

Buku Pegangan Data Center

Teknik Disain, Perencanaan, Deployment, Environmentally Friendly
Secure Data Center

Onno W. Purbo
onno@indo.net.id
onno@itts.ac.id
Twitter onnowpurbo

Institut Teknologi Tangerang Selatan (ITTS)
Dinas KOMINFO Tangerang Selatan
OnnoCenter
2026

Lisensi: Karya ini dilisensikan di bawah **Creative Commons Attribution (CC BY) 4.0 International**. Anda bebas menggunakan, membagikan, dan mengadaptasi karya ini untuk tujuan apa pun, termasuk komersial, dengan tetap mencantumkan atribusi yang layak kepada penulis.

Disclaimer: Buku ini disusun untuk tujuan edukasi, dokumentasi, dan refleksi publik berdasarkan sumber-sumber yang dianggap kredibel pada saat penulisan. Penulis telah berupaya menjaga akurasi, namun sangat mungkin masih terdapat kekurangan atau kekeliruan; karena itu, buku ini tidak dimaksudkan sebagai satu-satunya rujukan yang final, dan penulis terbuka terhadap koreksi serta masukan yang membangun

Benang Merah Buku

Buku ini dibangun dengan satu pesan kuat: **data center profesional harus aman, efisien, terukur, dan siap diaudit sejak tahap desain**. Pertanyaan yang dibawa dalam setiap bab:

1. **Apa keputusan desain yang harus dibuat?**
2. **Apa rumus / bukti / dokumen yang harus disiapkan?**
3. **Apa risiko jika keputusan itu salah?**

Kata Pengantar

Puji syukur kehadiran Tuhan Yang Maha Esa, buku **Teknik Desain, Perencanaan, Deployment, Environmentally Friendly Secure Data Center** ini dapat disusun sebagai referensi praktis bagi para profesional yang ingin memahami, merancang, menguji, mengoperasikan, dan menyiapkan *data center* secara lebih matang.

Buku ini ditulis dengan satu keyakinan dasar: **data center bukan sekadar ruang berisi server**, melainkan infrastruktur kritikal yang menggabungkan listrik, pendinginan, jaringan, keamanan, operasi, keberlanjutan, dan tata kelola risiko. Kesalahan kecil dalam desain atau operasi dapat berdampak besar pada layanan, bisnis, keamanan data, bahkan reputasi organisasi.

Isi buku ini disusun untuk mendukung kebutuhan **sertifikasi profesional data center**. Pembahasan dimulai dari pemahaman kebutuhan bisnis, risiko, kapasitas, desain ruang, sistem kelistrikan, thermal design, efisiensi energi, jaringan, keamanan, deployment, commissioning, hingga operasi harian dan readiness audit. Pendekatannya dibuat seimbang: **cukup teoritis untuk memahami prinsip**, tetapi tetap **praktis untuk digunakan di lapangan**.

Pembaca akan menemukan banyak template, checklist, rumus, studi kasus, dan contoh dokumen yang dapat langsung diadaptasi. Tujuannya bukan hanya agar pembaca mengenal istilah seperti PUE, UPS, *spine-leaf*, ASHRAE, DCIM, atau *Zero Trust*, tetapi mampu menjawab pertanyaan yang lebih penting: **apa yang harus dihitung, apa yang harus diuji, apa yang harus dicatat, dan bukti apa yang harus disiapkan saat audit atau sertifikasi**.

Buku ini juga menekankan bahwa *data center* masa kini tidak cukup hanya andal. Ia harus **aman, hemat energi, sadar karbon, efisien air, mudah dioperasikan, terdokumentasi, dan siap berkembang**. Karena itu, pembahasan mengenai *environmentally friendly data center*, *waste heat reuse*, *carbon-aware operation*, monitoring, capacity review, dan operasi berkelanjutan menjadi bagian penting dari keseluruhan buku.

Semoga buku ini dapat menjadi pegangan bagi engineer, operator, perencana, auditor, konsultan, manajer infrastruktur, dan peserta sertifikasi yang ingin membangun cara berpikir profesional dalam dunia *data center*. Harapannya, pembaca tidak hanya mampu menghafal standar, tetapi mampu **mendesain dengan benar, menghitung dengan masuk akal, menguji dengan disiplin, mengoperasikan dengan rapi, dan mempertanggungjawabkan setiap keputusan teknis dengan bukti**.

Akhir kata, semoga buku ini bermanfaat bagi penguatan kompetensi profesional *data center* di Indonesia, serta mendorong lahirnya infrastruktur digital yang lebih andal, aman, efisien, dan berkelanjutan.

Jakarta, Mei 2026
Onno W. Purbo

Daftar Isi

Kata Pengantar.....	4
Daftar Isi.....	5
Bab 1. Data Center sebagai Infrastruktur Kritis.....	14
1.1 Definisi Data Center Modern.....	14
1.2 Perbedaan Server Room, Enterprise Data Center, Colocation, Edge Data Center, dan Hyperscale.....	15
1.3 Komponen Utama Data Center: IT Load, Power, Cooling, Network, Storage, Security, Monitoring.....	17
1.4 Prinsip Desain: Availability, Scalability, Security, Performance, Manageability.....	18
1.5 Mengapa Keputusan Desain Tidak Boleh Terpisah Antar Tim.....	19
1.6 Dampak AI, IoT, 5G, dan Beban Komputasi Padat GPU terhadap Desain Data Center	20
Materi Praktek 1: Checklist Identifikasi Tipe Data Center.....	21
Materi Praktek 2: Template “Data Center Design Brief” 1 Halaman.....	22
Data Center Design Brief.....	22
Materi Praktek 3: Contoh Klasifikasi Kebutuhan.....	24
Contoh 1 — Data Center Kecil.....	24
Contoh 2 — Data Center Menengah.....	24
Contoh 3 — Data Center Kritis.....	24
Contoh 4 — Edge Data Center.....	24
Ringkasan Bab 1.....	25
Checklist Akhir Bab 1.....	25
Bab 2. Kebutuhan Bisnis, Risiko, dan Target Sertifikasi.....	26
2.1 Menentukan Kebutuhan Bisnis dan Layanan.....	26
2.2 Service Level Requirement: Uptime, RTO, RPO, Latency, Kapasitas.....	27
2.3 Analisis Risiko: Listrik, Pendinginan, Kebakaran, Banjir, Gempa, Keamanan, SDM, Vendor.....	29
2.4 Pemetaan Standar: ISO/IEC 22237, Uptime Tier, TIA-942, ASHRAE.....	30
2.5 Memilih Target Desain: Basic, Redundant, Concurrently Maintainable, Fault Tolerant..	32
2.6 Kesalahan Umum: Mengejar Sertifikat tanpa Kesiapan Operasi.....	33
Materi Praktek 1: Template Business Requirement Document.....	34
Materi Praktek 2: Matriks Risiko — Risiko → Dampak → Kontrol → Bukti Audit....	35
Materi Praktek 3: Contoh Pemilihan Target Sertifikasi Berdasarkan Aplikasi Kritis	36
Kasus 1 — Sistem Arsip Internal.....	36
Kasus 2 — Sistem ERP / Operasional 24x7.....	36
Kasus 3 — Sistem Transaksi Kritis.....	36
Kasus 4 — Edge Data Center untuk IoT / 5G / Industri.....	36
Ringkasan Bab 2.....	37
Checklist Akhir Bab 2.....	37
Bab 3. Perhitungan Kapasitas: IT Load, Rack, Space, Power, Cooling.....	38
3.1 Menghitung IT Load.....	38

3.2 Menghitung Kebutuhan Rak.....	40
3.3 Menghitung Kebutuhan Ruang White Space.....	41
3.4 Menghitung Kebutuhan Daya Total.....	42
3.5 Menghitung Kebutuhan UPS.....	43
3.6 Menghitung Kebutuhan Generator.....	44
3.7 Menghitung Kapasitas Pendinginan.....	45
3.8 Menghitung Estimasi PUE dan Biaya Energi.....	46
3.9 Menghitung Pertumbuhan 3–5 Tahun.....	47
3.10 Menentukan Ruang Cadangan dan Stranded Capacity.....	48
Materi Praktek 1: Contoh Perhitungan Data Center 10 Rack.....	49
Materi Praktek 2: Contoh Perhitungan Data Center 50 Rack.....	50
Materi Praktek 3: Contoh Perhitungan Data Center 100 Rack.....	51
Materi Praktek 4: Tabel Perhitungan Rack Density.....	52
Materi Praktek 5: Template Kalkulasi Kapasitas 5 Tahun.....	53
Materi Praktek 6: Latihan — 30 Rack @ 6 kW/Rack.....	54
Ringkasan Bab 3.....	55
Checklist Akhir Bab 3.....	55
Bab 4. Desain Ruang, Rack, Kabel, Jalur, dan White Space.....	56
4.1 Prinsip Space Planning.....	56
4.2 White Space, Gray Space, Ruang MEP, Ruang Staging, dan Ruang NOC.....	57
4.3 Layout Rak: Baris, Lorong Panas, Lorong Dingin.....	58
4.4 Raised Floor vs Slab Floor.....	59
4.5 Jalur Kabel Data dan Kabel Power.....	60
4.6 Labeling, Dokumentasi, dan Standar Instalasi.....	61
4.7 Beban Lantai, Akses Barang, Pintu, Ramp, dan Jalur Evakuasi.....	62
4.8 Kesalahan Umum Desain Ruang.....	63
Materi Praktek 1: Contoh Layout 10 Rack.....	64
Asumsi.....	64
Rekomendasi Layout.....	64
Catatan Desain.....	64
Materi Praktek 2: Contoh Layout 50 Rack.....	65
Asumsi.....	65
Rekomendasi Layout.....	65
Catatan Desain.....	65
Materi Praktek 3: Checklist Desain Ruangan.....	66
Materi Praktek 4: Template Penomoran Rack, Patch Panel, PDU, dan Jalur Kabel.....	67
Format Penomoran Rack.....	67
Format Patch Panel.....	67
Format Port.....	67
Format PDU.....	68
Format Jalur Kabel.....	68
Materi Praktek 5: Contoh Bill of Quantity Awal.....	69
Ringkasan Bab 4.....	70
Checklist Akhir Bab 4.....	70

Bab 5. Sistem Kelistrikan: Utility, UPS, Generator, PDU, Grounding.....	71
5.1 Arsitektur Power Data Center.....	71
5.2 Utility Feed dan Panel Utama.....	72
5.3 UPS: Kapasitas, Runtime, Baterai, Bypass, Modularitas.....	73
5.4 Generator: Kapasitas, Bahan Bakar, ATS/AMF, Durasi Operasi.....	75
5.5 PDU, RPP, dan Rack PDU.....	76
5.6 Grounding dan Bonding.....	77
5.7 Redundansi N, N+1, 2N.....	78
5.8 Proteksi Petir dan Surge.....	79
5.9 Testing Kelistrikan.....	80
5.10 Dokumentasi Single Line Diagram.....	81
Materi Praktek 1: Cara Menghitung Kapasitas UPS.....	82
Langkah Perhitungan.....	82
Rumus Dasar.....	82
Contoh.....	82
Materi Praktek 2: Cara Menghitung Kebutuhan Baterai.....	83
Rumus Estimasi Energi.....	83
Contoh.....	83
Hal yang Wajib Diperiksa.....	83
Materi Praktek 3: Cara Menghitung Generator Berdasarkan IT Load dan Beban Pendukung.....	84
Langkah Perhitungan.....	84
Contoh Sesuai Soal.....	84
Durasi Bahan Bakar.....	85
Materi Praktek 4: Checklist Inspeksi Panel, UPS, PDU, dan Grounding.....	86
Ringkasan Bab 5.....	87
Checklist Akhir Bab 5.....	87
Bab 6. Thermal Design: Airflow, Containment, Liquid Cooling, dan ASHRAE.....	88
6.1 Prinsip Perpindahan Panas di Data Center.....	88
6.2 Inlet Temperature, Outlet Temperature, dan Delta T.....	89
6.3 Hot Aisle dan Cold Aisle.....	90
6.4 Containment: HAC dan CAC.....	91
6.5 CRAC, CRAH, Chiller, dan Cooling Tower.....	92
6.6 Free Cooling dan Economizer.....	93
6.7 Liquid Cooling: Rear-Door Heat Exchanger, Cold Plate, Immersion Cooling.....	94
6.8 Tantangan Rack Density Tinggi dan GPU.....	95
6.9 Kelembaban, Dew Point, Korosi, dan ESD.....	96
6.10 Pengukuran Thermal dan Sensor.....	97
Materi Praktek 1: Cara Membaca Thermal Map.....	98
Materi Praktek 2: Cara Menghitung Kebutuhan Cooling.....	99
Contoh 1 — IT Load 100 kW.....	99
Contoh 2 — IT Load 200 kW.....	99
Contoh 3 — IT Load 30 Rack @ 6 kW/Rack.....	100
Materi Praktek 3: Checklist Airflow.....	101

Materi Praktek 4: Studi Kasus — Rak Panas karena Airflow Salah, Bukan karena AC Kurang.....	102
Ringkasan Bab 6.....	103
Checklist Akhir Bab 6.....	104
Bab 7. Environmentally Friendly Data Center: PUE, Energi, Air, Karbon.....	105
7.1 Konsep Green Data Center.....	105
7.2 PUE, DCiE, WUE, CUE, ERE.....	106
7.3 Efisiensi IT: Konsolidasi Server, Virtualisasi, Right-Sizing.....	108
7.4 Efisiensi Cooling.....	109
7.5 Energi Terbarukan dan Renewable Matching.....	110
7.6 Pengelolaan Air.....	111
7.7 Waste Heat Reuse.....	112
7.8 Carbon-Aware Operation.....	113
7.9 Audit Energi Data Center.....	114
7.10 Membuat Roadmap Efisiensi Energi.....	115
Materi Praktek 1: Cara Menghitung PUE Bulanan.....	116
Materi Praktek 2: Cara Membaca Tagihan Listrik Data Center.....	117
Materi Praktek 3: Template Audit Energi Sederhana.....	118
Materi Praktek 4: Contoh Program Penurunan PUE dari 2,0 ke 1,6.....	119
Kondisi Awal.....	119
Tahap 1 — 0 sampai 3 Bulan: Perbaikan Dasar.....	119
Tahap 2 — 3 sampai 6 Bulan: Optimasi Cooling.....	119
Tahap 3 — 6 sampai 12 Bulan: Optimasi Sistem.....	120
Tahap 4 — 12 sampai 18 Bulan: Transformasi.....	120
Materi Praktek 5: Checklist Green Retrofit untuk Data Center Lama.....	121
Ringkasan Bab 7.....	122
Checklist Akhir Bab 7.....	122
Bab 8. Desain Jaringan Data Center: Spine-Leaf, Underlay, Overlay, DCI.....	123
8.1 Evolusi Arsitektur Jaringan Data Center.....	123
8.2 Three-Tier Architecture vs Spine-Leaf Architecture.....	124
8.3 Top-of-Rack dan End-of-Row.....	125
8.4 Underlay Network.....	126
8.5 Overlay Network: VXLAN, EVPN, Tenant Segmentation.....	127
8.6 Routing Internal Data Center.....	128
8.7 Data Center Interconnect dan DR Site.....	129
8.8 Telemetry dan Observability Jaringan.....	130
8.9 Prinsip Keamanan Jaringan Data Center.....	131
8.10 Dokumentasi dan Validasi Desain Jaringan.....	132
Materi Praktek 1: Contoh Desain Jaringan 2 Spine 4 Leaf.....	133
Topologi Dasar.....	133
Prinsip Desain.....	133
Contoh Alokasi Fungsi.....	133
Hal yang Harus Diuji.....	134
Materi Praktek 2: Contoh Tabel VLAN / VRF / Segmentasi.....	135

Catatan Desain.....	135
Materi Praktek 3: Checklist Desain DCI.....	136
Materi Praktek 4: Template Network Low-Level Design.....	137
1. Informasi Umum.....	137
2. Topologi Fisik.....	137
3. Topologi Logis.....	137
4. Segmentasi.....	137
5. Routing Plan.....	137
6. Security Plan.....	138
7. Telemetry dan Monitoring.....	138
8. Test Plan.....	138
9. Dokumen Bukti.....	138
Ringkasan Bab 8.....	139
Checklist Akhir Bab 8.....	139
Bab 9. Secure Data Center: Physical, Network, Cyber, Zero Trust, Audit.....	140
9.1 Keamanan Fisik: Perimeter, Akses, CCTV, Mantrap.....	140
9.2 Keamanan Ruang: Rack Lock, Visitor Log, Escort Policy.....	141
9.3 Keamanan Jaringan: Firewall, ACL, IDS/IPS, Segmentasi.....	142
9.4 Keamanan Manajemen: OOB, MFA, Bastion, Logging.....	143
9.5 Keamanan OT: BMS, DCIM, UPS, Cooling Controller.....	144
9.6 Zero Trust untuk Data Center.....	145
9.7 Patch Management dan Vulnerability Management.....	146
9.8 Backup, DR, dan Ransomware Readiness.....	147
9.9 Audit Trail dan Bukti Kepatuhan.....	148
9.10 Incident Response Data Center.....	149
Materi Praktek 1: Matriks Kontrol Keamanan Data Center.....	150
Materi Praktek 2: Checklist Audit Akses Fisik.....	151
Materi Praktek 3: Checklist Hardening Management Network.....	152
Materi Praktek 4: Template Laporan Insiden.....	153
Materi Praktek 5: Contoh Desain Segmentasi.....	155
Ringkasan Bab 9.....	156
Checklist Akhir Bab 9.....	156
Bab 10. Deployment, Testing, Commissioning, dan Handover.....	157
10.1 Tahapan Deployment.....	157
10.2 Factory Acceptance Test dan Site Acceptance Test.....	158
10.3 Testing Power: UPS, Generator, ATS, Load Bank.....	159
10.4 Testing Cooling: Airflow, Thermal Load, Failover Cooling.....	160
10.5 Testing Network: Redundansi, Throughput, Failover.....	161
10.6 Testing Security: Akses, Log, Alarm, Incident Drill.....	162
10.7 Integrated System Test atau IST.....	163
10.8 Dokumentasi As-Built.....	164
10.9 Handover ke Operasi.....	165
10.10 Go-Live Checklist.....	166
Materi Praktek 1: Template Commissioning Plan.....	167

Materi Praktek 2: Contoh Skenario Integrated System Test.....	168
Skenario: Utility Power Failure.....	168
Kriteria Lulus.....	168
Materi Praktek 3: Checklist FAT/SAT.....	169
Materi Praktek 4: Checklist Dokumen As-Built.....	170
Materi Praktek 5: Template Berita Acara Serah Terima.....	171
Ringkasan Bab 10.....	173
Checklist Akhir Bab 10.....	173
Bab 11. Operasi, DCIM, Monitoring, Maintenance, dan Capacity Review.....	174
11.1 Operasi Harian Data Center.....	174
11.2 SOP, MOP, EOP.....	175
11.3 Preventive dan Predictive Maintenance.....	176
11.4 DCIM dan Monitoring.....	177
11.5 Sensor: Suhu, Kelembaban, Air Flow, Power, Leak Detection.....	178
11.6 Capacity Management.....	179
11.7 Change Management.....	180
11.8 Incident Management.....	181
11.9 Laporan Bulanan Operasi.....	182
11.10 Review PUE, SLA, Risiko, dan Kapasitas.....	183
Materi Praktek 1: Template SOP Operasi Harian.....	184
SOP Operasi Harian Data Center.....	184
Materi Praktek 2: Template MOP Pekerjaan Kritis.....	185
MOP — Method of Procedure.....	185
Materi Praktek 3: Template EOP Ketika Listrik Mati, UPS Alarm, Cooling Gagal...187	187
EOP 1 — Listrik Utama Mati.....	187
EOP 2 — UPS Alarm.....	187
EOP 3 — Cooling Gagal.....	188
Materi Praktek 4: Dashboard Minimum Operasi.....	189
Materi Praktek 5: Checklist Capacity Review Triwulanan.....	190
Ringkasan Bab 11.....	191
Checklist Akhir Bab 11.....	191
Bab 12. Studi Kasus, Checklist Sertifikasi, dan Roadmap Profesional.....	192
12.1 Studi Kasus 1: Membangun Data Center Kecil 10 Rack.....	193
12.2 Studi Kasus 2: Retrofit Data Center Lama agar Lebih Efisien.....	194
12.3 Studi Kasus 3: Desain Edge Data Center.....	196
12.4 Checklist Kesiapan Sertifikasi.....	197
12.5 Peta Kompetensi Profesional Data Center.....	198
12.6 Roadmap Belajar 6 Bulan.....	199
12.7 Kesalahan Fatal yang Sering Menggagalkan Sertifikasi.....	200
Materi Praktek 1: Checklist Final Sebelum Audit.....	201
Materi Praktek 2: Template Gap Analysis.....	202
Materi Praktek 3: Template Roadmap Peningkatan dari Kondisi Existing ke Target Sertifikasi.....	203
Materi Praktek 4: Contoh Portofolio Professional Data Center.....	204

Ringkasan Bab 12.....	205
Checklist Akhir Bab 12.....	205
Lampiran A. Template Data Center Design Brief.....	206
A.1 Informasi Umum Proyek.....	206
A.2 Tujuan Bisnis.....	206
A.3 Aplikasi Kritikal.....	207
A.4 Target Availability.....	207
A.5 Target Keamanan.....	208
A.6 Target PUE dan Efisiensi Energi.....	209
A.7 Kapasitas Awal dan Kapasitas 5 Tahun.....	210
A.8 Lokasi.....	211
A.9 Risiko Utama.....	212
A.10 Standar Acuan.....	213
A.11 Keputusan Manajemen yang Dibutuhkan.....	214
A.12 Ringkasan Eksekutif Design Brief.....	215
A.13 Persetujuan.....	215
Lampiran B. Template Perhitungan Kapasitas.....	216
B.1 Template Utama Perhitungan Kapasitas Perangkat.....	216
B.2 Rumus Dasar.....	217
B.3 Contoh Pengisian.....	218
B.4 Template Ringkasan Kapasitas.....	219
B.5 Template Perhitungan Rack Target.....	220
B.6 Template Growth 3 Tahun dan 5 Tahun.....	221
B.7 Catatan Desain yang Wajib Diisi.....	221
B.8 Checklist Validasi Perhitungan Kapasitas.....	222
B.9 Ringkasan Akhir Perhitungan.....	223
Lampiran C. Rumus-Rumus Penting.....	224
C.1 IT Load.....	224
C.2 Facility Load.....	225
C.3 PUE — Power Usage Effectiveness.....	226
C.4 DCiE — Data Center Infrastructure Efficiency.....	227
C.5 Cooling BTU/h.....	228
C.6 Energy Cost.....	229
C.7 Rack Density.....	230
C.8 UPS Sizing.....	231
C.9 Generator Sizing.....	232
C.10 Growth Capacity.....	233
C.11 Ringkasan Rumus Cepat.....	234
C.12 Contoh Ringkas Satu Kasus Lengkap.....	235
C.13 Checklist Validasi Rumus.....	236
Lampiran D. Checklist Desain Data Center.....	237
D.1 Checklist Site.....	237
D.2 Checklist Space.....	238
D.3 Checklist Rack.....	239

D.4 Checklist Power.....	240
D.5 Checklist Cooling.....	241
D.6 Checklist Network.....	242
D.7 Checklist Security.....	243
D.8 Checklist Fire Protection.....	244
D.9 Checklist Monitoring.....	245
D.10 Checklist Documentation.....	246
D.11 Ringkasan Status Desain.....	247
D.12 Persetujuan Review Desain.....	247
Lampiran E. Checklist Deployment dan Commissioning.....	248
E.1 Checklist FAT — Factory Acceptance Test.....	248
E.2 Checklist SAT — Site Acceptance Test.....	249
E.3 Checklist Load Bank Test.....	250
E.4 Checklist Integrated System Test — IST.....	251
E.5 Checklist Failover Test.....	252
E.6 Checklist Security Test.....	253
E.7 Checklist Handover Document.....	254
E.8 Template Ringkasan Status Commissioning.....	256
E.9 Template Persetujuan Commissioning.....	256
E.10 Checklist Final Sebelum Go-Live.....	257
Lampiran F. Checklist Operasi Harian Data Center.....	258
F.1 Informasi Shift Operasi.....	258
F.2 Checklist Suhu.....	259
F.3 Checklist Kelembaban.....	260
F.4 Checklist Alarm.....	261
F.5 Checklist UPS.....	262
F.6 Checklist Generator.....	263
F.7 Checklist PDU / Rack PDU.....	264
F.8 Checklist CRAC / CRAH.....	265
F.9 Checklist Access Log.....	266
F.10 Checklist Incident Log.....	267
F.11 Checklist Capacity Log.....	268
F.12 Ringkasan Harian Operasi.....	269
F.13 Eskalasi.....	270
F.14 Persetujuan Shift.....	270
Glosarium.....	271
Daftar Referensi.....	279
Tentang Penulis.....	281

Bab 1. Data Center sebagai Infrastruktur Kritis

Golden Rule: Data center bukan ruang server; data center adalah sistem kritis yang menggabungkan listrik, pendinginan, jaringan, keamanan, operasi, dan tata kelola risiko.

Bab ini menjadi fondasi buku. Tujuannya adalah membentuk cara pandang profesional bahwa *data center* bukan sekadar tempat menaruh perangkat TI, tetapi **infrastruktur strategis** yang menopang layanan digital, transaksi bisnis, layanan publik, komunikasi, penyimpanan data, komputasi AI, dan keberlanjutan operasi organisasi.

Dalam outline buku, Bab 1 ditempatkan sebagai bab fondasi dengan porsi 8 halaman dan diarahkan untuk membangun pemahaman bahwa *data center* harus dilihat sebagai **sistem terpadu** yang aman, efisien, terukur, siap audit, dan siap disertifikasi .

1.1 Definisi Data Center Modern

Secara sederhana, *data center* adalah fasilitas khusus untuk menempatkan, mengoperasikan, melindungi, dan mengelola perangkat komputasi, penyimpanan, jaringan, keamanan, dan sistem pendukungnya. Namun, definisi profesional harus lebih luas. *Data center* modern adalah **ekosistem infrastruktur kritis** yang mencakup bangunan, daya listrik, pendinginan, jaringan, keamanan fisik, keamanan siber, monitoring, prosedur operasi, dokumentasi, dan tata kelola risiko.

ISO/IEC 22237-1 menjelaskan prinsip umum, terminologi, model referensi, serta aspek fasilitas dan infrastruktur yang diperlukan untuk mendukung *data center*. Standar ini juga memperkenalkan klasifikasi terkait **availability**, **physical security**, dan **energy efficiency enablement** sepanjang siklus hidup fasilitas. ([ISO](#))

Artinya, *data center* tidak boleh dipahami hanya dari sisi perangkat TI. Sebuah *server* yang baik tetap bisa gagal melayani pengguna jika listrik tidak stabil, pendinginan buruk, kabel tidak terdokumentasi, akses fisik longgar, jaringan tidak redundan, atau prosedur operasi tidak disiplin. Dalam konteks profesional, **kegagalan data center adalah kegagalan sistem**, bukan sekadar kegagalan satu perangkat.

Buku *Data Center Handbook* menekankan pendekatan *plan, design, build, and operations*. Pendekatan ini penting karena desain *data center* tidak berhenti pada gambar teknis, tetapi berlanjut ke pembangunan, pengujian, operasi, efisiensi energi, manajemen risiko, dan perbaikan berkelanjutan.

Inti pemahaman:

- **Data center adalah fasilitas kritis**, bukan ruang teknis biasa.
- **Perangkat TI hanya satu bagian** dari sistem yang lebih besar.
- **Desain, konstruksi, operasi, dan audit** harus dipikirkan sejak awal.
- **Ketersediaan layanan** ditentukan oleh rantai terlemah: listrik, pendinginan, jaringan, keamanan, SDM, atau prosedur.

