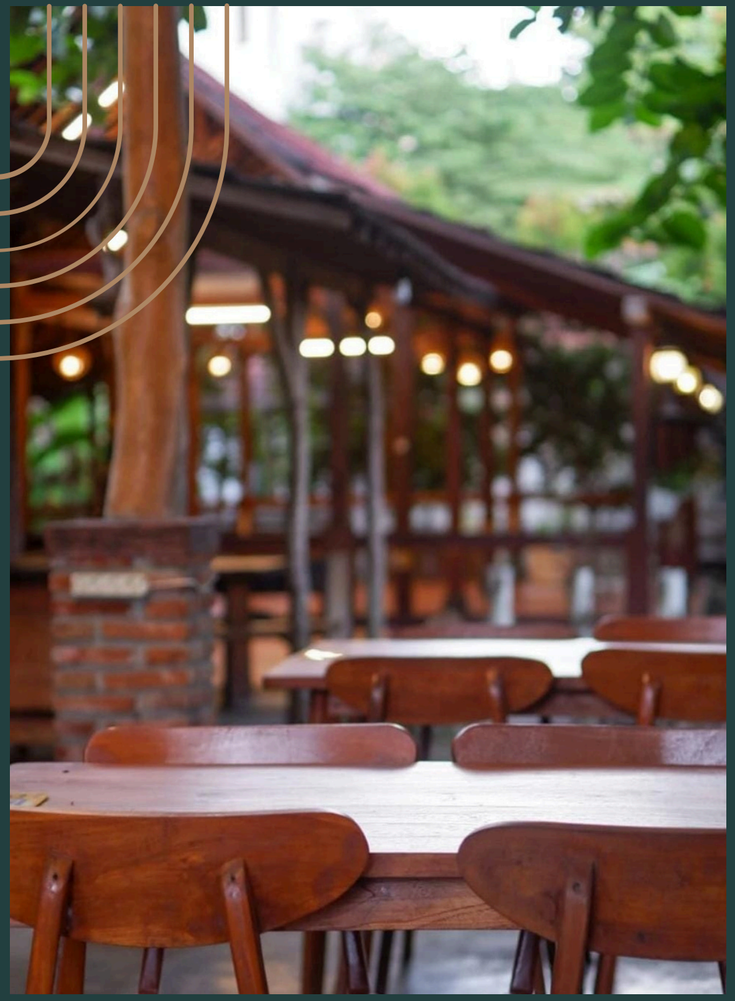
Audit Sistem Informasi Cafe Main-Main

Kelompok 1

Daftar Isi

Latar Belakang

Audit sistem informasi dilakukan untuk memastikan bahwa sistem kasir, pembayaran, dan jaringan yang digunakan oleh Café Main-Main berjalan aman dan efisien. Audit ini mengacu pada standar ISO/IEC 27001:2022 yang berfokus pada keamanan informasi, pengendalian akses, dan manajemen risiko.



Profil

Kafe Mainmain terletak di Jl. Sukun Raya No. 422, Banguntapan, Bantul, Yogyakarta. Kafe ini buka setiap hari pukul 09.00–02.00 WIB, menawarkan suasana santai dengan konsep semi-outdoor. Selain tempat nongkrong, kafe ini juga terhubung dengan toko buku, cocok untuk yang suka baca sambil ngopi.

Alasan Audit

- Untuk menjaga keamanan data transaksi
- Melindungi data pelanggan
- Mengevaluasi keamanan jaringan
- Memastikan efisiensi dan keandalan system
- Untuk kebutuhan manajerial dan Pengambilan keputusan

Ruang lingkup

Audit difokuskan pada:

- Sistem Point of Sale (POS) cafe
- Sistem pembayaran digital (QRIS, e-wallet, kartu)
- Jaringan Wi-Fi cafe (untuk pelanggan & internal staf)
- Data pelanggan (loyalty program)

Domain yang akan digunakan
pada audit cafe main-main

Domain	Subdomain	Fokus Audit
Keamanan Akses	Login individu per staf- Hak akses	Semua staf menggunakan login bersama
Manajemen Password	Kekuatan & pergantian password	Password kuat tapi tidak pernah diganti
Keamanan Data Pelanggan	Enkripsi data- Akses terbatas	Nomor HP pelanggan sudah dienkripsi

Domain	Subdomain	Fokus Audit
Keamanan Jaringan	Wi-Fi publik & internal- Segmentasi	Wi-Fi pelanggan dan staf masih satu jaringan
Logging dan Monitoring	Riwayat transaksi- Audit trail	Transaksi terekam otomatis dalam sistem POS
Manajemen Aset	Inventarisasi perangkat POS & Wi-Fi	Belum ada dokumentasi perangkat dan pengelolaannya

