

Pengurusan Operasi dan Keselamatan Pusat Data

Pengurusan Operasi Pusat Data



1

Menjamin operasi 24/7 tanpa gangguan

2

Mengurangkan risiko kegagalan sistem

3

Mengoptimumkan penggunaan sumber

4

Memastikan pematuhan piawaian & polisi

Objektif Reka Bentuk Pusat Data



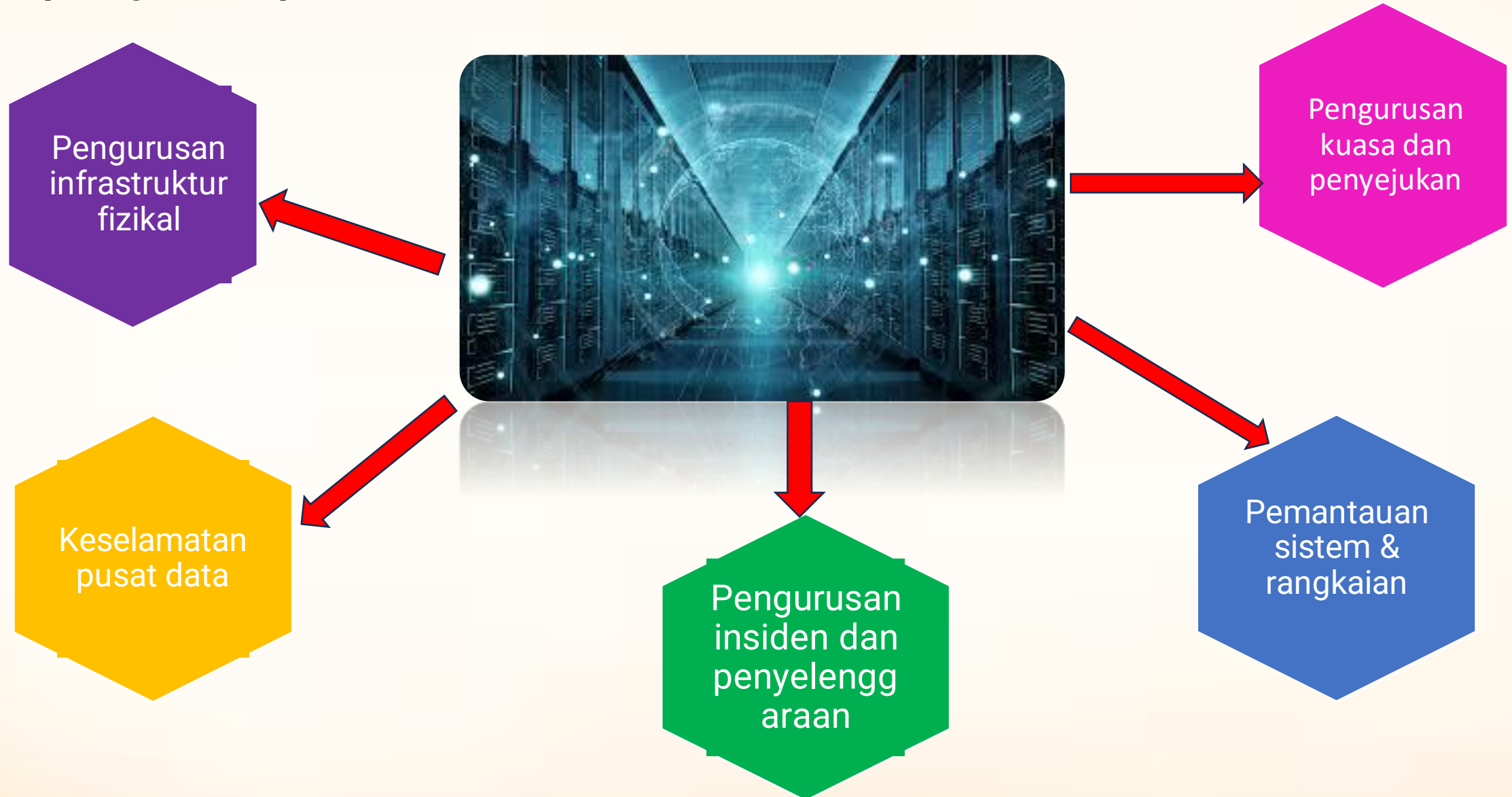
Pengurusan infrastruktur fizikal

Pengurusan kuasa dan penyejukan

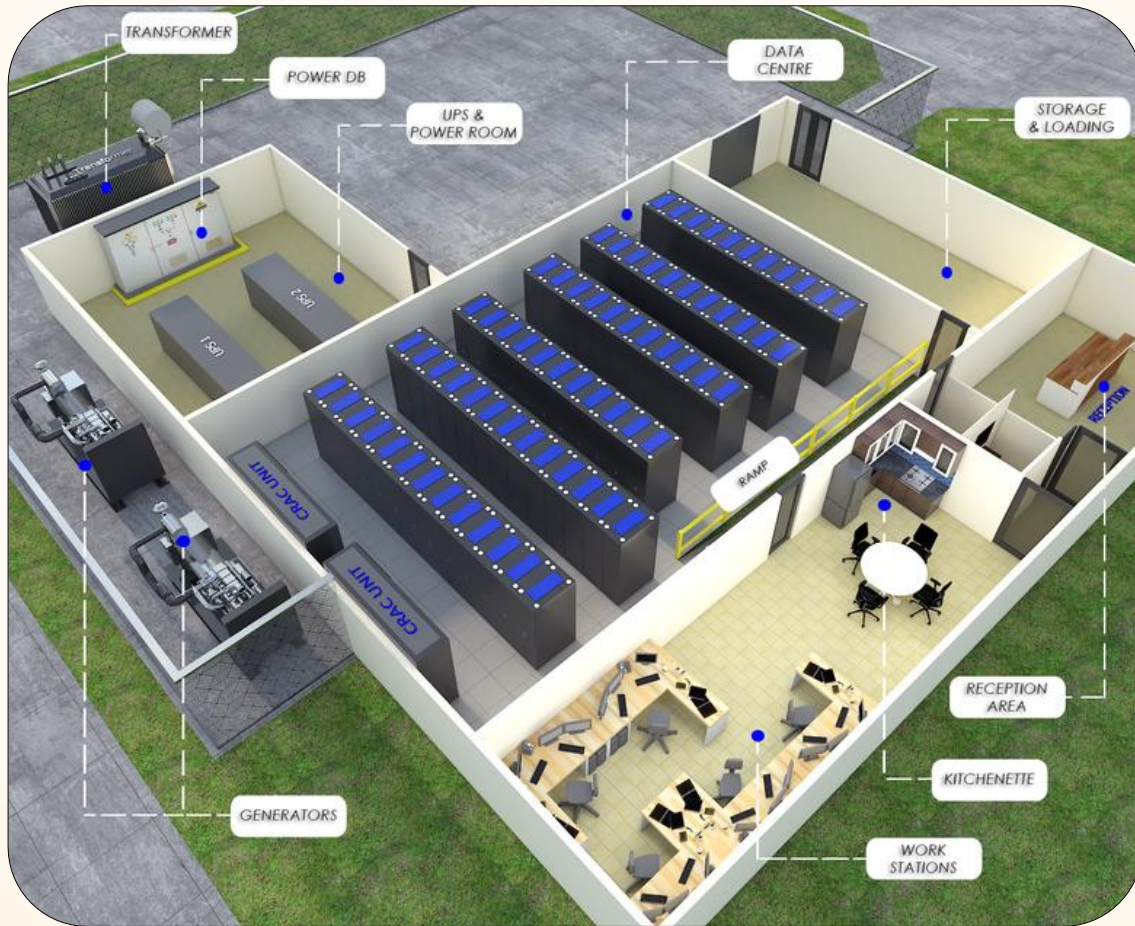
Pemantauan sistem & rangkaian

Pengurusan insiden dan penyelenggaraan

Skop Pengurusan Operasi Pusat Data



Pengurusan Infrastruktur Fizikal



**Rak Pelayan
(Servef Rack)**



**Label dan
Dokumentasi**



Susunan Kabel



**Storan dan
Rangkaian**

 **Tujuan: memudahkan penyelenggaraan & mengurangkan kesilapan**

Pengurusan Kuasa dan Penyejukan Pusat Data



1. Sumber kuasa utama dan sandaran

- UPS (Uninterruptible Power Supply)
- Generator



2. Sistem penyejukan:

- Air conditioning
- Kawalan suhu & kelembapan
- Elak overheat dan kerosakan peralatan

Pemantauan Operasi Pusat Data



**Pemantauan
pelayan,
rangkaian dan
storan**

**Penggunaan
sistem
pemantauan
otomatik**

