**Sistem Manajemen Risiko BBP - Panduan Instalasi dan Penggunaan**

**Persyaratan Sistem**

* MySQL/MariaDB (versi 5.2.1 atau lebih tinggi)
* PHP 8.1 atau lebih tinggi
* phpMyAdmin (opsional tapi direkomendasikan untuk manajemen database)

**Langkah-langkah Instalasi**

**1. Pengaturan Database**

1. Login ke server MySQL Anda
2. Buat database baru:

**Sql**

CREATE DATABASE bbp\_risk\_management;

1. Import file SQL dump:

* Menggunakan command line:

**Bash**

mysql -u username\_anda -p bbp\_risk\_management < bbp\_risk\_management.sql

Atau menggunakan phpMyAdmin:

* Buka phpMyAdmin
* Pilih database bbp\_risk\_management
* Klik tab "Import"
* Pilih file bbp\_risk\_management.sql
* Klik "Go" untuk mengimport

**2. Konfigurasi Awal**

Sistem dilengkapi dengan pengguna default untuk akses admin dan fakultas:

**Akun Admin**

* Email: admin@uin-suka.ac.id
* Password default: admin123
* Peran: admin

**Akun Fakultas**

Setiap fakultas memiliki akun sendiri dengan pola berikut:

Email: [kode\_fakultas]@uin-suka.ac.id

Contoh: faib@uin-suka.ac.id, fdk@uin-suka.ac.id, dll.

Password default: (nama fakultas)123

Peran: fakultas

**Struktur Sistem**

**Tabel Database**

1. **fakultas** - Menyimpan informasi fakultas

* Berisi 8 fakultas yang telah dikonfigurasi dengan kode masing-masing

2. **users** - Mengelola akun pengguna

* Menyimpan email, password (terenkripsi SHA256), peran, dan asosiasi fakultas

3.**risk\_registers** - Catatan utama penilaian risiko

* Mencatat kejadian risiko, penyebab, sumber, dan tingkat risiko inherent

4.**risk\_categories** - Mengkategorikan berbagai jenis risiko

5.**risk\_treatments** - Mendokumentasikan rencana mitigasi risiko

* Termasuk rencana mitigasi, PIC, dan jenis bukti

6.**mitigation\_timeline** - Melacak implementasi mitigasi

* Perencanaan dan realisasi per triwulan

**Panduan Penggunaan Dasar**

**1. Proses Manajemen Risiko**

**1.Identifikasi Risiko**

* Login ke sistem
* Navigasi ke bagian Risk Register
* Isi detail risiko termasuk:

1. Objektif bisnis
2. Proses bisnis
3. Kejadian risiko
4. Penyebab risiko
5. Sumber risiko (internal/eksternal)
6. Pemilik risiko

**2.Penilaian Risiko**

* Evaluasi kemungkinan (skala 1-5)
* Nilai dampak (skala 1-5)
* Sistem secara otomatis menghitung tingkat risiko

**3.Penanganan Risiko**

* Buat rencana mitigasi
* Tentukan PIC
* Tentukan jenis bukti
* Atur timeline implementasi per triwulan

**2. Pemantauan dan Review**

* Lacak kemajuan mitigasi melalui timeline
* Perbarui status realisasi setiap triwulan
* Tinjau efektivitas penanganan
* Sesuaikan rencana jika diperlukan

**3. Kontrol Akses**

**Peran Admin**

* Akses penuh ke sistem
* Dapat mengelola semua fakultas
* Dapat membuat/mengedit pengguna
* Akses ke semua laporan

**Peran Fakultas**

* Terbatas pada data fakultas sendiri
* Dapat membuat/mengedit risk register
* Dapat memperbarui progres mitigasi
* Akses ke laporan khusus fakultas

**Pertimbangan Keamanan**

1. Ganti password default segera setelah login pertama
2. Password disimpan menggunakan enkripsi SHA256
3. Manajemen sesi mencakup remember\_token untuk login yang aman
4. Kontrol akses berbasis peran menjaga pemisahan data

**Pemeliharaan**

1. Backup database secara berkala direkomendasikan
2. Monitor log sistem untuk aktivitas tidak biasa
3. Jaga PHP dan MySQL/MariaDB tetap diperbarui ke versi stabil terbaru
4. Tinjau akses pengguna secara berkala dan hapus akun yang tidak digunakan