1.2 Perbedaan Server Room, Enterprise Data Center, Colocation, Edge Data Center, dan Hyperscale

Banyak organisasi memulai dari *server room*. Ruang ini biasanya kecil, berada di dalam kantor, dan digunakan untuk menaruh beberapa *server*, perangkat jaringan, atau perangkat penyimpanan. Masalahnya, *server room* sering tumbuh tanpa desain jangka panjang. Kabel bertambah, beban listrik naik, pendinginan dipaksa bekerja lebih keras, dan dokumentasi tertinggal. Pada tahap ini, risiko mulai muncul: panas berlebih, gangguan listrik, akses tidak terkendali, dan kapasitas sulit diprediksi.

Enterprise data center lebih matang. Fasilitas ini dirancang untuk mendukung kebutuhan internal organisasi. Biasanya sudah memiliki perencanaan daya, pendinginan, jaringan, keamanan fisik, *backup*, monitoring, dan prosedur operasi. Fokus utamanya adalah **kontinuitas layanan internal**, kepatuhan, dan efisiensi biaya.

Colocation data center adalah fasilitas yang menyediakan ruang, listrik, pendinginan, konektivitas, dan keamanan bagi banyak pelanggan. Organisasi membawa atau menyewa perangkatnya, sementara pengelola fasilitas menyediakan infrastruktur dasar. Model ini cocok bila organisasi membutuhkan fasilitas profesional tetapi tidak ingin membangun semuanya sendiri.

Edge data center adalah fasilitas lebih kecil yang ditempatkan dekat dengan pengguna, sensor, perangkat industri, kota, kampus, pabrik, pelabuhan, perkebunan, atau lokasi operasional tertentu. Tujuannya adalah mengurangi *latency*, menghemat bandwidth, dan menjaga layanan tetap berjalan meskipun koneksi ke pusat terganggu. Kebutuhan *edge* semakin penting karena IoT, 5G, video analytics, dan AI lokal membutuhkan pemrosesan data dekat sumbernya.

Hyperscale data center adalah fasilitas skala sangat besar yang dirancang untuk beban komputasi masif. Fokusnya adalah skala, otomasi, efisiensi energi, desain modular, kepadatan tinggi, dan operasi industri. Model ini biasanya dipakai oleh penyedia layanan digital berskala sangat besar.

Tabel ringkas klasifikasi:

Jenis	Ciri Utama	Fokus Risiko	Cocok Untuk
<i>Server room</i>	Kecil, sering tumbuh organik	Panas, listrik, akses, dokumentasi	Kantor kecil, lab, tahap awal
<i>Enterprise data center</i>	Dimiliki organisasi	SLA, kepatuhan, kapasitas	Bank, kampus, industri, instansi
<i>Colocation</i>	Fasilitas bersama banyak pelanggan	Kontrak, konektivitas, kepatuhan	Organisasi yang butuh fasilitas siap pakai
<i>Edge data center</i>	Dekat pengguna / lokasi operasi	Lingkungan, koneksi, SDM lokal	IoT, 5G, pabrik, kota, cabang
<i>Hyperscale</i>	Sangat besar dan otomatis	Energi, cooling, skala, pasokan	Layanan digital berskala besar

Catatan kritis: tidak semua organisasi perlu membangun *hyperscale*. Keputusan yang benar adalah memilih tipe fasilitas sesuai **kebutuhan bisnis, risiko, kapasitas, lokasi, dan kemampuan operasi**.

1.3 Komponen Utama Data Center: IT Load, Power, Cooling, Network, Storage, Security, Monitoring

Komponen pertama adalah *IT load*, yaitu total beban daya dari perangkat TI yang benar-benar menjalankan layanan: *server*, *storage*, perangkat jaringan, perangkat keamanan, dan perangkat komputasi khusus seperti GPU. *IT load* menjadi dasar perhitungan listrik, pendinginan, kapasitas rak, ruang, dan biaya energi. Kesalahan menghitung *IT load* akan menjalar ke seluruh desain.

Komponen kedua adalah *power*. Sistem daya mencakup pasokan listrik utama, panel, UPS, baterai, generator, distribusi listrik, *rack PDU*, grounding, proteksi petir, dan sistem pemantauan daya. Dalam *data center*, listrik bukan sekadar “ada tegangan”. Listrik harus **stabil, redundan, aman, terukur, dan dapat dipelihara tanpa mematikan layanan**.

Komponen ketiga adalah *cooling*. Semua perangkat TI menghasilkan panas. Panas ini harus dipindahkan dari perangkat ke ruangan, dari ruangan ke sistem pendingin, lalu keluar ke lingkungan. *Data Center Handbook* menjelaskan bahwa perangkat TI menghasilkan panas dalam jumlah besar dan seluruh panas di dalam *data center* harus dikeluarkan ke lingkungan luar. Sistem pendinginan biasanya terbagi antara pendinginan di dalam ruang dan infrastruktur pendinginan di luar ruang.

Komponen keempat adalah *network*. Jaringan *data center* menghubungkan *server*, *storage*, sistem keamanan, sistem manajemen, pengguna, aplikasi, dan lokasi lain. Desain jaringan harus mempertimbangkan *latency*, bandwidth, segmentasi, jalur redundan, *east-west traffic*, *north-south traffic*, observability, dan keamanan.

Komponen kelima adalah *storage*. Data perlu disimpan, dicadangkan, direplikasi, dan dipulihkan. Dalam layanan kritis, desain *storage* harus mempertimbangkan kapasitas, performa, *availability*, *backup*, *replication*, enkripsi, dan *recovery*. Tanpa desain *storage* yang benar, organisasi bisa tetap “hidup” secara listrik tetapi “mati” secara data.

Komponen keenam adalah *security*. Keamanan *data center* mencakup keamanan fisik, keamanan jaringan, keamanan akses manajemen, keamanan data, keamanan sistem operasi, keamanan *backup*, dan keamanan sistem fasilitas seperti BMS, UPS, dan pendinginan. Keamanan tidak boleh hanya dipandang sebagai firewall. **Akses fisik ke rak yang salah bisa sama berbahayanya dengan celah siber.**

Komponen ketujuh adalah *monitoring*. Fasilitas profesional harus mengetahui kondisi suhu, kelembapan, daya, arus, kapasitas UPS, status generator, alarm kebocoran air, status pintu, log akses, utilisasi jaringan, kapasitas penyimpanan, dan insiden operasi. Tanpa monitoring, pengelola hanya bereaksi setelah gangguan terjadi.

Prinsip penting: *data center* adalah sistem yang hidup. Kapasitas berubah, beban naik, perangkat diganti, risiko bertambah, standar berkembang, dan ekspektasi pengguna meningkat.

1.4 Prinsip Desain: Availability, Scalability, Security, Performance, Manageability

Prinsip pertama adalah *availability*. Ini berarti layanan harus tersedia sesuai kebutuhan bisnis. Tidak semua sistem membutuhkan tingkat ketersediaan yang sama. Sistem transaksi keuangan, layanan publik kritikal, operasi rumah sakit, atau kendali industri membutuhkan standar lebih tinggi dibanding sistem arsip non-kritikal. Uptime Institute menjelaskan bahwa *Tier Classification System* digunakan untuk membedakan tingkat infrastruktur berdasarkan kebutuhan ketersediaan layanan, dengan tingkat yang berbeda sesuai kebutuhan operasi. ([Uptime Institute](#))

Prinsip kedua adalah *scalability*. *Data center* harus bisa tumbuh. Pertumbuhan tidak hanya berarti menambah *server*. Pertumbuhan berarti menambah rak, daya, pendinginan, kabel, port jaringan, kapasitas *storage*, ruang, lisensi, sensor, SDM, dan prosedur operasi. Desain yang tidak scalable akan mahal diperbaiki di kemudian hari.

Prinsip ketiga adalah *security*. Keamanan harus masuk sejak desain, bukan ditempel di akhir. Ruang, rak, akses, jaringan, akun manajemen, *backup*, log, dan dokumentasi harus memiliki kontrol. ISO/IEC 22237 juga menempatkan **physical security** sebagai bagian dari klasifikasi fasilitas *data center*, bukan tambahan opsional. ([VDE Verlag](#))

Prinsip keempat adalah *performance*. Kinerja *data center* ditentukan oleh kombinasi komputasi, memori, penyimpanan, jaringan, pendinginan, dan arsitektur aplikasi. Kinerja buruk tidak selalu disebabkan CPU kurang cepat. Bisa jadi masalahnya ada pada jalur jaringan, *bottleneck storage*, desain rak yang panas, atau *oversubscription* pada koneksi.

Prinsip kelima adalah *manageability*. Sistem yang tidak bisa dikelola akan menjadi risiko. Semua komponen harus bisa dipantau, didokumentasikan, diberi label, diuji, diperbarui, dan diaudit. *Data center* profesional membutuhkan SOP, MOP, EOP, log perubahan, daftar aset, peta kabel, peta daya, peta jaringan, dan laporan kapasitas.

Ringkasnya:

- *Availability* menjawab: **seberapa lama layanan boleh mati?**
- *Scalability* menjawab: **bagaimana fasilitas tumbuh tanpa bongkar total?**
- *Security* menjawab: **siapa boleh mengakses apa, dari mana, dan dengan bukti apa?**
- *Performance* menjawab: **apakah sistem mampu melayani beban nyata?**
- *Manageability* menjawab: **apakah semua bisa dikelola, diuji, dan diaudit?**

1.5 Mengapa Keputusan Desain Tidak Boleh Terpisah Antar Tim

Kesalahan paling umum dalam proyek *data center* adalah memisahkan keputusan desain antar tim. Tim TI memilih *server* sendiri. Tim jaringan membuat desain sendiri. Tim fasilitas menghitung listrik dan pendinginan sendiri. Tim keamanan masuk belakangan. Tim operasi baru dilibatkan saat fasilitas hampir selesai. Akibatnya, desain tampak benar di kertas, tetapi sulit dioperasikan.

Referensi *Data Center Virtualization Fundamentals* menegaskan bahwa solusi *data center* sangat saling tergantung. Jumlah *server* per kabinet bergantung pada desain distribusi daya. Desain jaringan harus mengetahui jumlah *server* per rak dan jumlah antarmukanya. Posisi perangkat jaringan mempengaruhi desain kabel. Kabel bisa ditempatkan di bawah *raised floor*. *Raised floor* dapat mempengaruhi sistem pendinginan. Karena semua terhubung, keputusan terisolasi dari satu tim dapat merugikan fasilitas secara keseluruhan.

Contoh sederhana: tim TI ingin memasang 20 *server* GPU dalam satu rak. Dari sisi komputasi, ini terlihat efisien. Namun dari sisi fasilitas, rak tersebut mungkin membutuhkan daya puluhan kW dan pendinginan khusus. Jika tim listrik belum siap, MCB bisa sering trip. Jika tim cooling belum siap, suhu *inlet* naik. Jika tim jaringan belum siap, kabel menumpuk. Jika tim keamanan belum siap, akses manajemen terbuka. Jika tim operasi belum siap, insiden menjadi sulit dilacak.

Dalam *data center*, **keputusan kecil bisa menjadi risiko besar**. Memilih jenis rak mempengaruhi aliran udara. Memilih jalur kabel mempengaruhi akses pemeliharaan. Memilih lokasi PDU mempengaruhi manajemen daya. Memilih layout ruangan mempengaruhi evakuasi, pemadam kebakaran, sensor, CCTV, dan ekspansi.

Karena itu, proyek *data center* harus memakai pendekatan lintas disiplin:

- Tim bisnis menetapkan kebutuhan layanan.
- Tim aplikasi menjelaskan karakter beban.
- Tim TI menghitung *IT load*.
- Tim jaringan merancang konektivitas dan segmentasi.
- Tim fasilitas menghitung listrik dan cooling.
- Tim keamanan menetapkan kontrol.
- Tim operasi memastikan SOP dan monitoring.
- Tim audit memastikan bukti dan dokumentasi tersedia.

Prinsip profesional: tidak ada desain *data center* yang benar jika hanya benar menurut satu tim.

1.6 Dampak AI, IoT, 5G, dan Beban Komputasi Padat GPU terhadap Desain Data Center

Perkembangan AI, IoT, 5G, video analytics, otomasi industri, dan layanan digital real-time mengubah cara *data center* dirancang. Beban komputasi semakin padat, data semakin besar, dan kebutuhan respons semakin cepat. Ini mendorong peningkatan densitas rak, kebutuhan jaringan berlatensi rendah, pendinginan lebih presisi, dan kebutuhan energi lebih besar.

Beban AI dan GPU berbeda dari beban *server* tradisional. GPU padat daya, padat panas, dan sering membutuhkan bandwidth tinggi antar-node. Rak yang dahulu cukup 3–6 kW dapat naik menjadi jauh lebih tinggi pada beban AI. Dampaknya langsung terasa pada sistem listrik, pendinginan, kabel, lantai, sensor, dan prosedur operasi.

ASHRAE TC 9.9 menjadi rujukan penting untuk panduan termal *data center* dan peralatan TI. ASHRAE menekankan bahwa kondisi operasi, temperatur, dan reliabilitas perangkat saling terkait; peningkatan temperatur dapat berdampak pada keandalan perangkat, termasuk peralatan daya yang berada pada ruang atau aliran udara yang sama dengan perangkat TI. ([ASHRAE](#))

IoT dan 5G juga mendorong pertumbuhan *edge data center*. Data tidak selalu efisien dikirim ke pusat. Dalam banyak kasus, data perlu diproses dekat lokasi: kamera, sensor, kendaraan, pabrik, pelabuhan, perkebunan, atau kota. Ini menciptakan kebutuhan fasilitas kecil tetapi tetap aman, terkelola, dan tahan gangguan.

Dampak strategisnya jelas: *data center* masa depan harus **modular, efisien, aman, dekat dengan beban kerja, dan siap menghadapi densitas tinggi**. Organisasi yang hanya menambah perangkat tanpa mengubah desain listrik, pendinginan, jaringan, dan operasi akan menghadapi risiko besar: panas berlebih, biaya energi naik, gangguan layanan, dan kegagalan audit.

Materi Praktek 1: Checklist Identifikasi Tipe Data Center

Gunakan checklist ini sebelum membuat desain awal.

Pertanyaan	Pilihan / Isian	Catatan
Apa tujuan utama fasilitas?	Operasional internal / layanan publik / komersial / AI / edge	Tentukan prioritas layanan
Berapa jumlah rak awal?	... rack	Jangan lupa growth 3–5 tahun
Berapa estimasi <i>IT load</i> awal?	... kW	Dasar power dan cooling
Berapa target <i>availability</i> ?	Rendah / sedang / tinggi / kritikal	Sesuaikan risiko bisnis
Apakah ada kebutuhan 24×7?	Ya / Tidak	Pengaruh ke operasi dan SDM
Apakah ada data sensitif?	Ya / Tidak	Pengaruh ke security dan audit
Apakah lokasi rawan banjir/gempa/panas?	Ya / Tidak	Pengaruh ke site dan desain
Apakah ada kebutuhan <i>low latency</i> ?	Ya / Tidak	Pertimbangkan edge
Apakah beban GPU/AI dominan?	Ya / Tidak	Pengaruh ke densitas dan cooling
Apakah akan disertifikasi?	Ya / Tidak	Tentukan standar sejak awal

Interpretasi cepat:

- Jika jumlah rak kecil, risiko rendah, dan tidak 24×7 → kemungkinan *server room* atau *small enterprise data center*.
- Jika layanan kritikal, butuh SLA, dan ada audit → *enterprise data center*.
- Jika ingin fasilitas profesional tanpa membangun sendiri → *colocation*.
- Jika butuh dekat lokasi operasi dan *latency* rendah → *edge data center*.
- Jika beban sangat besar, otomatis, dan skala industri → *hyperscale*.

Materi Praktek 2: Template “Data Center Design Brief” 1

Halaman

Template ini menjadi dokumen awal sebelum desain teknis detail.

Data Center Design Brief

1. Nama Proyek:

...

2. Tujuan Bisnis:

Contoh: mendukung layanan digital internal 24×7, sistem transaksi, layanan publik, AI lokal, atau *disaster recovery*.

3. Jenis Data Center:

Server room / enterprise data center / colocation / edge data center / hyperscale.

4. Aplikasi / Layanan Kritisal:

- ...
- ...
- ...

5. Target Availability:

Contoh: jam operasional kantor / 24×7 / kritisal / membutuhkan redundansi.

6. Kapasitas Awal:

- Jumlah rak: ...
- Estimasi *IT load*: ... kW
- Estimasi perangkat: ...
- Estimasi storage: ... TB/PB

7. Proyeksi 3–5 Tahun:

- Jumlah rak: ...
- *IT load*: ... kW
- Pertumbuhan data: ... % per tahun

8. Kebutuhan Power:

- Sumber listrik utama: ...
- UPS: Ya / Tidak
- Generator: Ya / Tidak
- Redundansi: N / N+1 / 2N

9. Kebutuhan Cooling:

- Target suhu ruang / *inlet*: ...
- Metode pendinginan: *air cooling* / *containment* / *liquid cooling* / lainnya
- Risiko panas tinggi: Ya / Tidak

10. Kebutuhan Network:

- Jumlah koneksi uplink: ...
- Segmentasi: Ya / Tidak
- DCI / DR site: Ya / Tidak

11. Kebutuhan Security:

- Kontrol akses fisik: ...
- CCTV: ...
- Segmentasi jaringan: ...
- Logging dan audit trail: ...

12. Standar / Sertifikasi Acuan:

ISO/IEC 22237 / Uptime Tier / TIA-942 / ASHRAE / internal audit.

13. Risiko Utama:

- Listrik
- Cooling
- Banjir
- Kebakaran
- Akses fisik
- SDM
- Vendor
- Kapasitas

14. Keputusan yang Harus Dibuat Manajemen:

- Target sertifikasi
- Anggaran awal
- Kapasitas 5 tahun
- Lokasi
- Tingkat redundansi
- Model operasi

Materi Praktek 3: Contoh Klasifikasi Kebutuhan

Contoh 1 — Data Center Kecil

Sebuah kantor memiliki 3 rak, beban awal 8 kW, jam layanan utama 08.00–18.00, dan hanya sebagian sistem yang harus aktif 24×7. Fasilitas ini tidak boleh diperlakukan seperti ruang biasa. Minimal harus ada UPS, pendinginan stabil, akses terbatas, monitoring suhu, labeling kabel, dan *backup*.

Keputusan desain: sederhana, tetapi tetap disiplin.

Risiko utama: panas, kabel tidak rapi, UPS tidak cukup, akses fisik terlalu bebas.

Contoh 2 — Data Center Menengah

Sebuah organisasi memiliki 20–40 rak, aplikasi internal penting, layanan pengguna 24×7, dan kebutuhan audit. Fasilitas ini membutuhkan perhitungan *IT load*, UPS, generator, *containment*, segmentasi jaringan, DCIM sederhana, SOP operasi, dan dokumentasi perubahan.

Keputusan desain: mulai memakai redundansi dan prosedur formal.

Risiko utama: kapasitas tumbuh tanpa kontrol, pendinginan tidak merata, dokumentasi tertinggal.

Contoh 3 — Data Center Kritis

Sebuah lembaga menjalankan layanan transaksi, data sensitif, layanan publik, atau operasi nasional. Gangguan beberapa menit saja dapat berdampak besar. Fasilitas ini memerlukan desain redundan, pengujian berkala, kontrol akses ketat, *disaster recovery*, audit trail, dan sertifikasi.

Keputusan desain: berbasis risiko bisnis dan target *availability*.

Risiko utama: salah memilih tingkat redundansi, tidak siap audit, SDM operasi kurang matang.

Contoh 4 — Edge Data Center

Sebuah fasilitas kecil ditempatkan dekat lokasi operasi, misalnya pelabuhan, pabrik, kampus, perkebunan, kota, atau area 5G. Tujuannya memproses data lokal agar respons cepat dan koneksi ke pusat tidak selalu menjadi ketergantungan utama.

Keputusan desain: ringkas, tahan lingkungan, mudah dipantau jarak jauh.

Risiko utama: lokasi ekstrim, listrik tidak stabil, SDM lokal terbatas, keamanan fisik lemah.

Ringkasan Bab 1

Bab ini menegaskan bahwa **data center adalah infrastruktur kritikal**, bukan sekadar ruang berisi perangkat. Setiap desain harus dimulai dari kebutuhan bisnis, risiko, beban TI, target *availability*, keamanan, efisiensi energi, dan kemampuan operasi.

Pelajaran paling penting adalah bahwa *data center* merupakan **sistem saling terkait**. Jumlah perangkat memengaruhi listrik. Listrik memengaruhi pendinginan. Pendinginan memengaruhi layout. Layout memengaruhi kabel. Kabel memengaruhi operasi. Operasi memengaruhi audit. Audit memengaruhi kepercayaan.

Untuk profesional dan peserta sertifikasi, pemahaman ini sangat penting: **yang dinilai bukan hanya kemampuan menyebut istilah, tetapi kemampuan melihat hubungan antar-komponen, menghitung konsekuensi desain, dan membuktikan kesiapan operasi.**

Checklist Akhir Bab 1

Sebelum masuk Bab 2, pembaca harus mampu menjawab:

- Apakah fasilitas yang dirancang termasuk *server room*, *enterprise data center*, *colocation*, *edge*, atau *hyperscale*?
- Apa layanan paling kritikal yang harus dilindungi?
- Berapa estimasi awal *IT load*?
- Apa target *availability*?
- Apa resiko terbesar: listrik, pendinginan, jaringan, keamanan, lokasi, atau SDM?
- Apakah desain sudah mempertimbangkan pertumbuhan 3–5 tahun?
- Apakah tim TI, fasilitas, jaringan, keamanan, dan operasi sudah duduk bersama?
- Apakah sudah ada *Data Center Design Brief* 1 halaman?
- Apakah desain diarahkan untuk siap audit dan sertifikasi?

Penutup bab: *Data center* professional dimulai dari cara berpikir profesional: **lihat sistem secara utuh, hitung dampaknya, dokumentasikan keputusannya, dan siapkan bukti operasinya sejak awal.**

Bab 2. Kebutuhan Bisnis, Risiko, dan Target Sertifikasi

Golden Rule: Sertifikasi data center tidak dimulai dari gambar teknis, tetapi dari risiko bisnis, target layanan, dan batas toleransi *downtime*.

Bab ini menjelaskan bahwa desain *data center* profesional harus dimulai dari **kebutuhan bisnis**, bukan dari pilihan perangkat, merek, atau gambar ruang. Dalam outline buku, Bab 2 diarahkan untuk membahas kebutuhan bisnis, *service level requirement*, risiko, standar sertifikasi, pilihan target desain, serta kesalahan umum dalam mengejar sertifikasi tanpa kesiapan operasi .

2.1 Menentukan Kebutuhan Bisnis dan Layanan

Langkah pertama dalam perencanaan *data center* adalah menjawab pertanyaan sederhana tetapi kritikal: **layanan apa yang harus dilindungi, untuk siapa, dan seberapa penting layanan itu bagi organisasi?**

Banyak proyek *data center* gagal karena langsung masuk ke desain teknis: jumlah rak, kapasitas UPS, tipe pendingin, kabel, atau jaringan. Padahal, keputusan teknis harus diturunkan dari kebutuhan bisnis. *Data Center Handbook* menegaskan bahwa proyek *data center* dimulai dari pemahaman aplikasi TI dan platform pendukungnya, lalu dilanjutkan dengan koordinasi kebutuhan fasilitas, arsitektur jaringan, layout ruang komputer, dan migrasi aplikasi bisnis ke platform baru .

Untuk sertifikasi profesional, kebutuhan bisnis harus diterjemahkan menjadi parameter teknis. Misalnya, sistem transaksi 24×7 membutuhkan tingkat *availability* yang berbeda dari sistem arsip internal. Sistem layanan publik membutuhkan kontrol risiko berbeda dari sistem laboratorium. Sistem AI dengan GPU padat daya membutuhkan perhitungan listrik dan pendinginan yang berbeda dari beban kantor biasa.

Pertanyaan utama yang harus dijawab:

- Apa layanan paling kritikal?
- Siapa pengguna layanan?
- Berapa jam layanan harus aktif?
- Apa dampak jika layanan berhenti?
- Berapa lama organisasi masih bisa menerima gangguan?
- Data apa yang tidak boleh hilang?
- Apakah layanan harus tetap berjalan saat maintenance?
- Apakah ada kewajiban regulasi, audit, atau kontrak?
- Apakah kebutuhan kapasitas akan naik dalam 3–5 tahun?

Prinsip penting: desain *data center* yang baik harus bisa menjelaskan **hubungan antara risiko bisnis dan keputusan teknis**.

2.2 Service Level Requirement: Uptime, RTO, RPO, Latency, Kapasitas

Service Level Requirement adalah terjemahan kebutuhan bisnis ke dalam ukuran layanan yang bisa dihitung, diuji, dan diaudit. Tanpa ukuran ini, desain hanya menjadi perkiraan.

Ukuran pertama adalah *uptime*. *Uptime* menjawab seberapa lama layanan harus tersedia dalam periode tertentu. Namun, *uptime* tidak boleh dipakai sendirian. Dua sistem bisa sama-sama menargetkan *uptime* tinggi, tetapi memiliki toleransi kehilangan data dan waktu pemulihan yang berbeda.

Ukuran kedua adalah RTO, atau *Recovery Time Objective*. RTO adalah **batas waktu maksimum layanan boleh berhenti setelah insiden besar**. Jika RTO sebuah layanan adalah 2 jam, maka desain listrik, pendinginan, jaringan, server, storage, backup, dan prosedur pemulihan harus mendukung pemulihan dalam batas tersebut.

Ukuran ketiga adalah RPO, atau *Recovery Point Objective*. RPO adalah **batas maksimum kehilangan data yang masih dapat diterima**. Jika RPO adalah 15 menit, maka strategi *backup* harian tidak cukup. Dibutuhkan replikasi, snapshot lebih sering, atau arsitektur pemulihan yang lebih serius. Referensi *Data Center Virtualization Fundamentals* menjelaskan bahwa RPO dan RTO harus dikarakterisasi dengan baik agar organisasi tidak bereaksi secara *best effort* saat bencana, atau sebaliknya mengeluarkan biaya berlebihan untuk risiko yang tidak membutuhkan teknologi mahal .

Ukuran keempat adalah *latency*. Untuk aplikasi transaksi, video, IoT, AI inferensi, kendali industri, atau layanan real-time, *latency* bisa menjadi faktor utama. Jika *latency* terlalu tinggi, layanan tetap “hidup” tetapi kualitasnya buruk.

Ukuran kelima adalah kapasitas. Kapasitas mencakup jumlah pengguna, jumlah transaksi, kapasitas data, jumlah rak, *IT load*, bandwidth, dan pertumbuhan 3–5 tahun. Kapasitas tidak boleh hanya dihitung untuk hari pertama operasi.

Contoh ringkas:

Layanan	Uptime	RTO	RPO	Latency	Implikasi Desain
Website profil organisasi	Sedang	24 jam	24 jam	Tidak kritikal	Backup rutin cukup
Sistem transaksi	Tinggi	1 jam	5–15 menit	Rendah	Redundansi, replikasi, monitoring ketat
Sistem layanan publik 24×7	Sangat tinggi	<30 menit	Mendekati nol	Rendah	DR, failover, operasi 24×7
AI lokal / GPU cluster	Tinggi	4 jam	Tergantung dataset	Internal rendah	Daya dan cooling padat
Edge IoT	Sedang–tinggi	1–4 jam	Lokal	Sangat rendah	Lokasi dekat sumber data

Catatan kritis: semakin kecil RTO dan RPO, biasanya semakin tinggi biaya desain, kompleksitas operasi, dan kebutuhan SDM.

2.3 Analisis Risiko: Listrik, Pendinginan, Kebakaran, Banjir, Gempa, Keamanan, SDM, Vendor

Analisis risiko adalah inti perencanaan *data center*. Sertifikasi tidak hanya memeriksa apakah fasilitas terlihat bagus, tetapi apakah risiko sudah dikenali, dikendalikan, diuji, dan dibuktikan.

Risiko listrik mencakup pemadaman, tegangan tidak stabil, kegagalan UPS, baterai lemah, generator gagal start, distribusi daya tidak seimbang, grounding buruk, dan kesalahan saat maintenance. Risiko listrik sangat berbahaya karena dapat mematikan seluruh layanan dalam hitungan detik.