**Amaran awal
(alert) jika berlaku
masalah**

**Log sistem untuk
analisis prestasi**

Pemantauan Operasi Pusat Data



Keselamatan Fizikal

- Akses terhad (kad, biometrik)
- CCTV dan pengawal keselamatan

Keselamatan Logikal

- Firewall Kawalan akses pengguna
- Polisi keselamatan ICT

Pengurusan Insiden Pusat Data



1. Proses menangani gangguan sistem
2. Tindakan segera (response)
3. Perekodan insiden
4. Analisis punca masalah (root cause analysis)

Penyelenggaraan & Sokongan Pusat Data



PREVENTIVE
MAINTENANCE

MAINTENANCE
PREVENTIVE

1. Penyelenggaraan berkala (preventive maintenance)
2. Kemaskini perisian & firmware
3. Ujian sistem sandaran (backup & recovery)
4. Dokumentasi perubahan (change management)

Pengurusan Risiko Pusat Data

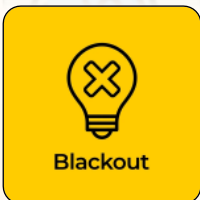


1. Mengelakkan gangguan perkhidmatan ICT
2. Mengurangkan kerosakan peralatan
3. Melindungi keselamatan data dan maklumat
4. Memastikan pematuhan polisi dan piawaian

Kategori Risiko Pusat Data



Risiko Fizikal



1. Kebakaran
2. Banjir
3. Suhu dan kelembapan tidak terkawal
4. Kegagalan bekalan elektrik

Kesan:

