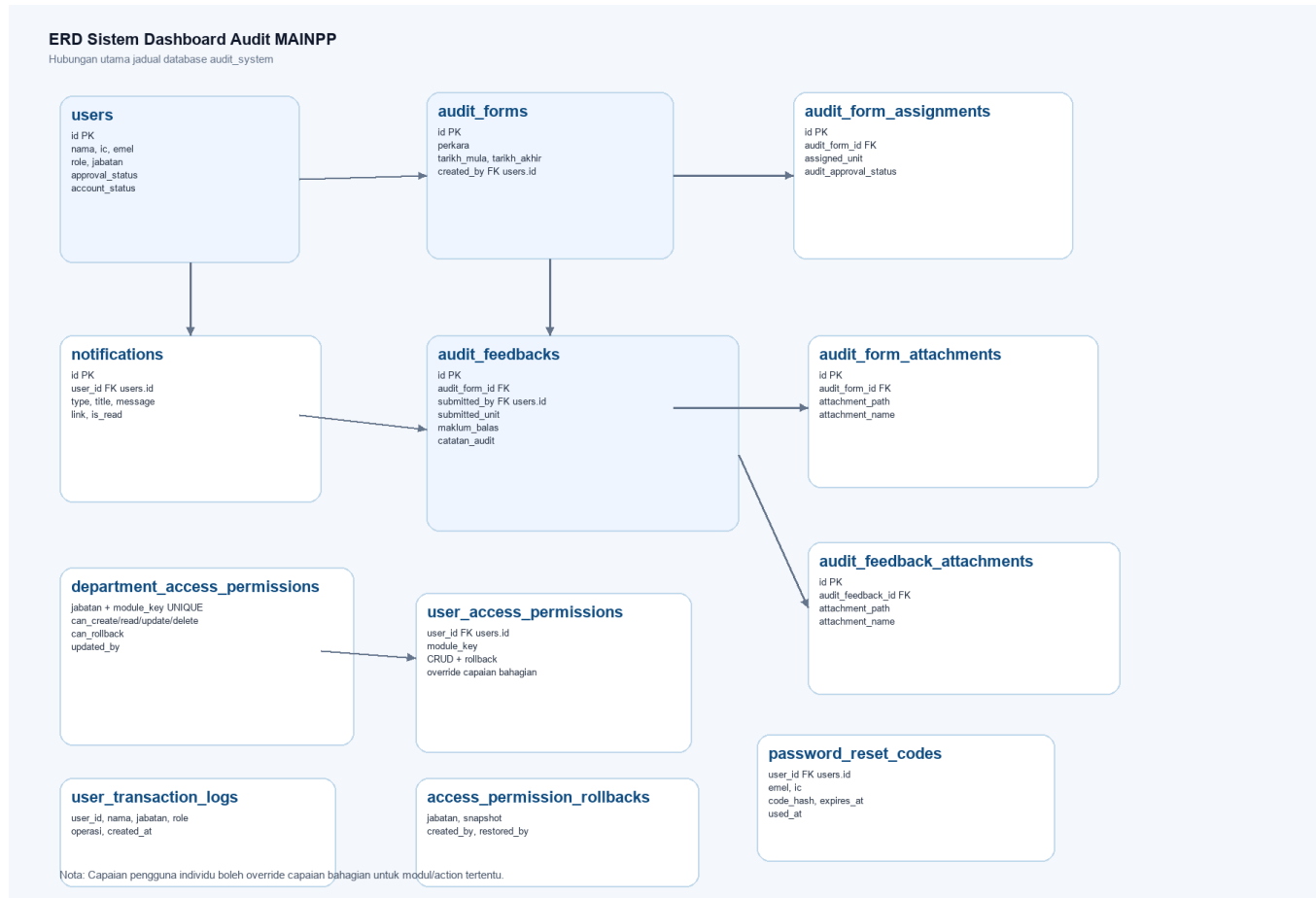
Flow Chart Lupa Kata Laluan

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.