Risiko pendinginan mencakup suhu naik, aliran udara buruk, kapasitas AC tidak cukup, *hot spot*, kegagalan chiller, kebocoran air, dan kesalahan layout rak. *Data Center Handbook* menekankan bahwa desain mekanikal *data center* menjadi menantang karena kebutuhan reliabilitas tinggi, konsekuensi kegagalan yang mahal, serta peningkatan kepadatan panas dari perangkat TI modern .

Risiko kebakaran harus dilihat dari sisi deteksi dini, sistem pemadaman, jalur evakuasi, material, ruang baterai, panel listrik, dan prosedur respons. Risiko banjir dan kebocoran air mencakup lokasi, drainase, pipa, atap, *water leak detection*, dan posisi perangkat kritis.

Risiko gempa atau getaran penting untuk lokasi tertentu. Rak, jalur kabel, pipa, panel, UPS, baterai, dan perangkat berat harus dipasang dengan aman. Risiko fisik tidak boleh dianggap urusan sipil saja, karena dampaknya langsung ke ketersediaan layanan.

Risiko keamanan mencakup akses fisik, pencurian perangkat, sabotase, kesalahan akses vendor, penyalahgunaan akun, segmentasi jaringan yang buruk, dan lemahnya *logging*. Ruang keamanan, sistem akses, dan CCTV juga termasuk sistem kritis. *Data Center Handbook* menyatakan sistem keamanan seperti akses kontrol dan CCTV penting untuk operasi *data center* dan sebaiknya mendapat pasokan dari sumber UPS .

Risiko SDM sering diabaikan. Banyak fasilitas memiliki perangkat bagus tetapi gagal karena tidak ada SOP, MOP, EOP, jadwal maintenance, pelatihan, dokumentasi, dan disiplin perubahan. Risiko vendor juga penting: SLA tidak jelas, suku cadang tidak tersedia, teknisi lambat, kontrak tidak mencakup insiden kritis, atau ketergantungan terlalu tinggi pada satu pihak.

Prinsip risiko: setiap risiko harus memiliki **pemilik risiko, kontrol, bukti audit, dan rencana respons**.

2.4 Pemetaan Standar: ISO/IEC 22237, Uptime Tier, TIA-942, ASHRAE

Standar membantu organisasi menghindari desain berbasis selera. Namun, standar harus dipilih sesuai tujuan. Tidak semua standar menjawab hal yang sama.

ISO/IEC 22237-1:2021 menjelaskan prinsip umum, terminologi, parameter, model referensi, serta aspek fasilitas dan infrastruktur untuk *data centre*. Standar ini juga mengatur klasifikasi fasilitas berdasarkan *availability*, *physical security*, dan *energy efficiency enablement* sepanjang siklus hidup *data center*. ([ISO](#))

Uptime Institute *Tier Standard* banyak dipakai untuk menilai desain, konstruksi, dan operasi fasilitas. Uptime Institute menyatakan *Tier Standard* telah digunakan untuk desain, konstruksi, dan operasi ribuan situs di lebih dari 122 negara, serta telah menerbitkan lebih dari 4.000 penghargaan sertifikasi. ([Uptime Institute](#))

TIA-942 menyediakan kerangka sertifikasi untuk menilai kesesuaian *data center* terhadap standar ANSI/TIA-942. Program TIA-942 mencakup listing fasilitas tersertifikasi, perusahaan audit berlisensi, serta pelatihan untuk auditor dan konsultan. ([TIA Online](#)) TIA-942 juga mengenal sertifikasi desain, fasilitas, dan kesiapan, dengan masa berlaku yang berbeda; sertifikasi fasilitas berlaku 3 tahun dengan audit pengawasan tahunan sebelum sertifikasi ulang. ([TIA Online](#))

ASHRAE TC 9.9 menjadi rujukan penting untuk desain dan operasi fasilitas teknologi, terutama cooling, energi, kelembaban, dan efisiensi penggunaan energi pada *data center*. ASHRAE menyatakan TC 9.9 dibentuk untuk membahas fasilitas *mission critical*, ruang teknologi, perangkat elektronik, desain, operasi, pemeliharaan, dan penggunaan energi efisien. ([ASHRAE](#))

Pemetaan praktis:

Standar / Kerangka	Fokus Utama	Dipakai Untuk
ISO/IEC 22237	Prinsip fasilitas, klasifikasi availability, keamanan fisik, efisiensi energi	Kerangka desain dan operasi menyeluruh
Uptime Tier	Ketersediaan infrastruktur, desain, konstruksi, operasi	Target availability dan validasi pihak ketiga
TIA-942	Telekomunikasi, arsitektur, listrik, mekanikal, keamanan, rating fasilitas	Sertifikasi desain dan fasilitas
ASHRAE TC 9.9	Thermal, humidity, cooling, energi	Desain lingkungan operasi perangkat TI

Catatan tajam: standar bukan pengganti berpikir. Standar membantu menyusun bukti, tetapi keputusan desain tetap harus berbasis risiko bisnis.

2.5 Memilih Target Desain: Basic, Redundant, Concurrently Maintainable, Fault Tolerant

Target desain harus dipilih berdasarkan dampak bisnis, bukan gengsi. Fasilitas kecil tidak harus langsung mengejar tingkat tertinggi. Sebaliknya, layanan kritikal tidak boleh dipaksa berjalan di fasilitas yang hanya cocok untuk kebutuhan dasar.

Target *basic* cocok untuk layanan non-kritikal, lab, pengembangan, atau sistem yang masih bisa menerima *downtime*. Desainnya sederhana, tetapi tetap harus aman, terdokumentasi, dan memiliki perlindungan minimum.

Target *redundant* menambahkan komponen cadangan pada bagian kritikal, misalnya UPS modular N+1, cooling cadangan, jalur jaringan ganda, atau power feed ganda ke perangkat. Tujuannya bukan membuat sistem kebal gagal, tetapi mengurangi risiko gangguan karena satu komponen rusak.

Target *concurrently maintainable* berarti sistem dapat dipelihara tanpa mematikan layanan utama. Ini penting untuk fasilitas profesional karena maintenance pasti terjadi. Sistem listrik, pendinginan, jaringan, dan keamanan harus bisa dirawat dengan prosedur terencana.

Target *fault tolerant* berarti sistem dirancang tetap berjalan meskipun terjadi kegagalan tertentu. Ini adalah level yang lebih mahal dan kompleks. Tidak hanya perlu perangkat redundan, tetapi juga desain tanpa *single point of failure*, prosedur operasi matang, pengujian rutin, dan SDM kompeten.

Panduan pemilihan cepat:

Dampak Gangguan	Target Desain	Contoh Layanan
Rendah	Basic	Lab, arsip non-kritikal
Sedang	Redundant	Sistem internal penting
Tinggi	Concurrently maintainable	Layanan 24×7, sistem transaksi
Sangat tinggi	Fault tolerant	Layanan publik kritikal, finansial, operasi nasional

Prinsip profesional: semakin tinggi target desain, semakin besar kebutuhan dokumentasi, pengujian, disiplin operasi, dan biaya siklus hidup.

2.6 Kesalahan Umum: Mengejar Sertifikat tanpa Kesiapan Operasi

Kesalahan pertama adalah menganggap sertifikasi sebagai proyek dokumen. Padahal sertifikasi *data center* menilai kesesuaian desain, fasilitas, prosedur, bukti, dan operasi. Gambar teknis yang baik tidak cukup jika operasi harian tidak disiplin.

Kesalahan kedua adalah memilih target terlalu tinggi tanpa menghitung biaya operasi. Target desain tinggi memerlukan listrik, pendinginan, sparepart, kontrak maintenance, pengujian berkala, SDM siaga, dan dokumentasi ketat. Tanpa itu, fasilitas terlihat “kelas tinggi” tetapi rapuh.

Kesalahan ketiga adalah tidak melibatkan tim operasi sejak awal. Tim operasi yang tidak ikut desain akan kesulitan menjalankan fasilitas. Mereka tidak memahami asumsi desain, jalur bypass, skenario failover, batas kapasitas, dan prosedur pemulihan.

Kesalahan keempat adalah tidak memiliki bukti audit. Dalam sertifikasi, yang dicari bukan hanya klaim, tetapi bukti: gambar *as-built*, hasil tes, log maintenance, laporan kapasitas, catatan insiden, daftar aset, SOP, MOP, EOP, kontrak SLA, dan hasil simulasi.

Kesalahan kelima adalah mengejar standar tanpa memahami konteks. Standar harus dipetakan ke risiko bisnis. Tidak semua layanan memerlukan target tertinggi, tetapi semua layanan kritis memerlukan desain yang dapat dipertanggungjawabkan.

Kalimat kunci: sertifikasi yang sehat adalah hasil dari desain yang benar dan operasi yang disiplin, bukan kosmetik proyek.

Materi Praktek 1: Template *Business Requirement Document*

Gunakan template ini sebelum desain teknis detail.

Business Requirement Document — Data Center

Bagian	Isi yang Harus Diisi
Nama proyek	...
Pemilik bisnis	...
Pemilik teknis	...
Tujuan utama	...
Layanan kritikal	...
Pengguna utama	Internal / publik / pelanggan / mitra
Jam operasi	8×5 / 12×6 / 24×7
Dampak jika layanan mati	Finansial / reputasi / hukum / operasional / keselamatan
Target uptime	...
RTO	... menit / jam
RPO	... menit / jam
Target latency	... ms
Kapasitas awal	... rack / ... kW / ... TB
Proyeksi 3–5 tahun	...
Data sensitif	Ya / Tidak
Kebutuhan audit	Ya / Tidak
Standar acuan	ISO/IEC 22237 / Uptime / TIA-942 / ASHRAE / internal
Risiko utama	...
Target desain	Basic / Redundant / Concurrently maintainable / Fault tolerant
Bukti yang harus tersedia	Gambar, log, hasil tes, SOP, kontrak, laporan

Cara memakai: dokumen ini harus disetujui oleh manajemen, TI, fasilitas, keamanan, dan operasi sebelum desain teknis dimulai.

Materi Praktek 2: Matriks Risiko — Risiko → Dampak → Kontrol → Bukti Audit

Risiko	Dampak	Kontrol	Bukti Audit
Listrik utama padam	Layanan mati	UPS, generator, ATS/AMF, uji berkala	Hasil load test, log generator, diagram listrik
UPS gagal	Gangguan layanan kritikal	Redundansi, bypass, maintenance	Log UPS, kontrak servis, laporan inspeksi
Cooling gagal	Suhu naik, perangkat rusak	CRAC/CRAH cadangan, sensor suhu, alarm	Grafik suhu, log alarm, laporan maintenance
Hot spot rak	Performa turun, perangkat mati	Blanking panel, containment, thermal mapping	Foto rak, thermal map, checklist airflow
Kebakaran	Kerusakan fasilitas	Deteksi dini, sistem pemadaman, SOP evakuasi	Sertifikat inspeksi, hasil simulasi
Banjir / kebocoran air	Perangkat rusak	Sensor kebocoran, raised protection, drainase	Log sensor, inspeksi lokasi
Gempa / getaran	Rak roboh, kabel rusak	Anchoring, bracing, layout aman	Foto instalasi, laporan inspeksi
Akses fisik tidak sah	Pencurian, sabotase	Access control, CCTV, visitor log	Log akses, rekaman CCTV, daftar tamu
Kesalahan operator	Gangguan saat perubahan	SOP, MOP, EOP, approval perubahan	Change log, dokumen MOP, laporan insiden
Vendor lambat	Downtime panjang	SLA, spare part, escalation path	Kontrak SLA, tiket insiden, laporan response time
Kapasitas habis	Layanan tidak bisa tumbuh	Capacity planning, review berkala	Laporan kapasitas, proyeksi 3–5 tahun
Tidak siap audit	Sertifikasi gagal	Dokumentasi dan evidence management	Daftar bukti, hasil audit internal

Prinsip: risiko yang tidak memiliki bukti kontrol berarti **belum siap diaudit**.

Materi Praktek 3: Contoh Pemilihan Target Sertifikasi Berdasarkan Aplikasi Kritikal

Kasus 1 — Sistem Arsip Internal

Sistem arsip hanya dipakai jam kerja. Jika berhenti satu hari, dampak bisnis masih dapat diterima. RPO 24 jam dan RTO 24 jam masih masuk akal.

Target desain: *Basic* atau *Redundant* sederhana.

Fokus: backup, UPS dasar, kontrol akses, dokumentasi aset.

Risiko terbesar: kehilangan data karena backup tidak diuji.

Kasus 2 — Sistem ERP / Operasional 24×7

Sistem dipakai lintas unit kerja. Gangguan beberapa jam menghambat operasi organisasi. RTO 2–4 jam dan RPO 15–60 menit lebih realistis.

Target desain: *Redundant* menuju *concurrently maintainable*.

Fokus: UPS, generator, cooling cadangan, monitoring, backup, prosedur perubahan.

Risiko terbesar: maintenance mematikan layanan karena jalur redundansi tidak diuji.

Kasus 3 — Sistem Transaksi Kritikal

Sistem melayani transaksi, pelanggan, atau layanan publik. Gangguan beberapa menit berdampak finansial, reputasi, dan kepatuhan.

Target desain: *Concurrently maintainable* atau *fault tolerant*.

Fokus: DR, failover, replikasi data, jaringan redundan, operasi 24×7, audit trail.

Risiko terbesar: desain bagus, tetapi prosedur failover tidak pernah diuji.

Kasus 4 — Edge Data Center untuk IoT / 5G / Industri

Fasilitas berada dekat lokasi operasi. Kebutuhan *latency* rendah, tetapi lingkungan mungkin tidak ideal.

Target desain: *Redundant* yang ringkas dan tahan lokasi.

Fokus: power stabil, cooling sederhana, monitoring jarak jauh, keamanan fisik.

Risiko terbesar: lokasi lemah, SDM terbatas, akses vendor lambat.

Ringkasan Bab 2

Bab ini menegaskan bahwa **sertifikasi data center harus dimulai dari kebutuhan bisnis dan risiko**, bukan dari gambar desain. Standar seperti ISO/IEC 22237, Uptime Tier, TIA-942, dan ASHRAE adalah rujukan penting, tetapi pemilihannya harus sesuai konteks layanan dan dampak bisnis.

Professional *data center* harus mampu menerjemahkan kebutuhan bisnis menjadi parameter teknis: *uptime*, RTO, RPO, *latency*, kapasitas, risiko, kontrol, dan bukti audit. Tanpa ini, desain mudah menjadi mahal tetapi tidak tepat sasaran.

Inti bab: semakin kritis layanan, semakin kuat kebutuhan redundansi, pengujian, dokumentasi, operasi, dan bukti audit.

Checklist Akhir Bab 2

Sebelum masuk Bab 3, pembaca harus mampu menjawab:

- Apa layanan paling kritis yang akan dilindungi?
- Berapa target *uptime*?
- Berapa RTO dan RPO setiap aplikasi utama?
- Apa dampak finansial, hukum, reputasi, dan operasional jika layanan mati?
- Risiko terbesar ada pada listrik, cooling, keamanan, lokasi, SDM, atau vendor?
- Standar apa yang paling relevan: ISO/IEC 22237, Uptime Tier, TIA-942, ASHRAE, atau kombinasi?
- Apakah target desain realistis terhadap anggaran dan kemampuan operasi?
- Apakah sudah ada *Business Requirement Document*?
- Apakah setiap risiko sudah punya kontrol dan bukti audit?
- Apakah tim operasi siap menjalankan desain yang dipilih?

Penutup bab: *Data center* professional tidak dibangun dari ambisi sertifikasi, tetapi dari kejelasan kebutuhan bisnis, keberanian membaca risiko, dan kedisiplinan membuktikan kesiapan operasi.

Bab 3. Perhitungan Kapasitas: IT Load, Rack, Space, Power, Cooling

Golden Rule: Desain yang baik selalu dimulai dari angka beban, bukan dari merek perangkat.

Bab ini adalah jantung teknis awal dalam perencanaan *data center*. Setelah Bab 1 membangun cara pandang bahwa *data center* adalah infrastruktur kritikal, dan Bab 2 menjelaskan kebutuhan bisnis serta risiko, maka Bab 3 mengubah kebutuhan tersebut menjadi **angka desain**: berapa *IT load*, berapa rak, berapa ruang, berapa daya, berapa UPS, berapa generator, berapa kapasitas pendinginan, berapa biaya energi, dan berapa ruang pertumbuhan.

Dalam outline buku, Bab 3 memang diarahkan sebagai bab perhitungan kapasitas: *IT load*, rak, *white space*, daya total, UPS, generator, cooling, PUE, biaya energi, pertumbuhan 3–5 tahun, dan *stranded capacity*. Prinsip pentingnya: **sertifikasi data center tidak mungkin kuat jika angka dasarnya lemah.**

3.1 Menghitung IT Load

IT load adalah total beban listrik dari perangkat TI yang benar-benar menjalankan layanan. Yang termasuk di dalamnya adalah *server*, *storage*, perangkat jaringan, perangkat keamanan, perangkat manajemen, dan perangkat komputasi khusus seperti GPU.

Perhitungan *IT load* harus menjadi dasar desain. Jangan mulai dari luas ruangan. Jangan mulai dari kapasitas AC. Jangan mulai dari jumlah rak. Mulailah dari pertanyaan: **perangkat apa saja yang akan hidup, berapa watt per perangkat, dan berapa pertumbuhannya?**

Rumus dasar:

Total *IT Load* = jumlah perangkat × konsumsi daya rata-rata per perangkat

Namun untuk desain profesional, konsumsi daya tidak cukup memakai angka maksimum di brosur. Perlu dibedakan:

- **Nameplate power**: angka maksimum di label perangkat.
- **Typical power**: konsumsi rata-rata pada beban normal.
- **Peak power**: konsumsi saat beban tinggi.
- **Design power**: angka yang dipakai untuk desain, biasanya memakai margin.

Contoh sederhana:

Perangkat	Jumlah	Daya Rata-rata	Total
Server aplikasi	20	500 W	10.000 W
Storage	4	800 W	3.200 W
Network switch	4	400 W	1.600 W
Perangkat keamanan	2	300 W	600 W
Total IT Load			15.400 W / 15,4 kW

Tambahkan margin desain, misalnya 20%:

$$\text{IT Load Desain} = 15,4 \text{ kW} \times 1,2 = 18,48 \text{ kW}$$

Catatan tajam: *IT load* yang terlalu rendah membuat fasilitas cepat penuh. *IT load* yang terlalu tinggi membuat investasi mahal, banyak kapasitas menganggur, dan PUE bisa terlihat buruk saat beban masih rendah.

3.2 Menghitung Kebutuhan Rak

Rak bukan sekadar lemari perangkat. Rak adalah titik pertemuan antara **daya, pendinginan, kabel, beban lantai, akses operasi, dan kapasitas ekspansi**.

Secara umum, rak standar sering memiliki 42U, tetapi tidak semua U boleh dianggap terpakai penuh. Harus ada ruang untuk patch panel, manajemen kabel, perangkat jaringan, airflow, blanking panel, dan kemudahan kerja teknisi.

Rumus sederhana:

$$\text{Jumlah Rack} = \text{total U perangkat} / \text{kapasitas U efektif per rack}$$

Contoh:

- Total kebutuhan perangkat = 280U
- Kapasitas fisik rak = 42U
- Kapasitas efektif = 32U per rak
- Jumlah rak = $280 / 32 = 8,75$
- Maka dibulatkan menjadi **9 rak**

Tetapi untuk desain profesional, jumlah rak juga harus dicek dengan **rack density**:

$$\text{Rack Density} = \text{Total IT Load} / \text{Jumlah Rack}$$

Contoh:

- Total IT Load = 90 kW
- Jumlah rak = 15
- Rack Density = $90 / 15 = 6 \text{ kW/rack}$

Jika densitas rak naik, dampaknya langsung terasa pada listrik, pendinginan, kabel, dan layout lorong panas/dingin. Buku *Data Centers of the Future* menekankan bahwa seluruh listrik yang digunakan oleh perangkat, jaringan, cooling, dan bahkan pencahayaan pada akhirnya berubah menjadi panas; karena itu membuang panas adalah isu utama dalam desain data center .

Prinsip desain rak:

- Jangan menghitung rak hanya dari jumlah U.
- Hitung juga **kW per rack**.
- Pisahkan rak biasa dan rak densitas tinggi.
- Siapkan ruang untuk patching, sensor, dan manajemen kabel.
- Jangan isi rak sampai penuh jika cooling belum siap.

3.3 Menghitung Kebutuhan Ruang White Space

White space adalah area utama tempat rak TI ditempatkan. Tetapi ruang data center tidak hanya berisi rak. Dibutuhkan lorong, area kerja, jalur kabel, jalur evakuasi, ruang staging, area panel, dan ruang untuk ekspansi.

Pendekatan cepat:

Kebutuhan White Space = jumlah rak × luas efektif per rak

Untuk perhitungan awal, satu rak sering membutuhkan sekitar 2–3 m² ruang efektif jika memperhitungkan lorong depan, lorong belakang, akses kerja, dan ruang manajemen kabel. Angka ini harus disesuaikan dengan standar desain, layout, regulasi keselamatan, dan tipe fasilitas.

Contoh:

- Jumlah rak = 20
- Ruang efektif per rak = 2,5 m²
- White space awal = $20 \times 2,5 = 50 \text{ m}^2$
- Tambahkan ruang ekspansi 30% = 15 m²
- Total rencana white space = **65 m²**

Catatan critical: ruang terlalu kecil akan membuat operasi mahal. Teknisi sulit bekerja, kabel sulit dirapikan, cooling tidak merata, dan ekspansi menjadi bongkar ulang. Ruang terlalu besar juga tidak ideal karena biaya konstruksi, keamanan, cooling, dan monitoring naik.

Untuk sertifikasi, *white space* harus dapat dijelaskan dengan logika:

- Berapa rak awal?
- Berapa rak 3 tahun?
- Berapa rak 5 tahun?
- Berapa kW per rak?
- Apakah lorong cukup?
- Apakah jalur evakuasi aman?
- Apakah cooling mengikuti layout?
- Apakah ekspansi tidak merusak operasi berjalan?

3.4 Menghitung Kebutuhan Daya Total

Daya total fasilitas tidak sama dengan *IT load*. *IT load* hanya beban perangkat TI. Fasilitas juga membutuhkan daya untuk UPS losses, PDU losses, cooling, fan, pump, lighting, security, monitoring, dan sistem pendukung lain.

Rumus awal:

$$\text{Total Facility Power} = \text{IT Load} \times \text{PUE}$$

PUE, atau *Power Usage Effectiveness*, adalah rasio antara total energi fasilitas dengan energi perangkat TI. The Green Grid menjelaskan PUE sebagai metrik yang membantu mengukur efisiensi energi infrastruktur data center; rumus dasarnya adalah total energi fasilitas dibagi energi perangkat TI (datacenters.lbl.gov).

Contoh:

- IT Load = 200 kW
- Target PUE = 1,6
- Total Facility Power = $200 \times 1,6 = 320 \text{ kW}$

Tambahkan margin desain, misalnya 20%:

$$\text{Daya desain} = 320 \text{ kW} \times 1,2 = 384 \text{ kW}$$

Angka ini penting untuk memperkirakan kapasitas trafo, panel utama, UPS, generator, sistem distribusi, dan biaya energi. Namun perlu hati-hati: PUE bukan angka tetap. PUE berubah berdasarkan beban IT, iklim, desain cooling, desain listrik, dan tingkat utilisasi. *Data Center Handbook* menjelaskan bahwa PUE bisa terlihat sangat buruk saat beban IT masih rendah, karena fasilitas tetap memiliki konsumsi energi dasar meskipun perangkat TI belum penuh terpasang.

Prinsip praktis:

- Jangan gunakan PUE sebagai angka kosmetik.
- Gunakan PUE untuk estimasi biaya dan efisiensi.
- Ukur PUE saat operasi sudah berjalan.
- Pahami bahwa PUE saat fasilitas baru kosong akan berbeda dari PUE saat penuh.

3.5 Menghitung Kebutuhan UPS

UPS melindungi beban kritis dari gangguan listrik. UPS bukan sekadar baterai besar. UPS adalah bagian dari arsitektur ketersediaan layanan.

Langkah dasar menghitung UPS:

1. Tentukan *critical IT load*.
2. Tambahkan margin pertumbuhan.
3. Tentukan redundansi: N, N+1, atau 2N.
4. Tentukan *runtime* baterai.
5. Perhitungkan faktor daya dan efisiensi.
6. Pastikan jalur distribusi dan bypass aman.

Rumus awal:

$$\text{UPS Capacity Design} = \text{Critical IT Load} \times \text{Margin}$$

Contoh:

- Critical IT Load = 100 kW
- Margin pertumbuhan = 25%
- UPS minimal = $100 \times 1,25 = 125 \text{ kW}$

Jika memakai N+1 modular, misalnya modul UPS 50 kW:

- Kebutuhan efektif = 125 kW
- Kombinasi modul = 3 modul aktif = 150 kW
- Tambah 1 modul cadangan = 200 kW terpasang
- Arsitektur = **N+1**

Untuk sertifikasi, yang penting bukan hanya kapasitas UPS, tetapi bukti bahwa UPS bisa mendukung operasi:

- Diagram *single line*
- Data kapasitas UPS
- Hasil uji baterai
- Hasil uji bypass
- Jadwal maintenance
- Log alarm
- Prosedur saat UPS bermasalah

Kesalahan umum: UPS dihitung dari kondisi hari pertama, bukan kondisi 5 tahun. Akibatnya, saat rak bertambah, UPS menjadi bottleneck.

3.6 Menghitung Kebutuhan Generator

Generator diperlukan jika layanan harus tetap berjalan saat listrik utama mati lebih lama dari kapasitas baterai UPS. Generator harus mampu menanggung beban kritis, sebagian beban cooling, sistem keamanan, monitoring, dan sistem pendukung yang dibutuhkan untuk menjaga layanan tetap hidup.

Rumus awal:

$$\text{Generator Capacity} \approx \text{Beban Kritis Fasilitas} \times \text{Margin}$$

Namun generator tidak boleh dihitung terlalu sederhana. Faktor yang perlu diperhatikan:

- *IT load*
- Beban cooling yang harus tetap hidup
- UPS charging
- Inrush current
- Faktor daya
- Ketinggian lokasi
- Suhu lingkungan
- Redundansi
- Durasi bahan bakar
- Jadwal pengujian

Contoh:

- IT Load = 200 kW
- Beban cooling kritis = 90 kW
- Beban fasilitas lain = 30 kW
- Total beban kritis = 320 kW
- Margin 25% = 80 kW
- Kapasitas generator desain = **400 kW**

Jika target desain lebih tinggi, generator dapat dibuat N+1 atau 2N. Tetapi setiap pilihan meningkatkan biaya bahan bakar, ruang, suara, perizinan, maintenance, dan kompleksitas operasi.

Catatan strategis: generator besar tanpa uji berkala adalah rasa aman palsu. Untuk sertifikasi, generator harus punya bukti *load test*, log bahan bakar, SOP start manual, SOP transfer beban, dan kontrak maintenance.

3.7 Menghitung Kapasitas Pendinginan

Semua daya yang dipakai perangkat TI pada akhirnya menjadi panas. Karena itu, perhitungan cooling harus dimulai dari *IT load*. Jika IT load 100 kW, maka secara praktis data center harus mampu membuang panas setara 100 kW dari perangkat TI, ditambah pengaruh sistem lain sesuai desain.

Rumus konversi dasar:

$$\text{Cooling Capacity} \approx \text{IT Load dalam kW} \times 3.412 \text{ BTU/h}$$

Contoh:

- IT Load = 100 kW
- Cooling Capacity = $100 \times 3.412 = 341.200 \text{ BTU/h}$

Konversi ke TR, dengan pendekatan $1 \text{ TR} \approx 12.000 \text{ BTU/h}$:

$$\text{TR} \approx 341.200 / 12.000 = 28,43 \text{ TR}$$

Tambahkan margin, misalnya 20%:

$$\text{Cooling Design} \approx 34 \text{ TR}$$

Tetapi kapasitas cooling bukan hanya angka TR. Cooling harus sampai ke depan perangkat, terutama ke *server inlet*. ASHRAE TC 9.9 menjadi rujukan penting untuk kondisi termal data center; referensi ASHRAE menekankan bahwa temperatur, kelembaban, dew point, dan laju perubahan lingkungan harus dikontrol sesuai kelas perangkat ([ASHRAE](#)).