- Kerosakan peralatan
- Operasi pusat data terganggu

Risiko Keselamatan

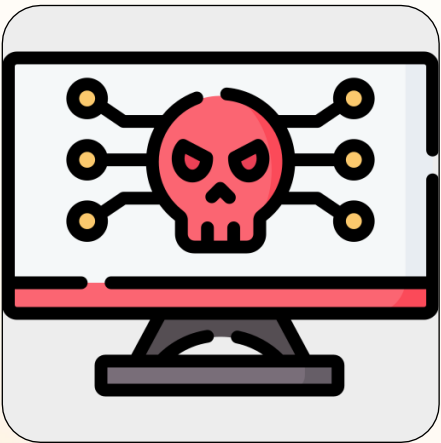


1. Keselamatan Fizikal

- Pencerobohan tanpa kebenaran
- Kecurian peralatan

2. Keselamatan Logikal

- Serangan siber
- Akses tidak sah
- Malware & virus



Risiko Operasi



1

**Kesilapan manusia
(human error)**

2

**Prosedur kerja tidak
dipatuhi**

3

Kurang Latihan kakitangan

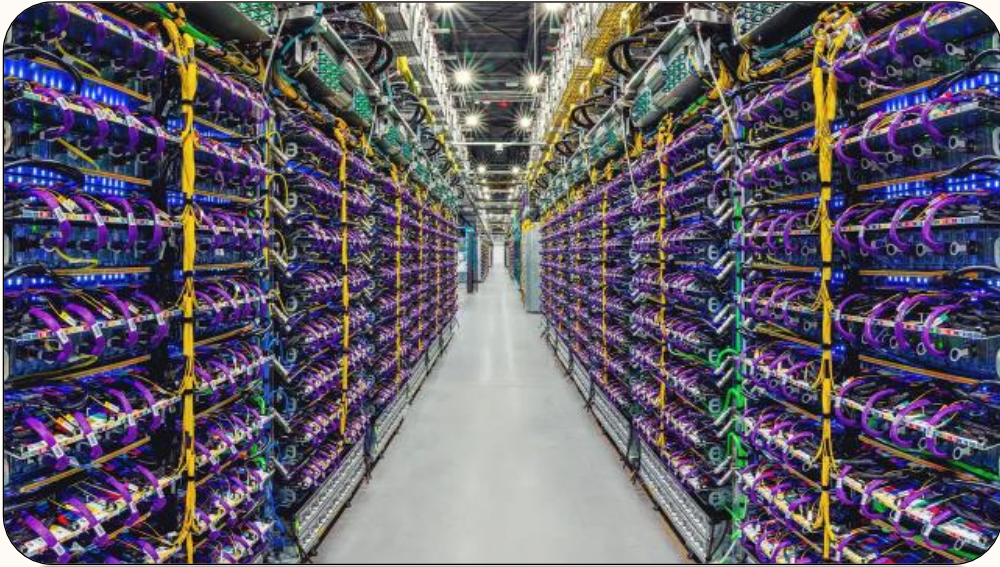
4

Dokumen tidak lengkap

Proses Pengurusan Risiko



Pengenalpastian Risiko



**Mengenal pasti semua ancaman kepada pusat data
Menggunakan:**

- 1. Pemeriksaan fizikal**
- 2. Laporan insiden lepas**
- 3. Audit sistem**
- 4. Pendapat pakar**

Analisis dan Penilaian Risiko

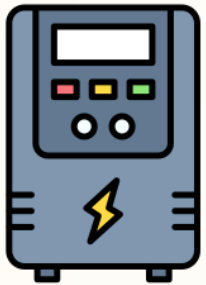


**Menilai:Kebarangkalian risiko berlaku
Tahap kesan terhadap operasi**

Risiko dikategorikan sebagai:

- 1. Rendah**
- 2. Sederhana**
- 3. Tinggi**

Kawalan Risiko (Risk Control)



Kaedah kawalan:

1. Mengelakkan risiko
2. Mengurangkan risiko
3. Memindahkan risiko (insurans)
4. Menerima risiko (jika kesan rendah)

Contoh:

1. Sistem pemadam kebakaran automatik
2. UPS dan generator sandaran
3. Sistem backup dan recovery
4. Polisi keselamatan ICT
5. Latihan kakitangan berkala

Pelan Pemulihan Bencana (Disaster Recovery)



**Prosedur pemulihan selepas bencana
Lokasi pusat data sandaran
Ujian pemulihan secara berkala
Mengurangkan masa henti sistem (downtime)**

Kesimpulan



**Pengurusan risiko adalah elemen penting pusat data
Risiko tidak dapat dielakkan sepenuhnya
Perancangan dan kawalan yang baik dapat mengurangkan kesan risiko
Operasi pusat data lebih selamat dan stabil**

Amalan Terbaik (Best Practice)

Pemantauan berterusan
Dokumentasi lengkap
Latihan kakitangan
Pelan pemulihan bencana (Disaster Recovery Plan)
Audit dan penilaian berkala



**THANK
YOU**