Domain	Subdomain	Fokus Audit
Backup dan Pemulihan	Backup otomatis data transaksi	Belum ada sistem backup rutin
Kesadaran Keamanan Staf	Pelatihan staf- Edukasi SOP keamanan	Belum ada pelatihan keamanan informasi untuk staf

Klausul

Penjelasan Klausul ISO/IEC 27001:2022 yang Digunakan

- Klausul A.5.9 – Penggunaan Akun Pengguna

  Klausul ini menekankan bahwa setiap pengguna sistem informasi harus memiliki identitas unik, yaitu akun pribadi yang tidak digunakan bersama. Hal ini untuk memastikan:

  - Jejak aktivitas pengguna dapat dilacak (audit trail)
  - Meningkatkan akuntabilitas
  - Mengurangi risiko penyalahgunaan sistem oleh pengguna yang tidak berwenang

  Temuan di Cafe Main-Main: Semua staf menggunakan satu akun login yang sama ke sistem POS. Ini melanggar prinsip akuntabilitas dan keamanan.

- Klausul A.5.13 – Pengelolaan Autentikasi (Password)

  Klausul ini membahas bagaimana autentikasi (termasuk password) harus diatur secara aman. Beberapa prinsip pentingnya:

  - Password harus cukup kompleks
  - Password harus diubah secara berkala
  - Tidak boleh disimpan secara terbuka atau mudah ditebak

  Temuan di Cafe Main-Main: Password kasir cukup kuat, tapi belum pernah diganti sejak sistem dipasang. Ini meningkatkan risiko akses tidak sah jika password diketahui pihak luar.

- Klausul A.5.20 – Perlindungan Informasi Pelanggan

  Klausul ini menekankan bahwa informasi pribadi pelanggan, seperti nama, nomor telepon, dan data transaksi, harus:

  - Disimpan dengan aman
  - Dibatasi aksesnya hanya kepada yang berwenang
  - Dilindungi dari penyalahgunaan atau kebocoran

  Temuan di Cafe Main-Main: Data pelanggan (nomor HP) pada loyalty program disimpan dalam bentuk terenkripsi. Ini merupakan praktik yang baik dan sesuai dengan klausul ini.

- Klausul A.5.30 – Segmentasi Jaringan

  Klausul ini mengatur bahwa jaringan harus dipisahkan sesuai fungsi dan penggunaannya untuk meminimalkan risiko keamanan. Contohnya:

  - Memisahkan jaringan internal (staf) dengan jaringan publik (pelanggan)
  - Mencegah pelanggan mengakses sistem kasir, database, atau printer internal

  Temuan di Cafe Main-Main: Wi-Fi pelanggan dan staf menggunakan jaringan yang sama. Ini berisiko karena perangkat pelanggan bisa menjadi pintu masuk ke sistem internal.

- Klausul A.5.23 – Logging dan Monitoring

  Klausul ini menyarankan adanya sistem logging (pencatatan) yang mencatat:

  - Aktivitas transaksi
  - Akses login pengguna
  - Perubahan sistem

  Logging ini membantu:

  - Melacak insiden keamanan
  - Menganalisis kejadian sistem
  - Menyediakan bukti audit

  Temuan di Cafe Main-Main: Transaksi dari sistem POS terekam dan bisa dilihat kembali, sehingga sesuai dengan kontrol ini. Namun belum ada sistem logging untuk aktivitas login pengguna karena semua pakai akun yang sama.

- Klausul A.5.9.2 – Inventarisasi Aset Informasi

  Aset informasi seperti perangkat POS, router, dan sistem backend harus didaftarkan dan dikelola. Tujuannya:

  - Mengetahui siapa yang bertanggung jawab atas setiap aset
  - Menghindari kehilangan atau penyalahgunaan
  - Menyusun rencana perawatan dan pengamanan

  Catatan di Cafe Main-Main: Tidak disebutkan secara eksplisit dalam temuan, tapi disarankan ditambahkan agar perangkat POS dan jaringan Wi-Fi dicatat sebagai aset yang dikelola.

- Klausul A.5.32 – Pengelolaan Backup

  Klausul ini menyarankan bahwa informasi penting dan sistem harus dibackup secara:

  - Terjadwal dan otomatis
  - Disimpan di lokasi aman
  - Diuji secara berkala untuk pemulihan

  Catatan di Cafe Main-Main: Tidak ditemukan sistem backup otomatis transaksi. Hal ini berisiko jika sistem POS rusak atau terhapus datanya.

- Klausul A.6.3 – Kesadaran Keamanan Informasi

  Karyawan/staf harus diberikan:

  - Pelatihan dasar tentang keamanan informasi
  - Pemahaman tentang SOP seperti tidak berbagi password, mengenali ancaman phishing, dan melapor insiden

  Temuan di Cafe Main-Main: Belum ada pelatihan atau edukasi bagi staf mengenai praktik keamanan informasi.