Data Center Handbook juga menekankan bahwa konsumsi energi HVAC dipengaruhi oleh kondisi luar, strategi economization, dan jenis cooling yang dipakai. Artinya, lokasi dan desain cooling akan mempengaruhi biaya operasi jangka panjang .

Checklist cooling awal:

- Berapa total IT load?
- Berapa kW per rack?
- Apakah ada rack densitas tinggi?
- Apakah memakai *hot aisle* / *cold aisle*?
- Apakah perlu *containment*?
- Apakah ada sensor suhu di *inlet* rak?
- Apakah ada jalur bypass udara?
- Apakah cooling tetap cukup saat satu unit gagal?

Kesalahan umum: membeli AC besar tanpa memperbaiki airflow. Akibatnya, ruangan dingin di titik tertentu, tetapi rak tetap panas.

3.8 Menghitung Estimasi PUE dan Biaya Energi

PUE membantu memperkirakan efisiensi fasilitas. Rumusnya:

$$\text{PUE} = \text{Total Energi Fasilitas} / \text{Energi Perangkat IT}$$

atau untuk estimasi daya:

$$\text{PUE} = \text{Total Facility Power} / \text{IT Load}$$

Contoh:

- IT Load = 100 kW
- Total Facility Power = 160 kW
- $\text{PUE} = 160 / 100 = 1,6$

Biaya energi tahunan:

$$\text{Energy Cost per Year} = \text{kW} \times 24 \times 365 \times \text{tarif listrik}$$

Contoh:

- Total Facility Power = 160 kW
- Operasi = 24 jam $\times$ 365 hari
- Tarif listrik = Rp1.500/kWh

Maka:

$$160 \times 24 \times 365 \times 1.500 = \text{Rp2.102.400.000 per tahun}$$

Jika PUE turun dari 1,8 ke 1,5 untuk IT Load 100 kW:

- PUE 1,8 $\rightarrow$ 180 kW fasilitas
- PUE 1,5 $\rightarrow$ 150 kW fasilitas
- Selisih = 30 kW
- Penghematan tahunan = $30 \times 24 \times 365 \times 1.500$
- Penghematan = **Rp394.200.000 per tahun**

The Green Grid juga menekankan bahwa PUE perlu digunakan sebagai alat analisis, bukan satu-satunya ukuran keberhasilan; publikasi PUE membahas fasilitas khusus, fasilitas campuran, *partial PUE*, skalabilitas, dan pemanfaatan ulang panas (thegreengrid.org). *Data Center Handbook* memperingatkan bahwa PUE yang lebih rendah bisa menyesatkan jika tidak disertai data granular IT load dan efisiensi perangkat; pengukuran sebaiknya dilakukan dalam periode penggunaan yang mewakili beban nyata .

Kalimat kunci: PUE penting, tetapi biaya energi nyata lebih penting.

3.9 Menghitung Pertumbuhan 3–5 Tahun

Data center yang baik tidak hanya cukup untuk hari pertama. Ia harus dirancang untuk tumbuh tanpa membongkar sistem utama. Pertumbuhan harus dihitung pada empat dimensi:

- Pertumbuhan jumlah perangkat
- Pertumbuhan *IT load*
- Pertumbuhan rak
- Pertumbuhan cooling dan power

Rumus sederhana:

$$\text{Kapasitas Tahun ke-}n = \text{Kapasitas Awal} \times (1 + \text{Growth Rate})^n$$

Contoh:

- IT Load awal = 100 kW
- Growth = 15% per tahun
- Tahun ke-5 = $100 \times (1,15)^5$
- Tahun ke-5 $\approx$ **201 kW**

Artinya, dalam 5 tahun, beban bisa menjadi dua kali lipat. Jika desain hanya menyiapkan 120 kW, fasilitas akan cepat penuh.

Contoh tabel pertumbuhan:

Tahun	IT Load	Jumlah Rack	Rata-rata kW/Rack	Catatan
0	100 kW	20	5 kW	Awal operasi
1	115 kW	23	5 kW	Tambah layanan
2	132 kW	26	5,1 kW	Perlu cek cooling
3	152 kW	30	5,1 kW	Review UPS
4	175 kW	34	5,1 kW	Review generator
5	201 kW	40	5 kW	Butuh ekspansi formal

Prinsip desain: kapasitas 5 tahun tidak harus langsung dibeli semua, tetapi **jalur ekspansinya harus sudah disiapkan:** ruang, panel, jalur kabel, pipa cooling, breaker, monitoring, dan rencana migrasi.

3.10 Menentukan Ruang Cadangan dan Stranded Capacity

Stranded capacity adalah kapasitas yang secara teori tersedia, tetapi tidak bisa dipakai karena ada bottleneck di komponen lain.

Contoh:

- Masih ada ruang untuk 10 rak, tetapi daya sudah habis.
- UPS masih cukup, tetapi cooling tidak cukup.
- Cooling masih cukup, tetapi panel distribusi penuh.
- Rak masih kosong, tetapi port jaringan tidak cukup.
- Generator cukup besar, tetapi jalur distribusi tidak mendukung.
- Ruang masih luas, tetapi lantai tidak kuat untuk rak berat.

Stranded capacity berbahaya karena menciptakan ilusi kapasitas. Manajemen merasa fasilitas masih longgar, padahal secara operasional sudah buntu.

Cara mencegah:

- Hitung kapasitas per domain: space, power, cooling, network, storage, security.
- Gunakan dashboard kapasitas.
- Lakukan review triwulanan.
- Jangan hanya melaporkan jumlah rak kosong.
- Laporkan **kapasitas yang benar-benar dapat dipakai**.

Rumus berpikir: kapasitas data center = kapasitas terkecil dari semua sistem pendukung.

Materi Praktek 1: Contoh Perhitungan Data Center 10 Rack

Asumsi

- Jumlah rak: 10
- Rata-rata beban: 5 kW/rack
- IT Load: $10 \times 5 = \mathbf{50\ kW}$
- Target PUE: 1,7
- Margin desain: 20%
- Tarif listrik: Rp1.500/kWh

Perhitungan

Total Facility Power = IT Load $\times$ PUE
 $50 \times 1,7 = \mathbf{85\ kW}$

Daya desain dengan margin
 $85 \times 1,2 = \mathbf{102\ kW}$

Cooling Capacity
 $50 \times 3.412 = \mathbf{170.600\ BTU/h}$

Cooling dalam TR
 $170.600 / 12.000 = \mathbf{14,2\ TR}$

Dengan margin 20%:

$14,2 \times 1,2 = \mathbf{17\ TR}$

Biaya energi tahunan
 $85 \times 24 \times 365 \times 1.500 = \mathbf{Rp1.116.900.000\ per\ tahun}$

Catatan Desain

Untuk 10 rak, fokus utama adalah **disiplin dasar**: UPS cukup, cooling merata, kabel rapi, akses fisik terkendali, monitoring suhu tersedia, dan kapasitas tumbuh tidak liar.

Materi Praktek 2: Contoh Perhitungan Data Center 50 Rack

Asumsi

- Jumlah rak: 50
- Rata-rata beban: 6 kW/rack
- IT Load: $50 \times 6 = \mathbf{300 \text{ kW}}$
- Target PUE: 1,6
- Margin desain: 20%
- Tarif listrik: Rp1.500/kWh

Perhitungan

Total Facility Power

$$300 \times 1,6 = \mathbf{480 \text{ kW}}$$

Daya desain dengan margin

$$480 \times 1,2 = \mathbf{576 \text{ kW}}$$

Cooling Capacity

$$300 \times 3.412 = \mathbf{1.023.600 \text{ BTU/h}}$$

Cooling dalam TR

$$1.023.600 / 12.000 = \mathbf{85,3 \text{ TR}}$$

Dengan margin 20%:

$$85,3 \times 1,2 = \mathbf{102,4 \text{ TR}}$$

Biaya energi tahunan

$$480 \times 24 \times 365 \times 1.500 = \mathbf{Rp6.307.200.000 \text{ per tahun}}$$

Catatan Desain

Pada 50 rak, pendekatan *server room* tidak lagi memadai. Dibutuhkan **capacity planning formal**, *containment*, UPS yang jelas arsitekturnya, generator, sensor lingkungan, dokumentasi kabel, dan prosedur perubahan.

Materi Praktek 3: Contoh Perhitungan Data Center 100 Rack

Asumsi

- Jumlah rak: 100
- Rata-rata beban: 8 kW/rack
- IT Load: $100 \times 8 = \mathbf{800 \text{ kW}}$
- Target PUE: 1,5
- Margin desain: 20%
- Tarif listrik: Rp1.500/kWh

Perhitungan

Total Facility Power

$$800 \times 1,5 = \mathbf{1.200 \text{ kW}}$$

Daya desain dengan margin

$$1.200 \times 1,2 = \mathbf{1.440 \text{ kW}}$$

Cooling Capacity

$$800 \times 3.412 = \mathbf{2.729.600 \text{ BTU/h}}$$

Cooling dalam TR

$$2.729.600 / 12.000 = \mathbf{227,5 \text{ TR}}$$

Dengan margin 20%:

$$227,5 \times 1,2 = \mathbf{273 \text{ TR}}$$

Biaya energi tahunan

$$1.200 \times 24 \times 365 \times 1.500 = \mathbf{Rp15.768.000.000 \text{ per tahun}}$$

Catatan Desain

Pada 100 rak, kesalahan kecil menjadi biaya besar. Selisih PUE 0,1 saja pada IT Load 800 kW berarti:

$$0,1 \times 800 = \mathbf{80 \text{ kW}}$$

Pengaruh biaya tahunan:

$$80 \times 24 \times 365 \times 1.500 = \mathbf{Rp1.051.200.000 \text{ per tahun}}$$

Kesimpulan: efisiensi bukan isu lingkungan saja; efisiensi adalah isu anggaran dan daya saing.

Materi Praktek 4: Tabel Perhitungan *Rack Density*

Kategori Rak	kW/Rack	Karakter	Implikasi Desain
Rendah	1–3 kW	Perangkat ringan	Cooling sederhana, risiko rendah
Menengah	4–6 kW	Umum untuk enterprise	Perlu airflow baik dan monitoring
Tinggi	7–12 kW	Beban padat	Perlu containment dan distribusi daya kuat
Sangat tinggi	>12 kW	GPU / HPC / AI	Perlu desain cooling khusus, mungkin liquid cooling

Catatan: angka kategori bersifat panduan awal. Desain final harus mengikuti perangkat nyata, standar lingkungan, kemampuan cooling, dan target sertifikasi.

Materi Praktek 5: Template Kalkulasi Kapasitas 5 Tahun

Item	Tahun 0	Tahun 1	Tahun 2	Tahun 3	Tahun 4	Tahun 5
Jumlah rack						
Rata-rata kW/rack						
Total IT Load						
Target PUE						
Total Facility Power						
Kebutuhan UPS						
Kebutuhan generator						
Cooling BTU/h						
Cooling TR						
Kapasitas jaringan						
Kapasitas storage						
Risiko bottleneck						
Keputusan ekspansi						

Cara membaca template: kolom tahun ke-3 dan ke-5 sangat penting untuk sertifikasi, karena auditor dan manajemen perlu melihat apakah desain hanya cukup untuk hari pertama atau benar-benar siap tumbuh.

Materi Praktek 6: Latihan — 30 Rack @ 6 kW/Rack

Soal

Sebuah organisasi ingin membangun *data center* 30 rak. Setiap rak direncanakan memiliki beban rata-rata 6 kW. Target PUE adalah 1,6. Tarif listrik Rp1.500/kWh. Margin desain 20%.

Hitung:

1. Total IT Load
2. Total Facility Power
3. Daya desain dengan margin
4. Cooling Capacity dalam BTU/h
5. Cooling Capacity dalam TR
6. Estimasi biaya energi tahunan
7. Risiko desain yang harus diperhatikan

Jawaban

1. Total IT Load

$$30 \times 6 \text{ kW} = \mathbf{180 \text{ kW}}$$

2. Total Facility Power

$$180 \times 1,6 = \mathbf{288 \text{ kW}}$$

3. Daya desain dengan margin 20%

$$288 \times 1,2 = \mathbf{345,6 \text{ kW}}$$

4. Cooling Capacity

$$180 \times 3.412 = \mathbf{614.160 \text{ BTU/h}}$$

5. Cooling dalam TR

$$614.160 / 12.000 = \mathbf{51,18 \text{ TR}}$$

Dengan margin 20%:

$$51,18 \times 1,2 = \mathbf{61,4 \text{ TR}}$$

6. Biaya energi tahunan

$$288 \times 24 \times 365 \times 1.500 = \mathbf{Rp3.784.320.000 \text{ per tahun}}$$

7. Risiko desain

- UPS kurang besar jika pertumbuhan cepat.
- Cooling tidak merata jika layout rak buruk.
- PUE target tidak tercapai jika beban awal rendah.
- Generator harus mampu membawa beban kritis.
- Kapasitas panel dan PDU harus mengikuti ekspansi.
- Rak 6 kW/rack perlu monitoring suhu dan daya per rak.

Ringkasan Bab 3

Bab ini menegaskan bahwa **perencanaan data center adalah pekerjaan angka**. Semua keputusan besar—ruang, rak, listrik, UPS, generator, cooling, PUE, biaya energi, dan ekspansi—harus diturunkan dari *IT load* yang jelas.

PUE penting sebagai ukuran efisiensi, tetapi tidak boleh dipakai secara dangkal. Beban rendah, desain listrik, strategi cooling, iklim, dan cara pengukuran dapat memengaruhi hasil PUE. Karena itu, pengelola harus membaca PUE bersama biaya energi, kapasitas terpakai, dan kualitas operasi. *Data Center Handbook* mengingatkan bahwa desain power dan cooling harus dioptimalkan bersama, bukan diputuskan terpisah antar-domain .

Inti bab: jangan membeli kapasitas sebelum menghitung beban; jangan mengejar efisiensi sebelum memahami pola operasi; jangan bicara sertifikasi sebelum punya angka desain yang bisa diaudit.

Checklist Akhir Bab 3

Sebelum masuk Bab 4, pembaca harus mampu menjawab:

- Berapa **Total IT Load** awal?
- Berapa **IT Load desain** setelah margin?
- Berapa jumlah rak yang dibutuhkan?
- Berapa rata-rata **kW/rack**?
- Berapa kebutuhan *white space*?
- Berapa **Total Facility Power**?
- Berapa kapasitas UPS?
- Berapa kapasitas generator?
- Berapa kapasitas cooling dalam BTU/h dan TR?
- Berapa estimasi PUE?
- Berapa estimasi biaya energi tahunan?
- Berapa kebutuhan kapasitas 3–5 tahun?
- Di mana potensi *stranded capacity*?
- Apakah semua angka sudah bisa menjadi **bukti desain untuk audit dan sertifikasi**?

Penutup bab: *Data center* professional tidak dimulai dari katalog perangkat, tetapi dari angka beban yang jujur, perhitungan yang rapi, dan keputusan kapasitas yang dapat dipertanggungjawabkan.

Bab 4. Desain Ruang, Rack, Kabel, Jalur, dan *White Space*

Golden Rule: Ruang data center harus dirancang untuk operasi, ekspansi, keselamatan, dan pemeliharaan, bukan sekadar agar perangkat bisa masuk.

Bab ini membahas desain fisik *data center*: ruang, rak, jalur kabel, jalur listrik, area kerja, akses barang, dan *white space*. Dalam outline buku, Bab 4 memang diarahkan untuk membahas *space planning*, *white space*, *gray space*, ruang MEP, ruang staging, NOC, layout rak, *raised floor*, *slab floor*, jalur kabel, labeling, akses barang, dan kesalahan umum desain ruang .

Inti bab ini sederhana: **ruang yang buruk akan membuat data center mahal dioperasikan, sulit diperluas, berisiko panas, sulit diaudit, dan berbahaya saat terjadi insiden.**

4.1 Prinsip *Space Planning*

Space planning adalah proses merancang ruang *data center* agar seluruh sistem dapat dipasang, dioperasikan, dipelihara, diamankan, dan dikembangkan secara teratur. Ruang tidak boleh dihitung hanya dari jumlah rak. Ruang harus dihitung dari **alur kerja manusia, alur udara, alur kabel, alur daya, alur barang, dan alur evakuasi.**

Data Center Handbook menekankan bahwa desain kapasitas awal dan ekspansi masa depan harus menyeimbangkan **scalability** dan **reliability**, termasuk pada layout rak, distribusi cooling, dan arsitektur jaringan . Ini penting karena data center bukan ruang statis. Beban akan tumbuh, rak bertambah, kabel berubah, perangkat diganti, dan sistem pendinginan harus tetap efektif.

Prinsip dasar *space planning*:

- **Ruang harus mendukung operasi harian**, bukan hanya instalasi awal.
- **Jalur teknisi harus jelas**, aman, dan tidak terganggu kabel.
- **Jalur barang harus cukup besar** dari loading area sampai ruang komputer.
- **Ruang ekspansi harus dirancang sejak awal**, bukan dicari belakangan.
- **Ruang kritikal harus dipisah** dari ruang non-kritikal.
- **Akses harus dikontrol**, terutama ke ruang komputer, ruang listrik, ruang baterai, dan ruang jaringan.

Dalam konteks sertifikasi, *space planning* harus bisa dibuktikan melalui gambar layout, daftar ruang, kapasitas rak, jalur akses, jalur kabel, jalur evakuasi, dan dokumentasi perubahan. ISO/IEC 22237 juga memandang data center sebagai fasilitas dengan kebutuhan desain, perencanaan, pengadaan, integrasi, instalasi, operasi, dan pemeliharaan yang saling terkait. ([ISO](#))

Kalimat kunci: ruang data center yang baik adalah ruang yang memudahkan operasi saat normal dan mempercepat respons saat krisis.

4.2 White Space, Gray Space, Ruang MEP, Ruang Staging, dan Ruang NOC

White space adalah ruang utama tempat perangkat TI dipasang: rak server, storage, perangkat jaringan, perangkat keamanan, dan sistem pendukung langsung. Inilah area yang sering dianggap sebagai “data center” oleh orang awam. Padahal, *white space* hanya satu bagian dari keseluruhan fasilitas.

Gray space adalah area pendukung fasilitas seperti ruang listrik, UPS, baterai, generator, panel distribusi, cooling plant, pompa, dan sistem mekanikal-elektrikal lainnya. Tanpa *gray space*, *white space* tidak bisa hidup. Banyak desain gagal karena terlalu fokus pada rak, tetapi melupakan ruang untuk panel, UPS, baterai, chiller, pipa, jalur maintenance, dan ruang servis.

Ruang MEP adalah ruang untuk *mechanical, electrical, and plumbing*. Ini termasuk ruang panel, ruang UPS, ruang baterai, ruang pendinginan, ruang pompa, ruang pipa, dan ruang kontrol fasilitas. Ruang ini harus mudah diakses teknisi, tetapi tetap aman dari akses tidak sah.

Ruang *staging* digunakan untuk menerima, membuka, memeriksa, merakit, memberi label, dan menguji perangkat sebelum masuk ke *white space*. Tanpa ruang *staging*, kardus, pallet, plastik, dan aktivitas bongkar perangkat akan masuk ke ruang komputer. Ini berisiko terhadap kebersihan, keamanan, dan keselamatan.

Ruang NOC, atau *Network Operations Center*, adalah ruang pemantauan operasi. *Data Center Handbook* menjelaskan bahwa NOC biasanya mendukung operasi TI 24×7, sering ditempatkan berdekatan dengan ruang komputer, dan dapat menjadi lapisan kontrol akses tambahan karena orang yang masuk ke ruang komputer dapat terlihat oleh personel NOC .

Pembagian ruang minimum:

Ruang	Fungsi	Catatan Desain
<i>White space</i>	Rak TI dan perangkat aktif	Fokus pada airflow, kabel, daya, keamanan
<i>Gray space</i>	Infrastruktur fasilitas	UPS, panel, cooling, baterai, generator
Ruang MEP	Mekanikal, elektrikal, plumbing	Harus mudah dipelihara
Ruang <i>staging</i>	Persiapan perangkat	Hindari kardus masuk ruang komputer
NOC	Monitoring dan operasi	Dekat ruang komputer, akses terkendali
Entrance room	Terminasi koneksi luar	Dekat ruang komputer, jalur aman

TIA-942 juga mencakup kebutuhan fisik data center seperti lokasi, arsitektur, listrik, mekanikal, *fire safety*, telekomunikasi, dan keamanan. Karena itu, pembagian ruang harus dipandang sebagai bagian dari desain sertifikasi, bukan sekadar layout arsitektur. ([TIA Online](#))

4.3 Layout Rak: Baris, Lorong Panas, Lorong Dingin

Layout rak menentukan kualitas air flow, panjang kabel, kemudahan maintenance, dan keamanan operasi. Pola paling umum adalah baris rak dengan orientasi **depan bertemu depan** dan **belakang bertemu belakang**. Bagian depan rak membentuk *cold aisle*, sedangkan bagian belakang rak membentuk *hot aisle*.

Cold aisle adalah lorong tempat udara dingin masuk ke bagian depan perangkat. *Hot aisle* adalah lorong tempat udara panas keluar dari belakang perangkat. Jika orientasi rak kacau, udara panas dapat kembali masuk ke bagian depan server. Akibatnya, suhu *inlet* naik, perangkat bekerja lebih keras, kipas berputar lebih cepat, konsumsi energi naik, dan risiko gangguan meningkat.

Referensi standar TIA menjelaskan bahwa rak sebaiknya disusun dengan pola bergantian agar membentuk *hot aisle* dan *cold aisle*; *cold aisle* berada di depan rak, sedangkan *hot aisle* berada di belakang rak. (grouper.ieee.org)

Prinsip layout rak:

- **Depan rak harus menghadap depan rak** untuk membentuk *cold aisle*.
- **Belakang rak harus menghadap belakang rak** untuk membentuk *hot aisle*.
- Gunakan *blanking panel* pada U kosong agar udara tidak bocor.
- Jangan campur perangkat yang membuang panas ke arah berbeda tanpa analisis airflow.
- Pisahkan rak densitas tinggi dari rak biasa jika cooling tidak merata.
- Sediakan ruang cukup di depan dan belakang rak untuk teknisi.
- Jangan meletakkan barang sementara di lorong panas atau lorong dingin.

Untuk desain profesional, layout rak harus selalu dikaitkan dengan *rack density*. Rak 3 kW, 6 kW, 12 kW, dan GPU tinggi tidak boleh diperlakukan sama. *Data Center Virtualization Fundamentals* menegaskan bahwa perangkat dengan densitas tinggi seperti *blade server* membutuhkan perhatian khusus dari sisi distribusi daya dan pendinginan .

Prinsip tajam: layout rak yang salah tidak bisa diselesaikan hanya dengan menambah AC.

4.4 Raised Floor vs Slab Floor

Raised floor adalah lantai panggung yang menyediakan ruang di bawah lantai. Secara historis, ruang ini sering dipakai untuk distribusi udara dingin, kabel, pipa, dan grounding. Keuntungannya adalah fleksibilitas, terutama untuk perubahan layout dan kebutuhan teknologi masa depan.

Namun *raised floor* bukan selalu pilihan terbaik. Ia membutuhkan tinggi ruang yang cukup, biaya tambahan, struktur yang benar, manajemen kebocoran udara, dan perhatian terhadap beban lantai. Jika tidak dirawat, ruang bawah lantai bisa penuh kabel, debu, hambatan airflow, dan titik risiko.

Slab floor adalah lantai langsung tanpa lantai panggung. Desain ini sering memakai jalur kabel dan distribusi daya dari atas. Keuntungannya adalah struktur lebih sederhana, akses bawah lantai tidak menjadi masalah, dan alur kabel bisa lebih terlihat. Namun desain ini menuntut koordinasi overhead yang rapi antara kabel data, kabel listrik, jalur grounding, lighting, sensor, sprinkler, dan containment.

Data Center Handbook menjelaskan bahwa jika cooling tidak memakai bawah lantai, *raised floor* tidak selalu diperlukan, tetapi *raised floor* tetap dapat memberi fleksibilitas untuk kebutuhan masa depan, termasuk potensi jalur fluida untuk teknologi *liquid cooling*. Buku yang sama juga mengingatkan bahwa perbedaan elevasi lantai dapat memaksa penggunaan ramp yang memakan ruang cukup besar.

Perbandingan ringkas:

Aspek	<i>Raised Floor</i>	<i>Slab Floor</i>
Fleksibilitas	Tinggi	Sedang
Distribusi udara bawah lantai	Bisa	Tidak
Jalur kabel bawah lantai	Bisa	Tidak
Jalur overhead	Tetap bisa	Umum dipakai
Risiko ruang tersembunyi	Ada	Lebih kecil
Biaya konstruksi	Lebih tinggi	Lebih sederhana
Cocok untuk retrofit	Tergantung tinggi ruang	Sering lebih mudah
Tantangan	Ramp, kebocoran udara, beban lantai	Koordinasi jalur atas

Kesimpulan praktis: pilih *raised floor* atau *slab floor* berdasarkan **cooling strategy, tinggi ruang, beban lantai, jalur kabel, kebutuhan ekspansi, dan target operasi**, bukan karena kebiasaan lama.

4.5 Jalur Kabel Data dan Kabel Power

Jalur kabel adalah urat saraf data center. Kabel yang buruk membuat troubleshooting lambat, airflow terganggu, risiko salah cabut meningkat, dan audit menjadi sulit. Jalur kabel harus dirancang sejak awal, bukan mengikuti sisa ruang.

Prinsip utama: **kabel data dan kabel power harus dipisahkan secara rapi dan aman.** Pemisahan ini mengurangi risiko gangguan, memudahkan identifikasi, dan membantu maintenance. Jalur kabel harus memiliki tray, ladder rack, conduit, atau jalur khusus yang terdokumentasi.

Dalam desain terstruktur, TIA-942 mengenal ruang dan elemen seperti *Entrance Room*, *Main Distribution Area* atau MDA, *Horizontal Distribution Area* atau HDA, *Equipment Distribution Area* atau EDA, *Zone Distribution Area* atau ZDA, serta *backbone cabling* dan *horizontal cabling*. MDA menjadi titik utama distribusi kabel, HDA menjadi titik distribusi horizontal, dan EDA menjadi area perangkat aktif; standar ini juga menekankan fleksibilitas, skalabilitas, reliabilitas, dan manajemen ruang .

Jalur kabel harus dirancang untuk:

- Kapasitas awal.
- Pertumbuhan 3–5 tahun.
- Pemisahan kabel data dan power.
- Pemisahan jalur A dan B untuk redundansi.
- Kemudahan patching.
- Radius tekuk kabel, terutama fiber.
- Labeling di kedua ujung kabel.
- Akses teknisi tanpa mengganggu airflow.
- Dokumentasi *as-built*.

Kesalahan umum: jalur kabel terlalu kecil untuk pertumbuhan. Pada tahun pertama terlihat rapi. Tahun ketiga penuh. Tahun kelima menjadi risiko operasi.

Aturan praktis: jangan hanya bertanya “kabel bisa masuk atau tidak”; tanyakan **apakah kabel masih bisa dikelola, dilacak, diganti, diaudit, dan diperluas.**

4.6 Labeling, Dokumentasi, dan Standar Instalasi

Labeling adalah bahasa operasional data center. Tanpa label yang konsisten, teknisi akan menebak. Dalam fasilitas kritikal, menebak adalah risiko.

Setiap rak, panel, PDU, port jaringan, patch panel, kabel, tray, sensor, perangkat, dan jalur daya harus memiliki identitas. Format penomoran harus konsisten sejak awal dan digunakan dalam gambar layout, tabel aset, *patching record*, *power map*, dan sistem monitoring.

Minimal dokumentasi yang harus tersedia:

- Layout ruang.
- Peta rak.
- Daftar rak dan perangkat.
- Peta patch panel.
- Peta koneksi kabel.
- Peta PDU dan sumber daya A/B.
- Gambar jalur kabel.
- Gambar jalur listrik.
- Data beban per rak.
- Dokumentasi perubahan.
- Foto instalasi.
- Dokumen *as-built*.

Untuk sertifikasi, dokumentasi bukan pelengkap. Dokumentasi adalah **bukti bahwa desain dapat dioperasikan dan diaudit**. Outline buku juga menekankan bahwa setiap bab perlu ditutup dengan keputusan desain, bukti yang disiapkan, dan risiko jika keputusan salah .

Kalimat tajam: kabel tanpa label adalah utang risiko yang akan ditagih saat insiden.

4.7 Beban Lantai, Akses Barang, Pintu, Ramp, dan Jalur Evakuasi

Ruang data center harus mampu menerima perangkat besar dan berat. Rak, UPS, baterai, perangkat storage, cooling unit, panel, dan pallet perangkat membutuhkan jalur masuk yang aman. Jangan sampai perangkat bisa dibeli tetapi tidak bisa masuk ke ruangan.

Data Center Handbook menjelaskan bahwa data center harus mendukung penggantian perangkat TI, power, dan cooling dengan clearance yang memadai dari loading dock ke ruang komputer, ruang listrik, dan ruang mekanikal. Referensi tersebut menyebut koridor minimal 2,7 m, pintu tunggal minimum 2,4 m tinggi dan 1,1 m lebar, serta pintu ganda minimum 1,8 m lebar sebagai pertimbangan desain akses .

Aspek yang harus dicek:

- Beban lantai untuk rak penuh.
- Beban titik untuk perangkat berat.
- Jalur dari loading area ke ruang data center.
- Lebar pintu.
- Tinggi pintu.
- Radius belok lorong.
- Ketersediaan ramp jika beda elevasi.
- Area manuver pallet.
- Jalur evakuasi manusia.
- Akses pemadam dan keselamatan.
- Pemisahan jalur barang dari jalur publik.

Ramp harus dihitung serius. Jika terlalu curam, berbahaya untuk perangkat berat. Jika terlalu panjang, memakan ruang. Jika terlalu sempit, tidak mendukung operasi.

Prinsip keselamatan: ruang data center tidak hanya harus aman untuk perangkat, tetapi juga **aman untuk manusia yang mengoperasikannya**.

4.8 Kesalahan Umum Desain Ruang

Kesalahan pertama adalah menghitung ruang hanya dari jumlah rak. Akibatnya, tidak ada ruang cukup untuk teknisi, kabel, panel, sensor, staging, dan ekspansi.

Kesalahan kedua adalah mencampur jalur kabel data dan kabel power tanpa disiplin. Ini menyulitkan audit, maintenance, dan troubleshooting.

Kesalahan ketiga adalah tidak menyiapkan ruang *staging*. Perangkat dibuka di ruang komputer, kardus masuk, debu masuk, dan proses instalasi mengganggu operasi.

Kesalahan keempat adalah layout rak tidak mengikuti prinsip *hot aisle* dan *cold aisle*. Akibatnya, air flow kacau dan cooling boros.

Kesalahan kelima adalah memilih *raised floor* tanpa menghitung ramp, tinggi ruang, beban lantai, dan dampak maintenance.

Kesalahan keenam adalah tidak menyediakan jalur barang yang memadai. Perangkat besar akhirnya harus dibongkar berlebihan, diputar di lorong sempit, atau dipasang dengan risiko.

Kesalahan ketujuh adalah dokumentasi terlambat. Setelah instalasi selesai, tim lupa mencatat kabel, port, PDU, dan posisi perangkat. Akibatnya, *as-built* tidak sama dengan kondisi nyata.

Kesalahan paling fatal: menganggap ruang data center sebagai urusan arsitektur saja. Padahal, ruang menentukan **power, cooling, network, security, maintenance, audit, dan keselamatan**.

Materi Praktek 1: Contoh Layout 10 Rack

Asumsi

- Jumlah rak: 10
- Beban rata-rata: 4–6 kW/rack
- Target: data center kecil / menengah awal
- Model cooling: udara dingin berbasis lorong
- Kebutuhan: mudah dipantau, mudah diperluas, tidak terlalu kompleks

Rekomendasi Layout

Gunakan 2 baris, masing-masing 5 rak.

```
Cold Aisle
[R1] [R2] [R3] [R4] [R5]
      <-- depan rak -->

      <-- belakang rak -->
[R6] [R7] [R8] [R9] [R10]
Hot Aisle
```

Catatan Desain

- Pastikan bagian depan rak saling berhadapan untuk membentuk *cold aisle*.
- Letakkan patch panel secara konsisten.
- Pisahkan jalur kabel power dan data.
- Sediakan ruang kecil untuk *staging*.
- Pasang sensor suhu di area *inlet* rak.
- Siapkan minimal 1–2 posisi rak kosong untuk ekspansi.
- Dokumentasikan port, PDU, dan kabel sejak hari pertama.

Risiko utama 10 rack: karena kecil, sering dianggap sederhana. Justru di sini disiplin awal menentukan apakah fasilitas bisa tumbuh tanpa kacau.

Materi Praktek 2: Contoh Layout 50 Rack

Asumsi

- Jumlah rak: 50
- Beban rata-rata: 5–8 kW/rack
- Target: data center profesional menengah
- Model: beberapa lorong panas/dingin
- Kebutuhan: ekspansi, redundansi, monitoring, dan kesiapan audit

Rekomendasi Layout

Gunakan 5 blok, masing-masing 10 rak. Setiap blok terdiri dari 2 baris × 5 rak.

Blok A	Blok B	Blok C	Blok D	Blok E
10 rack	10 rack	10 rack	10 rack	10 rack

Setiap blok harus memiliki pola:

- *Cold aisle* di depan rak.
- *Hot aisle* di belakang rak.
- Jalur kabel data terstruktur.
- Jalur power A/B jelas.
- Ruang kerja teknisi di depan dan belakang.
- Jalur evakuasi tidak terhalang.

Catatan Desain

Untuk 50 rack, desain harus mulai serius pada:

- Jalur kabel overhead atau bawah lantai.
- *Containment* jika densitas tinggi.
- Ruang MDA/HDA/EDA.
- Ruang NOC.
- Ruang *staging*.
- Jalur barang.
- Ruang listrik dekat *white space*.
- Monitoring suhu dan daya per baris/rack.
- Dokumentasi *as-built*.

Risiko utama 50 rack: ekspansi organik tanpa kontrol. Rak bertambah, kabel bertambah, cooling tertinggal, dan dokumentasi rusak.

Materi Praktek 3: Checklist Desain Ruangan

Area Pemeriksaan	Pertanyaan	Status
Fungsi ruang	Apakah <i>white space</i> , <i>gray space</i> , MEP, staging, dan NOC sudah dipisahkan?	Ya / Tidak
Kapasitas rak	Apakah jumlah rak awal dan 5 tahun sudah dihitung?	Ya / Tidak
Rack density	Apakah kW/rack sudah diketahui?	Ya / Tidak
Layout rak	Apakah sudah membentuk <i>hot aisle</i> dan <i>cold aisle</i> ?	Ya / Tidak
Cooling	Apakah airflow mengikuti layout rak?	Ya / Tidak
Kabel data	Apakah jalur kabel data jelas dan cukup untuk ekspansi?	Ya / Tidak
Kabel power	Apakah jalur power A/B dipisahkan dan terdokumentasi?	Ya / Tidak
Labeling	Apakah format label rak, kabel, port, dan PDU sudah baku?	Ya / Tidak
Akses barang	Apakah perangkat bisa masuk dari loading area ke ruang komputer?	Ya / Tidak
Pintu	Apakah tinggi dan lebar pintu cukup untuk rak/perangkat besar?	Ya / Tidak
Ramp	Apakah ramp aman, tidak terlalu curam, dan cukup lebar?	Ya / Tidak
Beban lantai	Apakah struktur lantai mendukung rak penuh?	Ya / Tidak
Evakuasi	Apakah jalur evakuasi tidak terhalang?	Ya / Tidak
Keamanan	Apakah akses ke ruang kritikal dikontrol?	Ya / Tidak
Dokumentasi	Apakah layout dan <i>as-built</i> siap diperbarui?	Ya / Tidak

Cara pakai: checklist ini dipakai sebelum desain final, sebelum konstruksi, dan sebelum audit internal.

Materi Praktek 4: Template Penomoran Rack, Patch Panel, PDU, dan Jalur Kabel

Format Penomoran Rack

Contoh:

DC1-R01-A01

Artinya:

- DC1 = lokasi data center
- R01 = baris rak nomor 01
- A01 = rak nomor 01 pada baris A

Contoh tabel:

Kode Rack	Baris	Posisi	Fungsi	kW Target	Catatan
DC1-A01	A	01	Network	4 kW	MDA
DC1-A02	A	02	Server	6 kW	Produksi
DC1-A03	A	03	Server	6 kW	Produksi
DC1-B01	B	01	Storage	8 kW	Perlu airflow baik

Format Patch Panel

Contoh:

PP-DC1-A01-01

Artinya:

- PP = patch panel
- DC1 = lokasi
- A01 = rack
- 01 = patch panel nomor 01

Format Port

Contoh:

DC1-A01-PP01-P24 → DC1-B03-SW01-P12

Artinya kabel menghubungkan patch panel port 24 di rack A01 ke switch port 12 di rack B03.

Format PDU

Contoh:

- **PDU-A-DC1-A01**
- **PDU-B-DC1-A01**

Setiap perangkat kritikal sebaiknya memiliki sumber A dan B jika desain mendukung.

Format Jalur Kabel

Contoh:

- **TRAY-DATA-A1**
- **TRAY-POWER-B1**
- **FIBER-BACKBONE-MDA-HDA01**

Prinsip: format penomoran harus pendek, konsisten, dan bisa dibaca oleh teknisi saat insiden.

Materi Praktek 5: Contoh *Bill of Quantity* Awal

Contoh ini bukan desain final, tetapi daftar awal untuk diskusi teknis dan anggaran.

Item	Satuan	Jumlah Awal	Catatan
Rack 42U	unit	10 / 50	Sesuaikan desain
Blanking panel	set	sesuai U kosong	Wajib untuk airflow
Cable manager vertical	unit	per rack	Untuk kerapian kabel
Cable manager horizontal	unit	sesuai kebutuhan	Patch panel dan switch
Patch panel fiber	unit	sesuai port	MDA/HDA/EDA
Patch panel tembaga	unit	sesuai port	Jika dibutuhkan
Fiber optic cable	meter	sesuai layout	Backbone / uplink
Kabel tembaga data	meter	sesuai layout	Horizontal cabling
Ladder rack / cable tray data	meter	sesuai jalur	Pisah dari power
Cable tray power	meter	sesuai jalur	Jalur A/B
Rack PDU A	unit	per rack	Sumber A
Rack PDU B	unit	per rack	Sumber B
Sensor suhu	unit	minimal per lorong/rack penting	Fokus <i>inlet</i>
Sensor kelembapan	unit	sesuai zona	Monitoring lingkungan
Label kabel	set	sesuai kabel	Dua ujung kabel
Label rack	set	per rack	Depan dan belakang
CCTV area	unit	sesuai desain keamanan	Akses dan lorong
Access control	titik	sesuai pintu	Ruang kritikal
Fire detection	titik	sesuai desain	Koordinasi keselamatan
Ruang staging	area	1	Dekat akses barang
Dokumentasi <i>as-built</i>	paket	1	Wajib untuk audit

Catatan: *bill of quantity* harus selalu dikaitkan dengan gambar layout. Daftar barang tanpa layout akan menimbulkan salah beli.

Ringkasan Bab 4

Bab ini menegaskan bahwa desain ruang data center adalah keputusan strategis. Ruang menentukan apakah fasilitas mudah dioperasikan, mudah diperluas, aman, efisien, dan siap diaudit.

Desain yang baik tidak hanya menghitung jumlah rak. Desain yang baik menghitung **alur teknisi, alur barang, alur udara, alur kabel, alur daya, ruang kerja, ruang ekspansi, ruang MEP, ruang NOC, dan jalur evakuasi**.

Data Center Handbook menekankan pentingnya koordinasi antara sistem karena ruang, power, cooling, pathway, dan sistem lain saling mempengaruhi. Karena itu, keputusan ruang tidak boleh diambil terpisah dari tim listrik, cooling, jaringan, keamanan, operasi, dan audit.

Inti bab: ruang data center yang baik bukan yang paling penuh, tetapi yang paling aman, teratur, mudah dirawat, dan siap tumbuh.

Checklist Akhir Bab 4

Sebelum masuk Bab 5, pembaca harus mampu menjawab:

- Apakah *white space*, *gray space*, MEP, staging, dan NOC sudah jelas?
- Apakah jumlah rak awal dan rak 5 tahun sudah dihitung?
- Apakah layout rak sudah membentuk *hot aisle* dan *cold aisle*?
- Apakah strategi *raised floor* atau *slab floor* sudah dipilih berdasarkan kebutuhan nyata?
- Apakah jalur kabel data dan power sudah dipisahkan?
- Apakah jalur A/B untuk daya sudah jelas?
- Apakah MDA, HDA, EDA, dan entrance room sudah dipetakan?
- Apakah akses barang dari loading area ke ruang komputer aman?
- Apakah pintu, ramp, dan lorong cukup untuk perangkat besar?
- Apakah beban lantai sudah diperiksa?
- Apakah jalur evakuasi bebas hambatan?
- Apakah format labeling sudah baku?
- Apakah dokumen *as-built* akan dibuat sejak awal?
- Apakah desain ruang sudah siap menjadi **bukti audit dan sertifikasi**?

Penutup bab: *Data center* professional dibangun dari ruang yang disiplin: **setiap rak punya posisi, setiap kabel punya jalur, setiap perangkat punya label, setiap teknisi punya akses aman, dan setiap keputusan punya dokumen.**

Bab 5. Sistem Kelistrikan: Utility, UPS, Generator, PDU, Grounding

Golden Rule: Sistem listrik data center harus dirancang dengan prinsip redundansi, selektivitas proteksi, keselamatan, dan kemudahan pemeliharaan.

Bab ini membahas sistem kelistrikan sebagai tulang punggung *data center*. Dalam outline buku, Bab 5 diarahkan untuk membahas arsitektur *power*, *utility feed*, panel utama, UPS, generator, PDU, *grounding*, redundansi N/N+1/2N, proteksi petir, pengujian kelistrikan, dan dokumentasi *single line diagram*.

Sertifikasi profesional tidak hanya menilai apakah listrik tersedia. Yang dinilai adalah apakah listrik **stabil, aman, redundan, terukur, dapat diuji, dapat dipelihara, dan memiliki bukti dokumentasi**. Uptime Institute menempatkan *Tier Standard* sebagai standar global untuk ketersediaan dan kinerja data center, termasuk kemampuan fasilitas memenuhi kebutuhan operasi melalui beberapa tingkat performa infrastruktur ([Uptime Institute](https://www.uptimeinstitute.com/)).

5.1 Arsitektur Power Data Center

Arsitektur listrik *data center* harus dipahami sebagai rantai energi dari sumber listrik sampai perangkat TI. Rantai ini biasanya dimulai dari sumber *utility*, masuk ke panel utama, melewati sistem proteksi, UPS, distribusi daya, PDU, *rack PDU*, lalu akhirnya sampai ke perangkat TI.

Data Center Handbook menggambarkan aliran listrik di *data center*: daya fasilitas masuk ke *switchgear*, lalu terbagi ke jalur IT dan jalur pendukung. Jalur IT dikondisikan melalui UPS, kemudian didistribusikan melalui PDU ke perangkat TI; sedangkan jalur pendukung dipakai untuk cooling, pompa, lampu, humidifikasi, dan beban fasilitas lain. Referensi yang sama menegaskan bahwa seluruh energi listrik pada akhirnya berubah menjadi panas dan harus dibuang oleh sistem pendinginan.

Secara sederhana, alur listrik dapat dibaca seperti ini:

```
Utility / PLN
↓
Panel Tegangan Menengah / Trafo
↓
Main Low Voltage Switchboard
↓
UPS + Baterai
↓
PDU / RPP / Busway
↓
Rack PDU
↓
Server / Storage / Network / Security Device
```

Untuk layanan kritikal, alur ini biasanya digandakan menjadi jalur A dan jalur B. Tujuannya adalah menghindari *single point of failure*. Jika satu jalur terganggu, perangkat dengan dua *power supply* tetap dapat hidup dari jalur lain.

Prinsip desain arsitektur power:

- **Sumber listrik harus stabil dan terlindungi.**
- **Jalur distribusi harus jelas dan terdokumentasi.**
- **Perangkat kritikal sebaiknya memiliki dual power input.**
- **Distribusi A/B harus benar-benar terpisah secara logis dan fisik.**
- **Setiap panel harus bisa dipelihara tanpa resiko mematikan seluruh layanan.**
- **Setiap titik kritikal harus dapat diukur dan diaudit.**

Kesalahan mendasar adalah membuat diagram listrik hanya untuk memenuhi dokumen proyek, bukan sebagai alat operasi. Dalam *data center*, diagram listrik harus menjadi **peta hidup** yang dipakai teknisi saat inspeksi, maintenance, pengujian, dan insiden.

5.2 Utility Feed dan Panel Utama

Utility feed adalah pasokan listrik utama dari penyedia listrik. Pada *data center* kecil, pasokan mungkin hanya satu jalur. Pada fasilitas yang lebih kritikal, dapat digunakan dua jalur masuk, trafo berbeda, atau konfigurasi lain sesuai ketersediaan jaringan listrik dan target *availability*.

Panel utama adalah pusat distribusi dan proteksi. Di sinilah daya dibagi ke UPS, cooling, pompa, lampu, sistem keamanan, sistem monitoring, dan beban lain. Panel utama harus dirancang dengan memperhatikan arus nominal, arus hubung singkat, kapasitas pemutus, selektivitas proteksi, ruang kerja, akses maintenance, suhu ruang, dan ekspansi.

Data Center Handbook menekankan bahwa *low voltage switchboard* adalah komponen mahal dan kritikal, karena harus memiliki performa tinggi untuk keselamatan manusia, keselamatan peralatan, reliabilitas, dan ketersediaan saat maintenance. Pemilihan *circuit breaker* juga harus mempertimbangkan rating arus, kemampuan pemutusan arus hubung singkat, *derating* akibat suhu panel, dan selektivitas proteksi.

Hal yang harus diperiksa pada panel utama:

- Kapasitas arus nominal.
- Kapasitas arus hubung singkat.
- *Circuit breaker* sesuai rating.
- Selektivitas proteksi antar panel.
- Label panel dan feeder.
- Ruang kerja teknisi di depan panel.
- Ventilasi dan suhu ruang panel.
- Metering daya.
- Grounding dan bonding.
- Jalur ekspansi.
- Dokumentasi *single line diagram*.

Catatan kritis: panel utama bukan sekadar kotak pembagi listrik. Panel utama adalah **titik kendali keselamatan, proteksi, pengukuran, dan ketersediaan layanan**.

5.3 UPS: Kapasitas, Runtime, Baterai, Bypass, Modularitas

UPS, atau *Uninterruptible Power Supply*, berfungsi menjaga beban kritikal tetap hidup saat terjadi gangguan listrik. UPS melindungi dari listrik padam, tegangan turun, lonjakan, dan gangguan kualitas daya. Namun UPS bukan tujuan akhir. UPS hanya memberi waktu agar generator menyala, beban dipindahkan, atau sistem dimatikan secara terkendali.

Ada beberapa pendekatan UPS. Untuk *data center* professional, yang paling penting adalah memahami kebutuhan beban kritikal, waktu cadangan, arsitektur redundansi, kesehatan baterai, jalur *bypass*, dan prosedur pengujian. *Data Center Handbook* menjelaskan perbedaan pendekatan UPS, termasuk *standby*, *line-interactive*, dan sistem lain. Untuk beban server dan perangkat jaringan besar, kualitas bentuk gelombang, waktu transfer, dan regulasi tegangan harus diperhatikan karena desain UPS murah dapat menimbulkan masalah pada perangkat kelas data center .

Komponen penting UPS:

- Kapasitas kW/kVA.
- Faktor daya.
- Efisiensi.
- Baterai.
- *Runtime*.
- *Static bypass*.
- *Maintenance bypass*.
- Modul redundan.
- Monitoring.
- Alarm.
- Log.
- Jadwal uji.

Runtime UPS harus ditentukan berdasarkan target operasi. Umumnya, UPS tidak dirancang untuk menanggung beban berjam-jam. UPS memberi jembatan waktu sampai generator mengambil alih. Buku *Data Centers of the Future* menyebutkan bahwa pada banyak desain, baterai UPS dapat memasok daya sekitar 5–10 menit dan generator diharapkan berjalan dalam waktu kurang dari 15 detik ketika listrik gagal .

Kesalahan umum UPS:

- Menghitung UPS hanya dari beban hari pertama.
- Tidak memasukkan pertumbuhan 3–5 tahun.
- Tidak membedakan kW dan kVA.
- Tidak memperhatikan faktor daya.
- Tidak menguji baterai.
- Tidak memiliki *maintenance bypass* yang aman.
- Tidak melatih operator untuk skenario UPS alarm.
- Tidak mendokumentasikan distribusi jalur A/B.

Prinsip profesional: UPS yang tidak diuji adalah **janji kosong**.

5.4 Generator: Kapasitas, Bahan Bakar, ATS/AMF, Durasi Operasi

Generator adalah sumber daya cadangan ketika gangguan listrik berlangsung lebih lama dari kapasitas UPS. Generator harus mampu memikul beban kritis: perangkat TI, sebagian cooling, sistem keamanan, monitoring, lampu darurat, pompa penting, dan sistem fasilitas lain yang diperlukan agar layanan tetap hidup.

Generator tidak boleh dihitung hanya dari *IT load*. Harus dihitung dari **beban kritis fasilitas**. Beban cooling sangat penting karena listrik yang terus memasok server akan berubah menjadi panas. Jika cooling tidak ikut hidup, layanan mungkin tetap menyala beberapa menit tetapi kemudian mati karena suhu naik.

Komponen penting sistem generator:

- Kapasitas kW/kVA.
- Faktor daya.
- *Derating* karena suhu dan ketinggian lokasi.
- Kapasitas tangki bahan bakar.
- Durasi operasi.
- ATS/AMF.
- Panel distribusi.
- Peredam suara.
- Ventilasi.
- Sistem pembuangan gas.
- Grounding.
- Jadwal *load test*.
- Kontrak bahan bakar dan maintenance.

Dalam sistem kritis, ATS/AMF harus bekerja andal. ATS atau *Automatic Transfer Switch* memindahkan beban dari sumber utama ke generator saat terjadi gangguan. AMF atau *Automatic Mains Failure* mendeteksi kegagalan pasokan utama dan memicu generator. Namun kontrol otomatis harus tetap memiliki prosedur manual jika sistem otomatis gagal.

Energy-Efficient Computing and Data Centers memberi gambaran arsitektur lama yang umum: sumber *utility*, generator N+1, bahan bakar tipikal 48 jam, UPS, baterai 10–15 menit, PDU A/B, chiller N+1, dan jalur distribusi ke beban TI .

Catatan tajam: generator besar tanpa bahan bakar, tanpa uji beban, dan tanpa SOP transfer adalah **risiko yang disamarkan sebagai redundansi**.

5.5 PDU, RPP, dan Rack PDU

PDU, atau *Power Distribution Unit*, mendistribusikan daya dari UPS atau panel distribusi ke beban TI. RPP, atau *Remote Power Panel*, sering dipakai untuk mendekatkan distribusi daya ke area rak. *Rack PDU* berada di dalam atau dekat rak dan menjadi titik akhir distribusi daya ke perangkat.

Dalam desain profesional, PDU tidak hanya dipilih karena jumlah colokan. PDU harus dipilih berdasarkan kapasitas arus, tegangan, fase, jenis konektor, metering, kemampuan monitoring, keselamatan, dan kompatibilitas dengan desain A/B.

Data Center Handbook menjelaskan bahwa *rack PDU* memiliki klasifikasi colokan dan receptacle yang dirancang agar perangkat tidak salah colok ke tegangan atau kapasitas arus yang tidak sesuai. Dokumen tersebut juga menekankan pentingnya pengamanan kabel agar colokan tidak terlepas tanpa sengaja, karena hal kecil seperti kabel tercabut dapat menyebabkan gangguan layanan .

Jenis *rack PDU* secara fungsi:

- PDU dasar: distribusi daya tanpa monitoring detail.
- PDU metered: menampilkan konsumsi daya.
- PDU monitored: dapat dipantau jarak jauh.
- PDU switched: outlet dapat dikendalikan.
- PDU cerdas: mendukung pengukuran per outlet, alarm, dan integrasi monitoring.

Prinsip desain PDU:

- Setiap rak harus memiliki kapasitas sesuai target kW/rack.
- Jalur A dan B harus jelas.
- Jangan membebani satu sisi saja.
- Gunakan PDU yang dapat diukur untuk rak kritikal.
- Pastikan kabel tidak mudah tercabut.
- Label setiap koneksi.
- Dokumentasikan perangkat ke PDU dan PDU ke panel.

Kalimat kunci: PDU adalah titik kecil yang menentukan apakah desain power benar-benar sampai ke perangkat.

5.6 Grounding dan Bonding

Grounding adalah sistem pembumian untuk keselamatan manusia dan peralatan. *Bonding* adalah penyambungan antar bagian logam agar memiliki referensi potensial yang sama. Keduanya penting untuk mengurangi resiko sengatan listrik, gangguan peralatan, kerusakan akibat lonjakan, dan masalah kualitas daya.

Dalam *data center*, *grounding* harus mencakup panel listrik, rak, cable tray, PDU, UPS, generator, sistem proteksi petir, dan perangkat pendukung lain. Desain *grounding* tidak boleh dipisahkan dari proteksi petir dan *surge protection*.

Hal yang perlu diperiksa:

- Sistem pembumian utama.
- Koneksi bonding antar rak.
- Bonding cable tray.
- Grounding panel.
- Grounding UPS.
- Grounding generator.
- Grounding sistem proteksi petir.
- Pengukuran tahanan grounding.
- Dokumentasi titik grounding.
- Inspeksi korosi dan koneksi longgar.

Catatan kritis: grounding yang buruk sering tidak terlihat saat normal, tetapi menjadi fatal saat gangguan listrik, petir, kebocoran arus, atau insiden keselamatan.

5.7 Redundansi N, N+1, 2N

Redundansi adalah kemampuan sistem tetap berjalan ketika ada komponen gagal atau sedang dipelihara. Tetapi redundansi harus dipahami dengan benar. Menambah perangkat tidak otomatis membuat sistem andal jika jalurnya masih bertemu di satu titik gagal.

N berarti kapasitas minimum yang dibutuhkan untuk menjalankan beban. Jika butuh 3 unit UPS dan hanya ada 3 unit, maka desainnya N. Jika satu unit gagal, kapasitas tidak cukup.

N+1 berarti ada satu unit cadangan tambahan. Jika beban membutuhkan 3 unit, maka dipasang 4 unit. Saat satu unit gagal atau dipelihara, sistem masih cukup.

2N berarti ada dua sistem penuh yang masing-masing mampu menanggung seluruh beban. Jalur A mampu 100%, jalur B juga mampu 100%. Ini lebih mahal, tetapi memberikan isolasi lebih kuat jika desain benar.

Data Center Handbook membedakan beberapa level kontinuitas layanan, mulai dari tanpa redundansi, backup untuk gangguan singkat, backup untuk gangguan panjang, sampai backup penuh untuk kegagalan grid maupun distribusi internal. Referensi tersebut juga menekankan bahwa desain sering berada di antara level penuh dan sebagian, karena masih mungkin ada *single failure point* bila arsitektur tidak benar-benar terpisah .

Tabel ringkas:

Model	Arti	Kelebihan	Risiko
N	Kapasitas pas kebutuhan	Murah, sederhana	Tidak tahan kegagalan
N+1	Ada satu cadangan	Lebih andal, masih efisien	Jalur bersama bisa jadi titik gagal
2N	Dua sistem penuh	Isolasi kuat	Mahal, kompleks, butuh disiplin operasi

Uptime Institute menekankan bahwa tingkat *Tier* berbeda sesuai kebutuhan ketersediaan, dan pengukuran kemampuan fasilitas harus sesuai kebutuhan performa layanan, bukan sekadar jumlah perangkat cadangan ([Uptime Institute](#)).

Prinsip tajam: redundansi bukan jumlah alat cadangan; redundansi adalah kemampuan layanan tetap berjalan saat terjadi kegagalan nyata.

5.8 Proteksi Petir dan Surge

Proteksi petir dan *surge* penting karena data center berisi perangkat elektronik sensitif, sistem kontrol, jaringan, UPS, generator, sensor, dan perangkat keamanan. Lonjakan tegangan dapat datang dari sambaran petir, switching beban besar, gangguan utilitas, atau kesalahan distribusi internal.

Proteksi harus dirancang berlapis:

- Proteksi petir eksternal.
- Jalur down conductor.
- Sistem grounding.
- *Surge Protective Device* di panel utama.
- SPD di panel distribusi.
- Proteksi pada jalur telekomunikasi.
- Proteksi pada jalur kontrol dan sensor.
- Inspeksi berkala.

Proteksi petir tidak boleh berdiri sendiri. Ia harus terintegrasi dengan grounding dan bonding. Jika tidak, energi gangguan dapat mencari jalur lain melalui perangkat, kabel data, atau sistem kontrol.

Kesalahan umum: memasang SPD tetapi grounding buruk. Dalam kondisi ini, proteksi menjadi tidak efektif.

5.9 Testing Kelistrikan

Sistem listrik data center harus diuji sebelum operasi dan diuji berkala setelah operasi. Tujuan pengujian adalah memastikan desain benar-benar bekerja, bukan hanya terlihat benar di gambar.

Jenis pengujian penting:

- Inspeksi visual panel.
- Pengujian torsi koneksi.
- Pengujian isolasi kabel.
- Pengujian grounding.
- Pengujian UPS.
- Pengujian baterai.
- Pengujian *bypass*.
- Pengujian generator *no-load* dan *load test*.
- Pengujian ATS/AMF.
- Pengujian transfer utility → UPS → generator.
- Pengujian failover jalur A/B.
- Pengujian alarm dan monitoring.
- Pengujian *emergency power off* jika digunakan.
- Pengujian termal panel dengan infrared.

Untuk sertifikasi, hasil pengujian harus menjadi bukti. Bukan cukup mengatakan “sudah dites”. Harus ada tanggal, metode, hasil, nama pemeriksa, alat ukur, kondisi beban, temuan, tindak lanjut, dan persetujuan.

TIA-942 menyatakan standar ini mencakup infrastruktur fisik data center, termasuk lokasi, arsitektur, elektrik, mekanik, *fire safety*, telekomunikasi, keamanan, dan persyaratan lainnya ([TIA Online](#)). Karena itu, pengujian listrik harus diposisikan sebagai bagian dari kesiapan fasilitas, bukan hanya pekerjaan teknisi listrik.

Kalimat kunci: yang tidak diuji tidak layak disebut siap operasi.

5.10 Dokumentasi Single Line Diagram

Single Line Diagram atau SLD adalah peta utama sistem kelistrikan. SLD menunjukkan sumber listrik, panel, trafo, UPS, baterai, generator, ATS, PDU, breaker, jalur distribusi, dan beban. Dalam insiden, SLD membantu teknisi memahami jalur daya dengan cepat.

SLD harus selalu diperbarui. SLD lama yang tidak sesuai kondisi lapangan dapat lebih berbahaya daripada tidak punya SLD, karena teknisi mengambil keputusan berdasarkan informasi salah.

SLD minimum harus memuat:

- Sumber *utility*.
- Trafo.
- Main panel.
- UPS.
- Baterai.
- Generator.
- ATS/AMF.
- Panel distribusi.
- PDU/RPP.
- Jalur A/B.
- Rating breaker.
- Kapasitas kabel utama.
- Titik metering.
- Titik grounding utama.
- Beban kritikal.
- Nomor panel dan feeder.

Prinsip audit: SLD adalah salah satu bukti paling penting bahwa sistem listrik dapat dipahami, dioperasikan, dipelihara, dan diaudit.

Materi Praktek 1: Cara Menghitung Kapasitas UPS

Langkah Perhitungan

1. Hitung *critical IT load*.
2. Tambahkan margin pertumbuhan.
3. Tentukan faktor daya.
4. Tentukan redundansi.
5. Tentukan kapasitas modul.
6. Validasi jalur distribusi dan bypass.

Rumus Dasar

$$\text{UPS kW} = \text{Critical IT Load} \times \text{Margin}$$

Jika perlu konversi ke kVA:

$$\text{UPS kVA} = \text{UPS kW} / \text{Power Factor}$$

Contoh

- Critical IT Load = 200 kW
- Margin desain = 20%
- Faktor daya = 0,9

UPS kW desain:

$$200 \times 1,2 = \mathbf{240 \text{ kW}}$$

UPS kVA:

$$240 / 0,9 = \mathbf{266,7 \text{ kVA}}$$

Dibulatkan ke kapasitas praktis:

UPS minimum sekitar 300 kVA

Jika target N+1 modular:

- Misal modul UPS = 100 kW
- Beban desain = 240 kW
- Kebutuhan aktif = 3 modul = 300 kW
- Tambahan 1 modul cadangan = 4 modul
- Arsitektur = **300 kW aktif + 100 kW cadangan**

Catatan: pemilihan final harus memperhitungkan efisiensi UPS, faktor daya aktual, karakter beban, harmonisa, inrush, jalur bypass, dan pertumbuhan.

Materi Praktek 2: Cara Menghitung Kebutuhan Baterai

Perhitungan baterai sangat bergantung pada teknologi baterai, tegangan sistem DC, efisiensi UPS, umur baterai, suhu ruang, dan batas *depth of discharge*. Untuk buku sertifikasi, gunakan pendekatan awal sebagai estimasi konseptual, lalu tekankan bahwa desain final harus divalidasi oleh perancang listrik profesional.

Rumus Estimasi Energi

$$\text{Energi Baterai kWh} = \text{Beban kW} \times \text{Runtime jam} / \text{Efisiensi UPS}$$

Contoh

- Beban kritikal = 200 kW
- Runtime target = 10 menit = 10/60 jam = 0,167 jam
- Efisiensi UPS = 0,95

Energi baterai:

$$200 \times 0,167 / 0,95 = \mathbf{35,16 \text{ kWh}}$$

Tambahkan margin 20%:

$$35,16 \times 1,2 = \mathbf{42,19 \text{ kWh}}$$

Jadi kebutuhan energi baterai konseptual sekitar **42 kWh**.

Hal yang Wajib Diperiksa

- Runtime pada beban penuh.
- Umur baterai.
- Suhu ruang baterai.
- Jadwal penggantian.
- Pengujian kapasitas.
- Alarm baterai.
- Risiko kebakaran.
- Ventilasi ruang baterai.
- Prosedur isolasi baterai.
- Dokumentasi hasil uji.

Catatan kritis: baterai lemah adalah salah satu risiko paling sering tersembunyi. UPS terlihat normal, tetapi gagal saat benar-benar dibutuhkan.

Materi Praktek 3: Cara Menghitung Generator Berdasarkan *IT Load* dan Beban Pendukung

Generator harus dihitung dari beban kritikal fasilitas, bukan dari IT load saja.

Langkah Perhitungan

1. Tentukan IT load.
2. Tentukan beban cooling kritikal.
3. Tambahkan UPS recharge.
4. Tambahkan sistem keamanan, monitoring, lampu darurat, pompa penting.
5. Tambahkan margin.
6. Perhitungkan faktor daya, inrush, suhu, ketinggian, dan ekspansi.
7. Tentukan durasi bahan bakar.

Contoh Sesuai Soal

- IT Load = **200 kW**
- PUE target = **1,6**
- Total Facility Load = $200 \times 1,6 = \mathbf{320\ kW}$
- Margin desain = 20%

Kapasitas desain awal:

$$320 \times 1,2 = \mathbf{384\ kW}$$

Namun kapasitas trafo/genset tidak boleh berhenti di angka 384 kW. Harus diperiksa:

- Faktor daya.
- Beban motor cooling.
- Arus start / *inrush*.
- UPS recharge setelah listrik kembali.
- Ketinggian lokasi.
- Suhu lingkungan.
- Beban masa depan.
- Apakah semua cooling perlu hidup atau hanya cooling kritikal.
- Apakah generator N, N+1, atau 2N.

Jika faktor daya desain 0,8:

$$\mathbf{Generator\ kVA = 384 / 0,8 = 480\ kVA}$$

Maka kapasitas praktis awal dapat diarahkan ke **±500 kVA**, sebelum disesuaikan dengan standar perancang, katalog teknis, dan skenario ekspansi.

Durasi Bahan Bakar

Jika target operasi cadangan 24 jam, maka harus dihitung:

- Konsumsi bahan bakar per jam pada beban tertentu.
- Kapasitas tangki.
- Kontrak pengisian ulang.
- Akses mobil bahan bakar saat bencana.
- Risiko kualitas bahan bakar.
- Prosedur pengujian.

Catatan tajam: durasi generator bukan hanya ukuran tangki, tetapi **kemampuan pasokan bahan bakar saat kondisi darurat.**

Materi Praktek 4: Checklist Inspeksi Panel, UPS, PDU, dan Grounding

Area	Item Pemeriksaan	Status
Panel utama	Label panel jelas	Ya / Tidak
Panel utama	Rating breaker sesuai desain	Ya / Tidak
Panel utama	Tidak ada panas berlebih	Ya / Tidak
Panel utama	Ruang kerja teknisi cukup	Ya / Tidak
Panel utama	Metering daya berfungsi	Ya / Tidak
Panel utama	SLD tersedia dan sesuai kondisi	Ya / Tidak
UPS	Kapasitas sesuai beban	Ya / Tidak
UPS	Beban aktual tercatat	Ya / Tidak
UPS	Baterai sehat	Ya / Tidak
UPS	Bypass diuji	Ya / Tidak
UPS	Alarm dan log aktif	Ya / Tidak
UPS	Maintenance terakhir tercatat	Ya / Tidak
Generator	Start otomatis berhasil	Ya / Tidak
Generator	Load test dilakukan	Ya / Tidak
Generator	Bahan bakar cukup	Ya / Tidak
Generator	ATS/AMF diuji	Ya / Tidak
PDU	Jalur A/B jelas	Ya / Tidak
PDU	Beban per PDU seimbang	Ya / Tidak
PDU	Kabel tidak longgar	Ya / Tidak
PDU	Label outlet tersedia	Ya / Tidak
Rack PDU	Tidak overload	Ya / Tidak
Grounding	Tahanan grounding terukur	Ya / Tidak
Grounding	Bonding rak tersedia	Ya / Tidak
Grounding	Cable tray ter-bonding	Ya / Tidak
Grounding	Tidak ada koneksi korosi/longgar	Ya / Tidak
Proteksi surge	SPD tersedia dan indikator normal	Ya / Tidak
Dokumentasi	Hasil inspeksi disimpan	Ya / Tidak

Cara pakai: checklist ini digunakan saat inspeksi berkala, sebelum audit, setelah pekerjaan listrik besar, dan setelah insiden.

Ringkasan Bab 5

Bab ini menegaskan bahwa sistem listrik *data center* adalah kombinasi antara **rekayasa, keselamatan, redundansi, pengujian, dan disiplin dokumentasi**. Sistem listrik tidak boleh dirancang hanya agar “cukup menyala”. Ia harus mampu mendukung operasi kritikal, menghadapi gangguan, menjalani maintenance, dan menyediakan bukti audit.

ISO/IEC 22237-1 menjelaskan prinsip umum fasilitas dan infrastruktur data center serta klasifikasi terkait *availability*, *physical security*, dan *energy efficiency enablement* ([ISO](#)). Dalam konteks listrik, ini berarti desain harus mampu menjawab tiga pertanyaan: **apakah layanan tetap hidup, apakah sistem aman, dan apakah energi digunakan secara efisien?**

PUE juga terkait langsung dengan listrik. The Green Grid mendefinisikan PUE sebagai total energi fasilitas dibagi energi perangkat TI, sehingga kerugian konversi listrik, UPS, distribusi, cooling, dan beban pendukung akan mempengaruhi efisiensi total fasilitas ([datacenters.lbl.gov](#)).

Inti bab: sistem listrik data center harus bisa dihitung, diuji, dipelihara, dan dibuktikan.

Checklist Akhir Bab 5

Sebelum masuk Bab 6, pembaca harus mampu menjawab:

- Apakah arsitektur listrik dari *utility* sampai rack PDU sudah jelas?
- Apakah jalur A/B benar-benar terpisah?
- Apakah panel utama memiliki rating dan proteksi yang sesuai?
- Apakah kapasitas UPS sudah menghitung margin 3–5 tahun?
- Apakah baterai UPS sudah diuji?
- Apakah *runtime* UPS sesuai kebutuhan operasi?
- Apakah generator mampu menanggung IT load dan beban pendukung kritikal?
- Apakah ATS/AMF sudah diuji?
- Apakah PDU dan rack PDU tidak overload?
- Apakah grounding dan bonding sudah diukur?
- Apakah proteksi petir dan *surge* terintegrasi?
- Apakah *load test* dilakukan berkala?
- Apakah *single line diagram* sesuai kondisi aktual?
- Apakah semua hasil inspeksi dan pengujian tersimpan sebagai **bukti audit dan sertifikasi?**

Penutup bab: *Data center* professional tidak hanya membutuhkan listrik yang besar, tetapi listrik yang aman, redundan, terukur, mudah dipelihara, dan siap dibuktikan saat audit.

Bab 6. Thermal Design: Airflow, Containment, Liquid Cooling, dan ASHRAE

Golden Rule: Pendinginan data center bukan soal membuat ruangan dingin, tetapi mengantarkan udara atau cairan pendingin tepat ke beban panas yang benar.

Bab ini membahas desain termal *data center*: bagaimana panas dihasilkan, dipindahkan, dikendalikan, diukur, dan dibuang. Dalam outline buku, Bab 6 memang diarahkan untuk membahas prinsip perpindahan panas, *inlet temperature*, *outlet temperature*, *delta T*, *hot aisle*, *cold aisle*, *containment*, CRAC, CRAH, chiller, *cooling tower*, *free cooling*, *liquid cooling*, GPU, kelembaban, sensor, serta Praktek membaca *thermal map* dan menghitung kebutuhan cooling .

6.1 Prinsip Perpindahan Panas di Data Center

Setiap watt listrik yang dipakai perangkat TI hampir seluruhnya berubah menjadi panas. Artinya, jika *IT load* adalah 200 kW, maka sistem pendinginan harus mampu membuang panas sekitar 200 kW dari ruang *data center*. Jika panas tidak dibuang dengan benar, suhu perangkat naik, kipas bekerja lebih keras, konsumsi energi meningkat, performa turun, dan risiko kerusakan bertambah.

Data Center Handbook menjelaskan jalur pembuangan panas melalui infrastruktur cooling: daya dari perangkat TI dan infrastruktur pendukung berubah menjadi panas, lalu dibawa oleh ACU/CRAH, chiller, pompa, dan *cooling tower* menuju lingkungan luar . Karena itu, cooling bukan hanya “AC ruangan”. Cooling adalah **rantai perpindahan panas**.

Ada tiga prinsip dasar:

- **Panas harus ditangkap dekat sumbernya.**
- **Udara dingin tidak boleh bercampur dengan udara panas.**
- **Cooling harus diukur di titik perangkat, bukan hanya di dinding ruangan.**

Dalam *data center* tradisional, udara dingin dikirim ke depan rak. Perangkat menarik udara dingin melalui bagian depan, lalu membuang udara panas ke belakang. Jika udara panas kembali masuk ke depan rak, terjadi *recirculation*. Jika udara dingin langsung kembali ke unit pendingin tanpa melewati perangkat, terjadi *bypass air*. Keduanya adalah pemborosan.

Kalimat kunci: masalah cooling sering bukan kekurangan AC, tetapi salah mengatur jalur udara.

6.2 Inlet Temperature, Outlet Temperature, dan Delta T

Inlet temperature adalah suhu udara yang masuk ke perangkat, biasanya di bagian depan server. Ini adalah suhu yang paling penting bagi perangkat TI. *Outlet temperature* adalah suhu udara panas yang keluar dari belakang perangkat. *Delta T* adalah selisih antara *outlet temperature* dan *inlet temperature*.

Rumus sederhana:

$$\text{Delta T} = \text{Outlet Temperature} - \text{Inlet Temperature}$$

Contoh:

- *Inlet temperature* = 24°C
- *Outlet temperature* = 38°C
- **Delta T = 14°C**

Delta T memberi gambaran seberapa efektif panas diambil dari perangkat. Jika *delta T* terlalu kecil, bisa jadi airflow terlalu besar atau udara tidak menyerap panas secara efektif. Jika *delta T* terlalu besar, bisa jadi airflow kurang atau beban terlalu tinggi. Namun interpretasi harus hati-hati, karena setiap perangkat memiliki karakter kipas dan beban berbeda.

ASHRAE TC 9.9 menjadi rujukan penting untuk kondisi lingkungan perangkat TI. Referensi ASHRAE 2021 mencantumkan contoh persyaratan tipikal untuk kondisi tertentu: suhu minimum 15°C, maksimum 32°C, RH 20–80%, *dew point* maksimum 22°C, laju perubahan suhu kurang dari 5°C/jam, laju perubahan kelembaban kurang dari 5% RH per jam, dan tanpa kondensasi ([ASHRAE](#)).

Prinsip pengukuran:

- Ukur suhu di **depan rak**, bukan hanya suhu ruangan.
- Pasang sensor di bagian atas, tengah, dan bawah rak kritikal.
- Catat *inlet*, *outlet*, dan *delta T*.
- Perhatikan tren, bukan hanya angka sesaat.
- Kaitkan suhu dengan beban kW/rack.

Catatan kritis: ruangan terasa dingin tidak berarti server aman. Yang penting adalah **suhu udara yang benar-benar masuk ke perangkat**.

6.3 Hot Aisle dan Cold Aisle

Hot aisle dan *cold aisle* adalah fondasi desain airflow berbasis udara. *Cold aisle* adalah lorong di depan rak, tempat udara dingin dikirim ke perangkat. *Hot aisle* adalah lorong di belakang rak, tempat udara panas keluar dari perangkat.

Pola yang benar:

```
Cold Aisle
[Depan Rack] [Depan Rack]

[Belakang Rack] [Belakang Rack]
Hot Aisle
```

Tujuan pola ini adalah memisahkan udara dingin dan udara panas. Jika rak menghadap sembarangan, udara panas dari satu rak dapat masuk ke depan rak lain. Ini menciptakan *hot spot*.

Data Center Handbook menjelaskan bahwa pada desain yang baik, rak disusun dalam konfigurasi *hot aisle–cold aisle*. Udara dingin dikirim ke *cold aisle*, masuk ke sisi *inlet* rak, lalu keluar sebagai udara panas ke *hot aisle*.

Prinsip penting:

- Depan rak harus menghadap depan rak.
- Belakang rak harus menghadap belakang rak.
- U kosong harus ditutup dengan *blanking panel*.
- Celah kabel harus ditutup.
- Jangan menyimpan kardus atau barang di lorong.
- Jangan mencampur perangkat dengan arah airflow berbeda tanpa analisis.
- Rak densitas tinggi perlu perhatian khusus.

Kesalahan umum: menambah unit pendingin tanpa memperbaiki pola lorong. Akibatnya konsumsi energi naik, tetapi *hotspot* tetap muncul.

6.4 Containment: HAC dan CAC

Containment adalah teknik mengurung udara panas atau udara dingin agar tidak bercampur. Dua pendekatan umum adalah *Hot Aisle Containment* atau HAC dan *Cold Aisle Containment* atau CAC.

HAC mengurung lorong panas. Udara panas dari belakang rak ditangkap dan dikembalikan ke unit cooling. Keuntungannya, ruang lain tetap relatif berada pada suhu *cold aisle*. HAC juga dapat memberi suhu return air lebih tinggi ke unit pendingin, sehingga efisiensi cooling bisa meningkat.

CAC mengurung lorong dingin. Udara dingin difokuskan masuk ke depan rak. Pendekatan ini sering dipakai pada retrofit karena lebih mudah dipasang ketika ruang sudah ada. Namun CAC harus memastikan udara dingin yang masuk ke lorong cukup. Jika kurang, perangkat hanya bisa menarik udara dari ruang tertutup tersebut.

Data Center Handbook menjelaskan bahwa HAC umumnya sedikit lebih efisien dan lebih mudah diterapkan dengan berhasil, sedangkan CAC sering lebih umum pada retrofit. Dengan CAC penuh, perangkat TI hanya dapat menggunakan udara yang masuk ke lorong tersebut sehingga manajemen airflow menjadi sangat kritikal; sensor tekanan dan suhu sering diperlukan .

Referensi yang sama juga mengingatkan bahwa desain *containment* harus dikoordinasikan dengan layout kabinet dan sistem proteksi kebakaran, karena tirai atau panel yang salah dapat menjadi hambatan jalur evakuasi atau masalah keselamatan .

Perbandingan ringkas:

Aspek	HAC	CAC
Yang dikurung	Udara panas	Udara dingin
Efisiensi	Umumnya sangat baik	Baik jika airflow terkontrol
Retrofit	Kadang lebih sulit	Sering lebih mudah
Kenyamanan kerja	Ruang umum lebih dingin	Ruang umum bisa lebih panas
Risiko utama	Hot aisle sangat panas	Kekurangan udara dingin di lorong
Sensor penting	Suhu return, airflow	Suhu dan tekanan diferensial

Prinsip tajam: containment bukan aksesori; containment adalah bagian dari sistem cooling.

6.5 CRAC, CRAH, Chiller, dan Cooling Tower

CRAC atau *Computer Room Air Conditioner* biasanya memakai sistem refrigeran langsung untuk mendinginkan udara ruang data center. CRAH atau *Computer Room Air Handler* biasanya menggunakan air dingin dari chiller untuk mengambil panas dari udara. Keduanya berfungsi mengelola udara di ruang TI, tetapi pendekatan teknisnya berbeda.

Chiller menghasilkan air dingin. Air dingin ini dipompa ke CRAH atau coil pendingin. Setelah menyerap panas, air kembali ke chiller untuk didinginkan lagi. *Cooling tower* membantu membuang panas dari sistem chiller ke lingkungan luar, terutama pada sistem berpendingin air.

Energy-Efficient Computing and Data Centers menjelaskan bahwa CRAH mengekstrak udara panas dari ruang mesin dan mengirimkan udara dingin; CRAH memakai kipas, coil pendingin, dan sistem chiller untuk menghilangkan panas. Referensi ini juga mengingatkan bahwa turbulensi dan *hot spot* dapat muncul tergantung airflow dan kapasitas panas yang dihasilkan rak .

Komponen cooling utama:

- CRAC / CRAH
- Chiller
- Pump
- Cooling tower / dry cooler
- Pipa chilled water
- Valve dan sensor
- Filter
- Fan
- Control system
- Leak detection
- Monitoring suhu dan kelembapan

Catatan penting: kapasitas cooling harus dilihat dari sistem penuh, bukan hanya kapasitas unit ruangan. Chiller besar tidak berguna jika airflow di ruang salah. CRAH kuat tidak berguna jika udara dingin bocor ke jalur yang salah.

6.6 Free Cooling dan Economizer

Free cooling adalah pemanfaatan kondisi lingkungan luar untuk mengurangi kerja kompresor chiller. Istilah “free” bukan berarti tanpa biaya, tetapi berarti memanfaatkan suhu luar yang lebih rendah agar konsumsi energi cooling turun.

Economizer adalah mekanisme untuk menggunakan udara luar atau air luar yang cukup dingin untuk membantu proses pendinginan. Dalam iklim tertentu, *economizer* dapat menghemat energi secara signifikan. Namun di iklim panas-lembab, manfaatnya harus dihitung hati-hati karena kelembaban, kualitas udara, korosi, filter, dan kontrol kondensasi menjadi isu penting.

Panduan Praktek efisiensi energi data center dari DOE menjelaskan bahwa desain hemat energi mencakup sistem TI, kondisi lingkungan, manajemen airflow, cooling plant, dan sistem listrik sebagai satu kesatuan (The Department of Energy's Energy.gov). Artinya, *free cooling* tidak boleh diputuskan hanya dari suhu luar rata-rata. Harus dilihat bersama beban IT, kelembapan, kualitas udara, lokasi, jam operasi, dan risiko peralatan.

Jenis pendekatan:

- *Air-side economizer*: memakai udara luar langsung atau tidak langsung.
- *Water-side economizer*: memakai air luar / cooling tower untuk membantu chilled water.
- *Indirect evaporative cooling*: memanfaatkan evaporasi tanpa mencampur udara luar langsung ke ruang TI.
- *Dry cooler*: membuang panas ke udara luar tanpa evaporasi besar.

Catatan kritis untuk Indonesia: potensi *free cooling* perlu analisis lokal. Di daerah dataran tinggi mungkin lebih menarik. Di daerah panas-lembab, tantangannya lebih besar karena kelembapan, korosi, dan kualitas udara.

Prinsip desain: *economizer* hanya baik jika **mengurangi energi tanpa menambah risiko operasional**.

6.7 Liquid Cooling: Rear-Door Heat Exchanger, Cold Plate, Immersion Cooling

Liquid cooling menjadi semakin penting karena densitas rak naik. Beban AI, GPU, HPC, dan komputasi padat membuat pendinginan udara tradisional semakin terbatas. Air memiliki kapasitas membawa panas yang jauh lebih baik daripada udara, sehingga cairan pendingin dapat membawa panas lebih efektif dari sumbernya.

Data Center Handbook menjelaskan bahwa ketika kebutuhan daya dan panas perangkat naik, solusi *close-coupled* atau *directly coupled cooling* menjadi dibutuhkan untuk membuang panas dari komponen utama seperti CPU, memori, dan GPU. Referensi tersebut juga menyebut bahwa komputer dengan *liquid cooling* dapat ditempatkan lebih rapat, mengurangi *hot spot*, dan dalam beberapa kasus tidak lagi membutuhkan konfigurasi *hot aisle/cold aisle* seperti sistem udara penuh .

Tiga pendekatan utama:

1. **Rear-Door Heat Exchanger** atau RDHx

Pintu belakang rak diganti dengan penukar panas. Udara panas keluar dari server, melewati coil berisi cairan, lalu panas dipindahkan ke air. Pendekatan ini cocok untuk retrofit atau rak densitas tinggi tertentu.

2. **Cold Plate**

Cairan dialirkan dekat atau langsung ke komponen panas seperti CPU/GPU melalui pelat konduktif. Ini lebih efektif untuk beban AI dan HPC karena panas ditangkap dekat sumbernya.

3. **Immersion Cooling**

Perangkat dicelupkan ke cairan dielektrik. Panas dipindahkan langsung ke cairan. Pendekatan ini dapat sangat efisien, tetapi memerlukan perubahan desain rak, operasi, maintenance, garansi perangkat, dan prosedur kerja.

Energy-Efficient Computing and Data Centers membahas tren kenaikan densitas daya yang membuat *liquid cooling* semakin relevan; buku tersebut juga memuat topik *liquid-cooled racks*, *liquid-cooled servers*, *cold plates*, *immersion cooling*, *free cooling*, dan *waste heat reuse* .

Catatan penting: *liquid cooling* tidak selalu menghilangkan kebutuhan air cooling sepenuhnya. *Data Center Handbook* menyebut sistem hybrid masih dapat memerlukan air cooling untuk 10–30% beban listrik komputer, sementara cairan menyerap sekitar 70% panas .

6.8 Tantangan Rack Density Tinggi dan GPU

Rak densitas tinggi mengubah desain data center. Pada rak biasa, beban 3–6 kW/rack mungkin masih dapat dikelola dengan airflow yang baik. Namun rak GPU atau HPC dapat melampaui kemampuan pendinginan udara tradisional. Tantangannya bukan hanya kW total, tetapi **konsentrasi panas dalam ruang kecil**.

Energy-Efficient Computing and Data Centers menegaskan bahwa peningkatan daya prosesor dan akselerator menaikkan kapasitas panas per rak, membuat pendinginan server padat dengan udara menjadi semakin menantang. Buku ini juga menunjukkan bahwa water cooling memungkinkan prosesor berjalan pada suhu lebih rendah karena kapasitas panas air yang tinggi, sehingga berpotensi menurunkan daya atau meningkatkan performa .

Dampak GPU terhadap desain:

- Beban kW/rack meningkat.
- Suhu *outlet* lebih tinggi.
- Airflow per rak meningkat.
- Jalur kabel dan jaringan lebih padat.
- Berat rak meningkat.
- PDU dan breaker harus lebih besar.
- Cooling tradisional bisa tidak cukup.
- Monitoring per rak menjadi wajib.
- Liquid cooling mungkin diperlukan.

Pertanyaan desain untuk rak GPU:

- Berapa kW/rack aktual?
- Apakah airflow server front-to-back?
- Apakah rak butuh RDHx atau *cold plate*?
- Apakah lantai kuat?
- Apakah PDU mendukung arus yang dibutuhkan?
- Apakah UPS dan generator mendukung beban puncak?
- Apakah ada sensor suhu per zona?
- Apakah prosedur maintenance aman untuk cairan pendingin?

Kalimat tajam: GPU bukan hanya proyek TI; GPU adalah proyek power, cooling, space, network, dan operasi.

6.9 Kelembaban, Dew Point, Korosi, dan ESD

Kelembaban sering disalahpahami. Kelembaban terlalu rendah dapat meningkatkan risiko ESD atau *electrostatic discharge*. Kelembaban terlalu tinggi dapat meningkatkan risiko kondensasi dan korosi. Karena itu, pengendalian kelembaban harus mengikuti standar lingkungan perangkat, bukan sekadar kenyamanan manusia.

ASHRAE TC 9.9 menekankan pentingnya parameter kelembaban, *dew point*, dan tidak adanya kondensasi. Referensi ASHRAE 2021 mencantumkan contoh kondisi tipikal untuk perangkat tertentu: RH 20–80%, *dew point* maksimum 22°C, perubahan suhu kurang dari 5°C/jam, perubahan kelembaban kurang dari 5% RH per jam, dan tanpa kondensasi ([ASHRAE](#)).

Dew point penting karena kondensasi terjadi ketika permukaan lebih dingin dari titik embun. Dalam desain yang memakai chilled water atau *liquid cooling*, risiko kondensasi harus benar-benar dikendalikan. Sensor suhu dan kelembaban saja tidak cukup; perlu logika kontrol yang memahami *dew point*.

Korosi juga penting, terutama di lokasi dengan polusi, udara pantai, gas korosif, atau kualitas filtrasi buruk. Partikel dan kontaminan dapat merusak konektor, board, dan jalur listrik. ASHRAE TC 9.9 dikenal sebagai rujukan industri untuk pengetahuan lingkungan dan Praktek terbaik data center ([TPC ASHRAE](#)).

Checklist lingkungan:

- Suhu *inlet* rak.
- RH.
- *Dew point*.
- Laju perubahan suhu.
- Laju perubahan kelembaban.
- Risiko kondensasi.
- Risiko ESD.
- Kualitas filtrasi udara.
- Polusi dan korosi.
- Alarm lingkungan.

Catatan kritis: mengejar suhu terlalu dingin bisa boros energi dan menambah risiko kondensasi. Yang dibutuhkan adalah **rentang lingkungan yang aman dan stabil**.

6.10 Pengukuran Thermal dan Sensor

Pengukuran adalah dasar operasi cooling. Tanpa sensor, pengelola hanya mengandalkan rasa dingin, dan itu berbahaya. Sensor harus ditempatkan pada titik yang benar: depan rak, belakang rak, atas-tengah-bawah, lorong panas, lorong dingin, return air, supply air, chilled water supply/return, dan titik risiko kebocoran.

Sensor yang diperlukan:

- Suhu *inlet* rak.
- Suhu *outlet* rak.
- Kelembapan.
- *Dew point*.
- Tekanan diferensial.
- Airflow.
- Suhu supply/return chilled water.
- Leak detection.
- Status CRAC/CRAH.
- Status chiller.
- Status fan/pump.
- Daya per rak untuk korelasi panas.

Data Center Handbook menjelaskan bahwa pada CAC penuh, sensor tekanan diferensial sering digunakan bersama sensor suhu, karena perangkat hanya bisa memakai udara yang dikirim ke lorong tersebut. Namun sensor dapat keluar dari kalibrasi dan harus diperiksa berkala .

Pengukuran harus masuk ke dashboard operasi. Dashboard minimum:

- Suhu *inlet* tertinggi.
- Rak dengan *hot spot*.
- Beban kW per rak.
- Status cooling unit.
- Alarm kelembaban.
- Alarm kebocoran air.
- Tren PUE.
- Tren suhu 24 jam / 7 hari.
- Kapasitas cooling tersisa.

Prinsip audit: sensor tanpa kalibrasi dan tanpa tindak lanjut bukan monitoring, hanya pajangan.

Materi Praktek 1: Cara Membaca *Thermal Map*

Thermal map adalah peta suhu ruang data center. Biasanya ditampilkan dengan warna: biru untuk dingin, hijau/kuning untuk normal, merah untuk panas. Tujuannya bukan membuat gambar indah, tetapi menemukan masalah airflow.

Langkah membaca *thermal map*:

1. **Lihat suhu di depan rak**, terutama bagian atas.
Bagian atas rak sering lebih panas karena udara panas naik atau terjadi *recirculation*.
2. **Bandingkan *cold aisle* dan *hot aisle***.
Jika *cold aisle* ikut panas, berarti udara panas masuk kembali ke sisi depan perangkat.
3. **Cari pola merah di area tertentu**.
Satu titik merah bisa berarti rak padat, blanking panel hilang, celah kabel terbuka, atau airflow kurang.
4. **Bandingkan dengan data kW/rack**.
Rak panas tetapi beban rendah menunjukkan masalah airflow. Rak panas dan beban tinggi menunjukkan kebutuhan cooling khusus.
5. **Cek posisi unit cooling**.
Jangan langsung tambah cooling. Pastikan udara dingin sampai ke *inlet* perangkat.
6. **Cek jalur bypass**.
Udara dingin yang kembali ke unit cooling tanpa melewati perangkat adalah pemborosan.
7. **Cek recirculation**.
Udara panas yang masuk lagi ke depan rak adalah risiko langsung bagi perangkat.

Interpretasi cepat:

Temuan	Kemungkinan Penyebab	Tindakan
Panas di bagian atas depan rak	Recirculation	Pasang blanking panel, tutup celah
Cold aisle tidak dingin merata	Airflow tidak seimbang	Atur perforated tile / duct / fan
Hot aisle terlalu menyebar	Tidak ada containment	Pertimbangkan HAC/CAC
Rak tertentu panas	Beban tinggi / airflow buruk	Cek kW/rack, kabel, fan, containment
Ruang dingin tapi rak panas	Udara dingin tidak sampai perangkat	Perbaiki jalur airflow

Materi Praktek 2: Cara Menghitung Kebutuhan Cooling

Perhitungan awal cooling dimulai dari *IT load*. Rumus dasar:

$$\text{Cooling Capacity} \approx \text{IT Load dalam kW} \times 3.412 \text{ BTU/h}$$

Konversi ke TR:

$$\text{TR} = \text{BTU/h} / 12.000$$

Contoh 1 — IT Load 100 kW

Cooling BTU/h:

$$100 \times 3.412 = \mathbf{341.200 \text{ BTU/h}}$$

Cooling TR:

$$341.200 / 12.000 = \mathbf{28,43 \text{ TR}}$$

Tambahkan margin 20%:

$$28,43 \times 1,2 = \mathbf{34,1 \text{ TR}}$$

Contoh 2 — IT Load 200 kW

Cooling BTU/h:

$$200 \times 3.412 = \mathbf{682.400 \text{ BTU/h}}$$

Cooling TR:

$$682.400 / 12.000 = \mathbf{56,87 \text{ TR}}$$

Tambahkan margin 20%:

$$56,87 \times 1,2 = \mathbf{68,24 \text{ TR}}$$

Contoh 3 — IT Load 30 Rack @ 6 kW/Rack

IT Load:

$$30 \times 6 = \mathbf{180 \text{ kW}}$$

Cooling BTU/h:

$$180 \times 3.412 = \mathbf{614.160 \text{ BTU/h}}$$

Cooling TR:

$$614.160 / 12.000 = \mathbf{51,18 \text{ TR}}$$

Dengan margin 20%:

$$51,18 \times 1,2 = \mathbf{61,4 \text{ TR}}$$

Catatan penting: angka TR tidak menjamin perangkat aman. Cooling harus sampai ke *inlet* rak. Jadi setelah menghitung TR, wajib memeriksa layout, airflow, containment, sensor, dan *rack density*.

Materi Praktek 3: Checklist *Airflow*

Area	Pertanyaan Pemeriksaan	Status
Layout rak	Apakah depan rak menghadap depan rak?	Ya / Tidak
Layout rak	Apakah belakang rak membentuk hot aisle?	Ya / Tidak
Blanking panel	Apakah semua U kosong tertutup?	Ya / Tidak
Celah kabel	Apakah lubang kabel ditutup?	Ya / Tidak
Bypass air	Apakah udara dingin bocor tanpa melewati perangkat?	Ya / Tidak
Recirculation	Apakah udara panas masuk ke depan rak?	Ya / Tidak
Rack density	Apakah kW/rack diketahui?	Ya / Tidak
Sensor	Apakah sensor ada di inlet rak?	Ya / Tidak
Containment	Apakah HAC/CAC diperlukan?	Ya / Tidak
Filter	Apakah filter cooling bersih?	Ya / Tidak
CRAC/CRAH	Apakah unit bekerja normal?	Ya / Tidak
Chilled water	Apakah supply/return temperature normal?	Ya / Tidak
Kebocoran air	Apakah leak detection tersedia?	Ya / Tidak
Kelembapan	Apakah RH dan dew point dipantau?	Ya / Tidak
Hot spot	Apakah ada rak dengan suhu abnormal?	Ya / Tidak
Dokumentasi	Apakah hasil inspeksi disimpan?	Ya / Tidak

Cara pakai: checklist ini digunakan saat audit internal, setelah penambahan rak, setelah perubahan kabel besar, setelah alarm suhu, dan sebelum sertifikasi.

Materi Praktek 4: Studi Kasus — Rak Panas karena Airflow Salah, Bukan karena AC Kurang

Situasi

Sebuah data center memiliki 20 rak. Suhu ruangan terasa dingin, sekitar 21°C. Namun beberapa server di rak bagian tengah sering memberi alarm suhu tinggi. Tim operasi awalnya menyimpulkan bahwa kapasitas AC kurang dan mengusulkan penambahan unit cooling.

Temuan Lapangan

Setelah dilakukan inspeksi:

- Suhu depan rak bagian bawah normal.
- Suhu depan rak bagian atas mencapai 31–34°C.
- Banyak U kosong tidak memakai *blanking panel*.
- Lubang kabel di bawah rak terbuka.
- Kabel belakang rak menumpuk dan menghalangi airflow.
- Beberapa rak tidak mengikuti arah *hot aisle/cold aisle*.
- Udara dingin banyak bocor ke area yang tidak melewati perangkat.
- Udara panas dari belakang rak masuk kembali ke depan rak.

Analisis

Masalah utama bukan kapasitas AC. Masalah utama adalah **pemisahan udara dingin dan panas gagal**. Udara dingin tidak diarahkan tepat ke *inlet* server, sementara udara panas berputar kembali ke depan rak.

Ini sesuai dengan prinsip efisiensi airflow: panduan DOE/LBNL menyebutkan bahwa manajemen udara data center bertujuan meminimalkan atau menghilangkan pencampuran udara dingin yang dipasok ke perangkat dan udara panas yang keluar dari perangkat. Implementasi air management yang efektif meminimalkan bypass udara dingin dan recirculation udara panas ([WBDG](#)).

Tindakan Korektif

1. Pasang *blanking panel* pada semua U kosong.
2. Tutup lubang kabel dengan brush grommet.
3. Rapihan kabel belakang rak.
4. Kembalikan orientasi rak ke pola *hot aisle/cold aisle*.
5. Pindahkan perangkat panas ke rak yang memiliki airflow lebih baik.
6. Pasang sensor suhu di depan rak bagian atas, tengah, dan bawah.
7. Buat *thermal map* sebelum dan sesudah perbaikan.
8. Evaluasi kebutuhan *containment*.

Hasil yang Diharapkan

- Suhu *inlet* rak turun.
- Alarm suhu berkurang.
- Fan server tidak bekerja berlebihan.
- Konsumsi energi cooling lebih terkendali.
- Penambahan AC dapat ditunda atau dikurangi.
- Bukti perbaikan tersedia untuk audit.

Pelajaran utama: jangan membeli cooling baru sebelum memperbaiki airflow.

Ringkasan Bab 6

Bab ini menegaskan bahwa cooling data center adalah ilmu mengelola panas, bukan sekadar membuat ruangan dingin. Yang harus dijaga adalah suhu udara atau cairan pendingin yang benar-benar mencapai perangkat.

Data Center Handbook menekankan bahwa desain modern dengan air cooling sebaiknya memakai bentuk *air containment* untuk memaksimalkan efektivitas cooling dan efisiensi energi. Sementara itu, *Energy-Efficient Computing and Data Centers* menunjukkan bahwa tren prosesor dan akselerator meningkatkan konsumsi daya dan panas, sehingga air cooling, water cooling, *free cooling*, dan *waste heat reuse* menjadi bagian penting dari desain masa depan.

ASHRAE TC 9.9 menjadi rujukan penting untuk batas lingkungan perangkat, termasuk suhu, kelembaban, *dew point*, dan stabilitas kondisi operasi. Namun angka standar tidak boleh dibaca kaku tanpa memahami perangkat, lokasi, densitas rak, risiko kondensasi, dan strategi operasi.

Inti bab: thermal design yang baik menggabungkan perhitungan panas, layout rak, airflow, containment, sensor, standar lingkungan, dan disiplin operasi.

Checklist Akhir Bab 6

Sebelum masuk Bab 7, pembaca harus mampu menjawab:

- Berapa total *IT load* yang berubah menjadi panas?
- Berapa kebutuhan cooling dalam BTU/h dan TR?
- Apakah suhu diukur di *inlet* rak?
- Apakah *delta T* dipantau?
- Apakah layout sudah membentuk *hot aisle* dan *cold aisle*?
- Apakah ada *bypass air*?
- Apakah ada *recirculation* udara panas?
- Apakah *blanking panel* sudah lengkap?
- Apakah celah kabel sudah ditutup?
- Apakah HAC atau CAC diperlukan?
- Apakah CRAC/CRAH, chiller, dan *cooling tower* dipantau?
- Apakah *free cooling* atau *economizer* layak untuk lokasi ini?
- Apakah beban GPU atau rack density tinggi membutuhkan *liquid cooling*?
- Apakah RH, *dew point*, ESD, korosi, dan kondensasi dipantau?
- Apakah sensor dikalibrasi berkala?
- Apakah hasil *thermal map* dan tindakan koreksi disimpan sebagai **bukti audit dan sertifikasi**?

Penutup bab: *Data center* professional tidak hanya dingin; ia mengalirkan panas secara benar, mengukur risiko termal secara disiplin, dan membuktikan bahwa setiap perangkat menerima kondisi operasi yang aman.

Bab 7. Environmentally Friendly Data Center: PUE, Energi, Air, Karbon

Alokasi: 10 halaman | Komposisi: 60% teori, 40% Praktek

Golden Rule: Data center hijau bukan hanya PUE rendah, tetapi efisiensi energi, pengurangan karbon, efisiensi air, pemanfaatan panas, dan operasi berkelanjutan.

Bab ini membahas *data center* dari sisi keberlanjutan. Dalam outline buku, Bab 7 diarahkan untuk membahas konsep *green data center*, PUE, DCiE, WUE, CUE, ERE, efisiensi IT, efisiensi cooling, energi terbarukan, pengelolaan air, *waste heat reuse*, *carbon-aware operation*, audit energi, dan roadmap efisiensi energi .

Inti bab ini: **efisiensi bukan kosmetik lingkungan. Efisiensi adalah strategi biaya, kapasitas, reputasi, dan kesiapan sertifikasi.**

7.1 Konsep *Green Data Center*

Green data center adalah fasilitas yang dirancang, dibangun, dan dioperasikan untuk menekan konsumsi energi, mengurangi emisi karbon, mengelola air secara bertanggung jawab, meminimalkan limbah, dan tetap menjaga *availability*. Fokusnya bukan hanya menghemat listrik, tetapi membangun fasilitas yang **andal, efisien, aman, dan berkelanjutan**.

Kesalahan umum adalah menyamakan *green data center* dengan PUE rendah. PUE memang penting, tetapi belum cukup. Data center bisa memiliki PUE baik, tetapi tetap memakai energi berkarbon tinggi, boros air, membuang panas tanpa manfaat, dan tidak memiliki program daur ulang perangkat. Karena itu, pendekatan profesional harus melihat energi, air, karbon, material, operasi, dan siklus hidup fasilitas.

ISO/IEC 22237-1 memasukkan *energy efficiency enablement* sebagai salah satu klasifikasi penting dalam fasilitas data center, bersama aspek *availability* dan *physical security*. Ini menunjukkan bahwa efisiensi energi bukan tambahan, tetapi bagian dari desain dan operasi fasilitas data center modern. ([ISO](#))

Buku *Data Centers of the Future* menekankan bahwa desain data center masa depan harus menjawab realitas pemanasan global melalui inovasi perangkat keras, perangkat lunak, bahan bakar alternatif, pembangkitan energi di lokasi, teknologi cooling baru, dan alat manajemen yang lebih baik .

Prinsip utama *green data center*:

- **Efisiensi energi:** mengurangi energi terbuang.
- **Efisiensi cooling:** menghindari pendinginan berlebihan.
- **Efisiensi IT:** menjalankan beban kerja dengan perangkat yang tepat.
- **Efisiensi air:** mengurangi konsumsi air langsung dan tidak langsung.
- **Pengurangan karbon:** memahami sumber energi dan emisi.
- **Pemanfaatan panas:** menggunakan panas buangan bila memungkinkan.
- **Operasi berbasis data:** keputusan diambil dari pengukuran, bukan asumsi.

Kalimat kunci: data center hijau bukan fasilitas yang sekadar dingin dan hemat listrik, tetapi fasilitas yang sadar energi, sadar air, sadar karbon, dan sadar siklus hidup.

7.2 PUE, DCiE, WUE, CUE, ERE

PUE, atau *Power Usage Effectiveness*, adalah metrik paling populer untuk mengukur efisiensi energi infrastruktur data center. Rumusnya:

$$\text{PUE} = \text{Total Energi Fasilitas} / \text{Energi Perangkat IT}$$

Jika total energi fasilitas 1.600 kWh dan energi perangkat IT 1.000 kWh, maka:

$$\text{PUE} = 1.600 / 1.000 = 1,6$$

Semakin dekat PUE ke 1,0, semakin kecil energi non-IT yang dipakai untuk cooling, UPS losses, distribusi listrik, lampu, dan sistem pendukung lain. The Green Grid memperkenalkan PUE dan kebalikannya, DCiE, sebagai metrik efisiensi energi data center untuk membantu pengelola memahami konsumsi energi fasilitas dibanding energi IT. (datacenters.lbl.gov)

DCiE, atau *Data Center Infrastructure Efficiency*, adalah kebalikan dari PUE:

$$\text{DCiE} = \text{Energi IT} / \text{Total Energi Fasilitas} \times 100\%$$

Jika PUE = 1,6, maka:

$$\text{DCiE} = 1 / 1,6 \times 100\% = 62,5\%$$

WUE, atau *Water Usage Effectiveness*, mengukur penggunaan air terhadap energi IT. The Green Grid menjelaskan WUE sebagai bagian dari keluarga metrik xUE bersama PUE dan CUE untuk membantu komunitas data center mengelola aspek energi dan keberlanjutan. (thegreengrid.org)

Rumus sederhana:

$$\text{WUE} = \text{Penggunaan Air Tahunan} / \text{Energi IT Tahunan}$$

CUE, atau *Carbon Usage Effectiveness*, mengukur emisi karbon terhadap energi IT. *Data Center Handbook* menjelaskan bahwa CUE menggambarkan jumlah karbon yang dikeluarkan dibanding energi IT tahunan, dan pengelola didorong menurunkan pembilang agar CUE semakin kecil .

ERE, atau *Energy Reuse Effectiveness*, mengukur manfaat pemanfaatan ulang energi. *Data Center Handbook* menjelaskan ERE sebagai metrik yang mengakui bahwa sebagian data center dapat menyediakan energi berguna untuk kebutuhan lain, misalnya panas buangan untuk memanaskan gedung sekitar atau air domestik .

Ringkasan metrik:

Metrik	Fokus	Rumus Sederhana	Makna
PUE	Efisiensi energi fasilitas	Total energi fasilitas / energi IT	Semakin rendah semakin baik
DCiE	Efisiensi infrastruktur	Energi IT / total energi fasilitas	Semakin tinggi semakin baik
WUE	Efisiensi air	Air tahunan / energi IT tahunan	Semakin rendah semakin baik
CUE	Intensitas karbon	Emisi karbon / energi IT tahunan	Semakin rendah semakin baik
ERE	Pemanfaatan ulang energi	Memperhitungkan energi yang digunakan ulang	Semakin rendah semakin baik

Catatan kritis: PUE tidak boleh dibaca sendirian. Data center dengan PUE rendah tetapi memakai energi berkarbon tinggi belum tentu lebih berkelanjutan dibanding fasilitas dengan PUE sedikit lebih tinggi tetapi memakai energi rendah karbon dan air lebih sedikit.

7.3 Efisiensi IT: Konsolidasi Server, Virtualisasi, Right-Sizing

Efisiensi data center tidak dimulai dari cooling. Efisiensi dimulai dari **beban IT**. Jika perangkat IT boros, tidak terpakai, atau terlalu besar dari kebutuhan, maka seluruh fasilitas ikut boros: listrik naik, panas naik, cooling naik, UPS naik, generator naik, dan biaya operasi naik.

Konsolidasi server bertujuan mengurangi jumlah perangkat fisik dengan menggabungkan beberapa beban kerja ke perangkat yang lebih efisien. Namun konsolidasi harus dilakukan hati-hati agar tidak membuat satu perangkat menjadi titik gagal besar. Konsolidasi harus disertai desain redundansi, backup, monitoring, dan kapasitas yang benar.

Virtualisasi membantu memaksimalkan penggunaan perangkat fisik. Beban kerja dapat dipindahkan, diperbesar, diperkecil, atau dimatikan sesuai kebutuhan. Dalam konteks profesional, virtualisasi bukan hanya teknologi, tetapi **alat manajemen kapasitas dan energi**.

Right-sizing berarti memilih kapasitas komputasi, memori, storage, dan jaringan sesuai kebutuhan nyata. Perangkat yang terlalu kecil mengganggu performa. Perangkat yang terlalu besar memboroskan energi dan ruang. *Data Center Handbook* menekankan bahwa metrik efisiensi paling berguna adalah metrik yang menghasilkan data bermakna untuk memperbaiki penggunaan energi fasilitas, bukan sekadar angka yang terlihat bagus .

Langkah efisiensi IT:

- Identifikasi *server* tidak terpakai.
- Cari beban kerja yang utilitasnya rendah.
- Konsolidasikan aplikasi ringan.
- Gunakan perangkat yang lebih efisien per watt.
- Pisahkan beban kritis dan non-kritis.
- Matikan perangkat yang tidak dibutuhkan.
- Evaluasi utilisasi CPU, memori, storage, dan jaringan.
- Hitung dampak energi sebelum membeli perangkat baru.

Kalimat tajam: server kosong tetap makan listrik, menghasilkan panas, memakai cooling, menghabiskan port, dan memenuhi rak.

7.4 Efisiensi Cooling

Cooling sering menjadi penyumbang besar konsumsi energi non-IT. Efisiensi cooling tidak berarti menaikkan suhu sembarangan. Efisiensi cooling berarti mengirim pendinginan tepat ke beban panas, menghindari pencampuran udara panas-dingin, mengurangi *bypass air*, mencegah *recirculation*, dan memakai teknologi cooling sesuai densitas rak.

ASHRAE TC 9.9 menjadi rujukan penting untuk desain dan operasi ruang teknologi, termasuk cooling, energi, kelembaban, dan penggunaan energi yang efisien. ([TPC ASHRAE](#)) ASHRAE juga mengingatkan bahwa kenaikan temperatur operasi dapat mempengaruhi reliabilitas peralatan, termasuk perangkat listrik yang berbagi ruang atau aliran udara dengan perangkat IT. ([ASHRAE](#))

Efisiensi cooling dapat dilakukan melalui:

- Layout *hot aisle* dan *cold aisle* yang benar.
- *Blanking panel* pada U kosong.
- Penutupan celah kabel.
- HAC atau CAC.
- Sensor suhu di *inlet* rak.
- Kontrol fan berbasis kebutuhan.
- Peningkatan temperatur set point secara terukur.
- *Free cooling* atau *economizer* bila lokasi mendukung.
- *Liquid cooling* untuk rak densitas tinggi.
- Pemeliharaan filter, coil, fan, pump, dan chiller.

Brochard dkk. menjelaskan bahwa *free cooling* terjadi ketika chiller tidak diperlukan untuk menghasilkan air dingin dan cooling tower atau dry cooler dapat digunakan sebagai pengganti; pemanfaatannya sangat bergantung pada kondisi lingkungan luar, terutama temperatur. Menaikkan temperatur ruang dan temperatur air dapat meningkatkan peluang *free cooling* serta menurunkan PUE dan TCO .

Prinsip praktis: sebelum membeli cooling baru, lakukan tiga hal: **rapikan airflow, ukur suhu di inlet rak, dan hitung kW/rack.**

7.5 Energi Terbarukan dan Renewable Matching

Energi terbarukan penting untuk menurunkan emisi karbon. Namun membeli energi terbarukan tidak otomatis membuat operasi data center hijau. Pengelola harus memahami kapan energi dipakai, dari mana energi berasal, dan apakah pasokannya sesuai dengan beban operasi.

Renewable matching adalah upaya mencocokkan konsumsi energi data center dengan pasokan energi terbarukan, baik secara tahunan, bulanan, harian, atau semakin ideal secara jam-ke-jam. Semakin rinci pencocokannya, semakin kuat klaim keberlanjutannya, tetapi semakin kompleks pengelolaannya.

Buku *Data Centers of the Future* menjelaskan bahwa lokasi ideal data center memiliki akses ke tenaga angin, surya, dan air, tetapi realitanya data center sering harus berada dekat populasi, konektivitas, atau pelanggan; ini membatasi pilihan energi dan air. Dokumen tersebut juga menekankan bahwa tidak ada dua data center yang benar-benar sama karena lokasi, model tenancy, usia fasilitas, ketersediaan air, energi, dan kebutuhan pelanggan berbeda .

Strategi energi terbarukan:

- Membeli listrik rendah karbon dari penyedia energi.
- Menggunakan kontrak energi terbarukan.
- Memasang pembangkit di lokasi bila layak.
- Menggunakan sistem penyimpanan energi.
- Mengatur beban kerja sesuai ketersediaan energi rendah karbon.
- Memilih lokasi dengan pasokan energi lebih bersih.
- Mengurangi konsumsi terlebih dahulu sebelum membeli energi.

Catatan kritis: energi terbarukan tidak boleh menjadi alasan untuk boros. **Energi paling hijau adalah energi yang tidak perlu dipakai.**

7.6 Pengelolaan Air

Air sering terlupakan dalam diskusi data center. Padahal, banyak sistem cooling memakai air, baik secara langsung maupun tidak langsung. Di lokasi yang airnya terbatas, penggunaan air dapat menjadi isu lingkungan, sosial, dan perizinan.

WUE membantu menghitung penggunaan air per energi IT. *Data Center Handbook* menjelaskan bahwa penurunan penggunaan air di fasilitas bisa saja meningkatkan penggunaan energi jika sistem cooling diganti ke DX air-cooled yang kurang efisien; karena itu, pengelolaan air harus dilihat bersama energi dan sumber air regional, bukan terpisah .

Aspek pengelolaan air:

- Berapa konsumsi air tahunan?
- Air dipakai untuk cooling atau kebutuhan lain?
- Apakah air berasal dari sumber lokal yang sensitif?
- Apakah kualitas air mempengaruhi perawatan cooling?
- Apakah blowdown cooling tower dikelola?
- Apakah ada daur ulang air?
- Apakah ada resiko kebocoran?
- Apakah WUE dilaporkan?
- Apakah pengurangan air justru menaikkan energi?

Prinsip desain: jangan mengejar PUE rendah dengan mengorbankan air secara tidak terkendali. **Efisiensi energi dan efisiensi air harus diseimbangkan.**

7.7 Waste Heat Reuse

Hampir semua listrik yang masuk ke perangkat IT berubah menjadi panas. Biasanya panas ini dibuang ke lingkungan. Pada pendekatan *waste heat reuse*, panas buangan dimanfaatkan kembali untuk kebutuhan lain: pemanas gedung, pemanas air, proses industri ringan, rumah kaca, kolam, atau jaringan pemanas kawasan bila tersedia.

Brochard dkk. menjelaskan bahwa cara paling sederhana memakai panas buangan adalah untuk pemanasan. Namun ada dua tantangan besar: sulitnya memindahkan panas jarak jauh dan kebutuhan temperatur panas yang cukup tinggi. Karena itu, target pemanfaatan panas sebaiknya dekat dengan data center, dan operasi pada temperatur lebih tinggi atau memakai water cooling dapat membantu meningkatkan nilai panas buangan .

Energy-Efficient Computing and Data Centers juga membahas kasus pemanfaatan ulang panas, termasuk data center yang menggunakan *free-air cooling* dan memanfaatkan panas di bagian gedung lain; pada salah satu contoh, PUE tahunan rata-rata 1,16 dicapai dibanding PUE 2,28 pada data center lama .

Contoh pemanfaatan panas:

- Pemanas kantor.
- Pemanas air domestik.
- Pemanas gedung sekitar.
- Proses pengeringan.
- Pertanian rumah kaca.
- Adsorption chiller untuk menghasilkan air dingin.
- Sistem kawasan jika tersedia.

Syarat sukses:

- Ada penerima panas yang dekat.
- Temperatur panas cukup berguna.
- Ada kebutuhan panas yang stabil.
- Ada perhitungan ekonomi.
- Ada metering energi.
- Ada kontrol risiko.
- Ada kontrak operasi.

Kalimat tajam: panas buangan adalah kerugian jika dibuang, tetapi dapat menjadi aset jika dirancang sejak awal.

7.8 Carbon-Aware Operation

Carbon-aware operation adalah pendekatan menjalankan beban kerja dengan mempertimbangkan intensitas karbon listrik. Jika suatu waktu atau lokasi memiliki pasokan listrik lebih rendah karbon, beban kerja yang fleksibel dapat dijadwalkan atau dipindahkan ke waktu/lokasi tersebut.

Tidak semua beban kerja bisa fleksibel. Sistem transaksi, layanan real-time, dan sistem kritikal harus berjalan sesuai SLA. Namun banyak beban kerja dapat dijadwalkan: *batch processing*, analitik, pelatihan model AI, indexing, backup non-kritikal, rendering, simulasi, dan proses laporan.

Buku *Data Centers of the Future* menjelaskan bahwa beban kerja dapat dipindahkan dari data center dengan karbon tinggi ke data center yang ditenagai sumber terbarukan, sehingga sebagian rak dapat dikurangi dayanya atau dipakai lebih efisien .

Langkah awal *carbon-aware operation*:

- Kelompokkan beban kritikal dan fleksibel.
- Ukur konsumsi energi per beban kerja.
- Pantau intensitas karbon listrik.
- Jadwalkan pekerjaan non-kritikal pada jam rendah karbon.
- Gunakan otomasi untuk menyesuaikan beban.
- Laporkan penghematan energi dan karbon.
- Pastikan tidak melanggar SLA.

Prinsip: *carbon-aware operation* bukan menurunkan layanan, tetapi **menjalankan beban fleksibel pada waktu dan tempat yang lebih bersih.**

7.9 Audit Energi Data Center

Audit energi adalah proses memeriksa bagaimana energi masuk, digunakan, hilang, dan dapat dihemat. Audit energi harus berbasis data. Jangan hanya melihat tagihan listrik total. Data center perlu memisahkan energi IT, cooling, UPS losses, distribusi, lampu, keamanan, monitoring, dan beban pendukung.

Panduan Praktek efisiensi energi data center dari DOE menekankan bahwa desain dan operasi hemat energi mencakup sistem IT, kondisi lingkungan, manajemen airflow, cooling plant, dan sistem listrik sebagai satu kesatuan. (datacenters.lbl.gov)

Komponen audit energi:

- Data tagihan listrik.
- Meter energi utama.
- Meter energi IT.
- Meter UPS.
- Meter cooling.
- Data suhu dan kelembaban.
- Data kW/rack.
- Data utilisasi server.
- Data PUE bulanan.
- Data WUE dan CUE jika tersedia.
- Kondisi airflow.
- Jadwal maintenance.
- Daftar perangkat tidak terpakai.
- Program perbaikan.

Energy-Efficient Computing and Data Centers menekankan pentingnya pengumpulan data sensor yang menyeluruh untuk evaluasi efisiensi, termasuk data dari perangkat IT, infrastruktur bangunan, smart meter, sensor, dan metrik performa aplikasi .

Pertanyaan audit energi:

- Energi terbesar dipakai di mana?
- Apakah IT load meningkat sebanding dengan energi fasilitas?
- Apakah cooling bekerja berlebihan?
- Apakah ada *server* menganggur?
- Apakah PUE dihitung konsisten?
- Apakah WUE dan CUE mulai diukur?
- Apakah ada target penghematan?
- Apakah hasil audit menjadi program kerja?

Kalimat kunci: audit energi yang baik tidak berhenti pada laporan, tetapi menghasilkan tindakan.

7.10 Membuat Roadmap Efisiensi Energi

Roadmap efisiensi energi adalah rencana bertahap untuk menurunkan konsumsi energi, air, dan karbon tanpa mengorbankan *availability*. Roadmap harus realistis. Jangan langsung melompat ke teknologi mahal bila masalah dasar seperti airflow, sensor, dan perangkat tidak terpakai belum dibereskan.

Tahapan roadmap:

Tahap 1 — Baseline

Ukur PUE, energi IT, energi fasilitas, tagihan listrik, suhu, kelembaban, kW/rack, dan kondisi airflow.

Tahap 2 — Quick Wins

Pasang *blanking panel*, tutup celah kabel, rapikan airflow, matikan perangkat tidak terpakai, perbaiki set point cooling secara bertahap.

Tahap 3 — Optimasi Sistem

Gunakan monitoring yang lebih rinci, evaluasi UPS, fan, pump, chiller, containment, dan kontrol cooling.

Tahap 4 — Transformasi Energi

Evaluasi energi terbarukan, *renewable matching*, penyimpanan energi, dan kontrak energi lebih bersih.

Tahap 5 — Circular & Net-Zero Direction

Mulai program *waste heat reuse*, pengurangan karbon, pengelolaan air, daur ulang perangkat, dan desain rendah karbon untuk ekspansi berikutnya.

Buku *Data Centers of the Future* menekankan bahwa data center masa depan harus berada di jalan menuju *net zero*, bukan menunggu teknologi sempurna. Komitmen harus dimulai sekarang melalui desain dan operasi yang optimal, sambil memanfaatkan teknologi baru saat tersedia .

Prinsip roadmap: ukur dahulu, perbaiki dasar, optimalkan sistem, lalu transformasikan energi dan karbon.

Materi Praktek 1: Cara Menghitung PUE Bulanan

Data yang Dibutuhkan

- Total energi fasilitas bulanan, dalam kWh.
- Energi perangkat IT bulanan, dalam kWh.
- Periode pengukuran yang sama.
- Lokasi meter yang jelas.
- Catatan perubahan besar selama bulan tersebut.

Rumus

$$\text{PUE Bulanan} = \text{Total Energi Fasilitas Bulanan} / \text{Energi IT Bulanan}$$

Contoh

- Total energi fasilitas bulan Januari = 240.000 kWh
- Energi IT bulan Januari = 150.000 kWh

$$\text{PUE Januari} = 240.000 / 150.000 = 1,6$$

Tabel PUE Bulanan

Bulan	Energi Fasilitas	Energi IT	PUE	Catatan
Januari	240.000 kWh	150.000 kWh	1,60	Normal
Februari	230.000 kWh	150.000 kWh	1,53	Cooling lebih efisien
Maret	255.000 kWh	152.000 kWh	1,68	Suhu luar naik
April	260.000 kWh	160.000 kWh	1,63	Beban IT naik

Cara Membaca

- PUE naik belum tentu buruk jika IT load berubah.
- PUE turun belum tentu baik jika ada beban IT pindah keluar.
- PUE harus dibaca bersama suhu luar, beban IT, kondisi cooling, dan perubahan operasi.
- PUE sebaiknya dilaporkan bersama biaya energi, bukan berdiri sendiri.

Catatan audit: simpan data meter, metode perhitungan, tanggal pembacaan, dan catatan perubahan fasilitas.

Materi Praktek 2: Cara Membaca Tagihan Listrik Data Center

Tagihan listrik bukan hanya angka biaya. Tagihan listrik adalah sumber informasi untuk melihat pola konsumsi, beban puncak, faktor daya, penalti, dan potensi efisiensi.

Item yang Harus Dibaca

Item	Makna	Pertanyaan Kritis
kWh	Energi terpakai	Apakah naik karena IT load atau pemborosan?
kW peak	Beban puncak	Apakah ada lonjakan tidak wajar?
Faktor daya	Efisiensi penggunaan daya	Apakah ada penalti?
Tarif	Biaya per kWh	Apakah ada jam mahal/murah?
Biaya tetap	Komponen biaya tetap	Apakah kapasitas kontrak terlalu besar?
Penalti	Biaya akibat faktor daya/kelebihan	Apa akar masalahnya?
Pajak dan biaya lain	Komponen tambahan	Perlu dipisah dalam analisis biaya

Contoh Analisis Sederhana

- Energi bulan ini naik 10%.
- IT load hanya naik 3%.
- Suhu luar relatif sama.
- Tidak ada penambahan rak besar.

Kemungkinan masalah:

- Cooling boros.
- Sensor rusak.
- Set point berubah.
- Filter kotor.
- Ada *bypass air*.
- UPS atau PDU losses naik.
- Perangkat tidak terpakai tetap menyala.

Prinsip: tagihan listrik harus dibaca bersama data PUE, IT load, cooling, dan suhu lingkungan.

Materi Praktek 3: Template Audit Energi Sederhana

Area Audit	Data yang Dikumpulkan	Temuan	Rekomendasi	Prioritas
Energi total	kWh bulanan			Tinggi/Sedang/Rendah
Energi IT	kWh IT			
PUE	PUE bulanan			
Cooling	kWh cooling / status unit			
Airflow	Thermal map / inspeksi			
Rack density	kW/rack			
Server idle	Daftar perangkat rendah utilisasi			
UPS	Beban, efisiensi, alarm			
PDU	Beban per rak			
WUE	Air tahunan / energi IT			
CUE	Emisi / energi IT			
Maintenance	Jadwal dan log			
Dokumentasi	Meter, foto, laporan			

Output Minimum Audit

- Baseline PUE.
- Baseline biaya energi.
- Daftar pemborosan.
- Daftar *quick wins*.
- Daftar investasi jangka menengah.
- Estimasi penghematan.
- Risiko terhadap *availability*.
- Rencana aksi 3, 6, dan 12 bulan.

Catatan: audit energi tidak boleh mengorbankan keandalan. Setiap penghematan harus diuji terhadap risiko layanan.

Materi Praktek 4: Contoh Program Penurunan PUE dari 2,0 ke 1,6

Kondisi Awal

- IT Load = 200 kW
- PUE awal = 2,0
- Total Facility Power = $200 \times 2,0 = 400 \text{ kW}$
- Target PUE = 1,6
- Total Facility Power target = $200 \times 1,6 = 320 \text{ kW}$
- Potensi pengurangan daya = **80 kW**

Jika tarif listrik Rp1.500/kWh:

$$\text{Penghematan tahunan} = 80 \times 24 \times 365 \times 1.500 = \text{Rp1.051.200.000}$$

Tahap 1 — 0 sampai 3 Bulan: Perbaikan Dasar

- Pasang *blanking panel*.
- Tutup celah kabel.
- Rapikan kabel belakang rak.
- Validasi *hot aisle* dan *cold aisle*.
- Pasang sensor *inlet* rak.
- Matikan perangkat tidak terpakai.
- Buat baseline PUE bulanan.

Target PUE: 2,0 → 1,85

Tahap 2 — 3 sampai 6 Bulan: Optimasi Cooling

- Evaluasi set point cooling.
- Bersihkan filter dan coil.
- Atur airflow.
- Evaluasi HAC/CAC.
- Cek *bypass air* dan *recirculation*.
- Korelasikan suhu dengan kW/rack.

Target PUE: 1,85 → 1,75

Tahap 3 — 6 sampai 12 Bulan: Optimasi Sistem

- Evaluasi efisiensi UPS.
- Evaluasi fan dan pump.
- Tambah metering energi.
- Terapkan dashboard energi.
- Konsolidasi server idle.
- Review kapasitas cooling.

Target PUE: 1,75 → 1,65

Tahap 4 — 12 sampai 18 Bulan: Transformasi

- Evaluasi *economizer*.
- Evaluasi energi terbarukan.
- Mulai WUE dan CUE.
- Kajian *waste heat reuse*.
- Integrasi audit energi ke KPI operasi.

Target PUE: 1,65 → 1,6

Catatan penting: target PUE harus realistis terhadap lokasi, usia fasilitas, densitas rak, teknologi cooling, dan pola beban. Tidak semua fasilitas bisa mengejar angka yang sama.

Materi Praktek 5: Checklist *Green Retrofit* untuk Data Center Lama

Area	Pertanyaan Pemeriksaan	Status
Baseline	Apakah PUE sudah dihitung 12 bulan?	Ya / Tidak
Metering	Apakah energi IT dan energi fasilitas terpisah?	Ya / Tidak
Tagihan listrik	Apakah beban puncak dan faktor daya dianalisis?	Ya / Tidak
Server idle	Apakah perangkat tidak terpakai sudah diidentifikasi?	Ya / Tidak
Konsolidasi	Apakah beban kerja bisa digabung?	Ya / Tidak
Rack density	Apakah kW/rack diketahui?	Ya / Tidak
Airflow	Apakah hot aisle/cold aisle sudah benar?	Ya / Tidak
Blanking panel	Apakah U kosong tertutup?	Ya / Tidak
Celah kabel	Apakah lubang kabel sudah ditutup?	Ya / Tidak
Containment	Apakah HAC/CAC layak?	Ya / Tidak
Cooling	Apakah set point dan kontrol fan/pump optimal?	Ya / Tidak
UPS	Apakah efisiensi UPS dievaluasi?	Ya / Tidak
WUE	Apakah penggunaan air dihitung?	Ya / Tidak
CUE	Apakah intensitas karbon dihitung?	Ya / Tidak
ERE	Apakah panas buangan bisa dimanfaatkan?	Ya / Tidak
Energi terbarukan	Apakah opsi energi rendah karbon dikaji?	Ya / Tidak
Limbah perangkat	Apakah ada prosedur daur ulang?	Ya / Tidak
Audit	Apakah temuan menjadi rencana aksi?	Ya / Tidak
Sertifikasi	Apakah bukti energi siap diaudit?	Ya / Tidak

Cara pakai: checklist ini dipakai untuk data center lama sebelum investasi besar. Tujuannya menemukan perbaikan murah dan berdampak tinggi sebelum mengganti sistem utama.

Ringkasan Bab 7

Bab ini menegaskan bahwa *environmentally friendly data center* tidak boleh dipersempit menjadi PUE rendah. PUE penting, tetapi keberlanjutan membutuhkan pandangan lebih luas: **energi, air, karbon, panas buangan, operasi, perangkat, dan siklus hidup fasilitas.**

Buku *Data Centers of the Future* menekankan bahwa setiap data center berbeda karena lokasi, model pelanggan, usia fasilitas, air, energi, dan kebutuhan operasional; karena itu strategi keberlanjutan tidak bisa disalin mentah-mentah. Brochard dkk. menunjukkan bahwa *free cooling, waste heat reuse, hot water cooling*, dan pemanfaatan panas dapat menjadi bagian penting menuju data center yang jauh lebih efisien.

Inti bab: data center hijau adalah data center yang diukur, dioptimalkan, dibuktikan, dan terus diperbaiki.

Checklist Akhir Bab 7

Sebelum masuk Bab 8, pembaca harus mampu menjawab:

- Apakah PUE bulanan sudah dihitung?
- Apakah energi IT dan energi fasilitas diukur terpisah?
- Apakah DCiE, WUE, CUE, dan ERE mulai dipahami?
- Apakah ada *server* atau perangkat idle?
- Apakah konsolidasi dan *right-sizing* sudah dilakukan?
- Apakah airflow sudah efisien?
- Apakah cooling bekerja sesuai kebutuhan, bukan berlebihan?
- Apakah konsumsi air dihitung?
- Apakah sumber energi dan intensitas karbon dipahami?
- Apakah beban kerja fleksibel dapat dijalankan secara *carbon-aware*?
- Apakah panas buangan bisa dimanfaatkan?
- Apakah audit energi menghasilkan rencana aksi?
- Apakah roadmap efisiensi energi sudah memiliki target 3, 6, 12, dan 24 bulan?
- Apakah semua data energi, air, karbon, dan tindakan perbaikan siap menjadi **bukti audit dan sertifikasi**?

Penutup bab: Data center professional tidak cukup hanya andal dan aman. Ia harus hemat energi, sadar air, rendah karbon, terukur, dan bertanggung jawab terhadap masa depan.

Bab 8. Desain Jaringan Data Center: Spine-Leaf, Underlay, Overlay, DCI

Golden Rule: Jaringan data center harus dirancang untuk *latency* rendah, jalur redundan, segmentasi aman, otomasi, dan kemudahan *troubleshooting*.

Bab ini membahas desain jaringan *data center* sebagai fondasi konektivitas layanan. Dalam outline buku, Bab 8 diarahkan untuk membahas evolusi arsitektur jaringan, perbandingan *three-tier* dan *spine-leaf*, *Top-of-Rack*, *End-of-Row*, *underlay*, *overlay*, VXLAN, EVPN, segmentasi tenant, routing internal, DCI, telemetri, keamanan jaringan, dokumentasi, dan validasi desain .

Jaringan *data center* modern tidak boleh hanya “asal tersambung”. Ia harus **terukur, redundant, tersegmentasi, mudah diotomasi, mudah dipantau, dan siap diaudit**.

8.1 Evolusi Arsitektur Jaringan Data Center

Jaringan *data center* lama banyak dibangun dengan pola berlapis: akses, agregasi, dan core. Pola ini cocok saat trafik dominan bergerak dari pengguna ke server dan kembali lagi. Namun pola trafik modern berubah. Virtualisasi, *container*, *storage over IP*, AI, analitik data, dan aplikasi terdistribusi membuat trafik antar-server atau *east-west traffic* meningkat tajam.

Karena itu, desain jaringan bergerak menuju *fabric*. Tujuannya adalah membuat koneksi antar-rak lebih konsisten, *latency* lebih rendah, jalur lebih banyak, dan skala lebih mudah. Buku *Cloud Data Center Network Architectures and Technologies* menjelaskan bahwa pembahasan DCN modern dimulai dari arsitektur fisik, evolusi teknologi, *underlay network*, *overlay network*, VXLAN, multi-DC, keamanan, dan Praktek deployment .

Evolusi ini bukan sekadar perubahan topologi. Ini adalah perubahan cara berpikir: dari jaringan sebagai kumpulan switch menjadi **jaringan sebagai fabric layanan**. Fabric harus dapat mendukung banyak tenant, banyak aplikasi, segmentasi, otomasi, monitoring, dan integrasi dengan operasi.

Prinsip evolusi:

- Dari trafik dominan *north-south* menuju kombinasi *north-south* dan *east-west*.
- Dari VLAN statis menuju segmentasi yang lebih elastis.
- Dari konfigurasi manual menuju otomasi.
- Dari monitoring pasif menuju *telemetry*.
- Dari jaringan tunggal menuju multi-site dan DR.
- Dari keamanan perimeter menuju segmentasi internal.

Kalimat kunci: jaringan data center modern bukan hanya jalur paket, tetapi sistem kendali layanan digital.

8.2 Three-Tier Architecture vs Spine-Leaf Architecture

Three-tier architecture terdiri dari tiga lapisan: access, aggregation, dan core. Lapisan access menghubungkan server. Lapisan aggregation mengumpulkan trafik dari banyak access. Lapisan core menjadi tulang punggung utama. Model ini mudah dipahami, tetapi dapat menimbulkan jalur tidak seimbang, bottleneck, dan *latency* tidak konsisten ketika trafik antar-server meningkat.

Spine-leaf architecture memakai dua lapisan utama. Leaf menghubungkan server atau rak. Spine menghubungkan semua leaf. Setiap leaf terhubung ke semua spine. Dengan pola ini, setiap leaf memiliki jalur yang lebih konsisten ke leaf lain. Desain ini sering memakai routing Layer 3 dan ECMP agar banyak jalur dapat digunakan secara aktif.

Referensi desain *data center fabric* menjelaskan bahwa desain klasik memakai access, aggregation, dan core, sedangkan tren modern bergerak ke *two-tier spine-leaf architecture*. Referensi yang sama menyebut workload seperti virtualized data center, *big data*, HPC, *ultra-low latency*, dan skala besar sebagai pendorong kebutuhan fabric yang lebih fleksibel.

Perbandingan ringkas:

Aspek	Three-Tier	Spine-Leaf
Lapisan	Access, aggregation, core	Leaf dan spine
Pola trafik cocok	North-south dominan	East-west dan north-south
Latency	Bisa bervariasi	Lebih konsisten
Skala	Lebih kompleks saat tumbuh	Tambah leaf/spine lebih mudah
Jalur aktif	Sering terbatas	Banyak jalur aktif via ECMP
Operasi	Familiar	Butuh disiplin routing dan otomasi
Cocok untuk	Data center tradisional	Cloud, virtualisasi, AI, HPC, multi-tenant

Catatan tajam: *spine-leaf* bukan otomatis lebih baik jika desain, kapasitas, routing, kabel, dan operasi tidak matang. Topologi yang baik tetap bisa gagal jika dokumentasi buruk dan monitoring lemah.

8.3 Top-of-Rack dan End-of-Row

Top-of-Rack atau ToR berarti switch ditempatkan di setiap rak atau dekat rak. Server dalam rak terhubung ke switch ToR, lalu ToR terhubung ke spine atau aggregation. Keunggulannya adalah kabel server lebih pendek, ekspansi per rak lebih mudah, dan batas gangguan lebih jelas. Kekurangannya adalah jumlah switch lebih banyak dan operasi harus disiplin.

End-of-Row atau EoR berarti switch ditempatkan di ujung baris rak. Server dari beberapa rak ditarik kabelnya ke switch di ujung baris. Keunggulannya adalah jumlah switch bisa lebih sedikit, tetapi kabel horizontal lebih banyak dan manajemen kabel lebih menantang.

Referensi *data center design* menyebut tiga pendekatan fisik utama: EoR, MoR, dan ToR. Pemilihan model dipengaruhi oleh ukuran *failure domain*, daya yang tersedia, jumlah server per rak, jumlah antarmuka per server, kecepatan antarmuka, batasan kabel, batasan operasi, bentuk switch, anggaran, dan rasio *oversubscription*.

Panduan pemilihan:

- Gunakan **ToR** jika jumlah rak banyak, kabel ingin pendek, dan pertumbuhan per rak penting.
- Gunakan **EoR** jika jumlah switch ingin ditekan dan jalur kabel masih terkendali.
- Gunakan pendekatan campuran jika ada rak khusus seperti storage, GPU, atau jaringan keamanan.
- Selalu kaitkan keputusan dengan power, cooling, kabel, operasi, dan dokumentasi.

Prinsip praktis: pemilihan ToR atau EoR bukan selera jaringan saja; ia memengaruhi kabel, listrik, airflow, rak, operasi, dan biaya.

8.4 Underlay Network

Underlay network adalah jaringan fisik yang membawa trafik antar-switch. Dalam desain modern, *underlay* biasanya dibangun sebagai jaringan Layer 3 yang stabil, sederhana, dan cepat konvergen. Tugas utamanya adalah menyediakan konektivitas IP antar-leaf, antar-spine, dan node penting lain.

Underlay yang baik harus sederhana. Jangan mencampur terlalu banyak fungsi layanan di *underlay*. Segmentasi layanan, tenant, dan logika aplikasi sebaiknya ditempatkan di *overlay*. Dengan begitu, jaringan fisik tetap kuat, mudah diaudit, dan mudah diperluas.

Buku *Cloud Data Center Network Architectures and Technologies* secara eksplisit memisahkan konstruksi jaringan fisik atau *underlay network* dan jaringan logis atau *overlay network*; *underlay* dibahas sebagai jaringan fisik, sedangkan *overlay* membahas VXLAN dan jaringan logis di atasnya .

Komponen desain *underlay*:

- Skema alamat IP point-to-point.
- Loopback untuk router ID dan peering.
- Routing internal.
- ECMP.
- MTU yang mendukung encapsulation.
- BFD jika dibutuhkan.
- Redundansi link.
- Monitoring link dan routing.
- Dokumentasi port antar-switch.

**Prinsip tajam: underlay harus membosankan, stabil, dan dapat diprediksi.
Kompleksitas layanan tempatkan di overlay.**

8.5 Overlay Network: VXLAN, EVPN, Tenant Segmentation

Overlay network adalah jaringan logis yang berjalan di atas *underlay*. Overlay memungkinkan layanan Layer 2 atau Layer 3 dibangun di atas jaringan fisik Layer 3. Ini penting untuk multi-tenant, segmentasi, mobilitas workload, dan skalabilitas yang lebih besar dibanding VLAN tradisional.

VXLAN atau *Virtual eXtensible LAN* digunakan untuk membuat overlay. RFC 7348 menjelaskan VXLAN sebagai mekanisme yang menjawab kebutuhan *overlay network* dalam *data center* virtual yang menampung banyak tenant; VXLAN digunakan pada cloud service provider maupun enterprise data center ([IETF Datatracker](#)).

EVPN sering dipakai sebagai *control plane* untuk VXLAN. RFC 7432 menjelaskan EVPN sebagai prosedur berbasis BGP untuk layanan Ethernet VPN; dalam Praktek modern, EVPN membantu distribusi informasi MAC, IP, dan segmentasi antar-VTEP secara lebih terkendali dibanding model flood-and-learn ([IETF Datatracker](#)).

Tenant segmentation berarti memisahkan jaringan berdasarkan fungsi, organisasi, aplikasi, atau tingkat keamanan. Segmentasi dapat dilakukan dengan VLAN, VRF, VXLAN VNI, ACL, firewall, atau microsegmentation. Tujuannya adalah membatasi dampak insiden dan mengurangi pergerakan lateral.

Istilah penting:

Istilah	Makna Praktis
VXLAN	Teknologi overlay untuk memperluas jaringan logis di atas IP
VNI	Identitas segmen VXLAN
VTEP	Titik awal/akhir enkapsulasi VXLAN
EVPN	<i>Control plane</i> untuk distribusi informasi overlay
VRF	Pemisahan tabel routing
Tenant	Unit logis layanan / pelanggan / aplikasi
Microsegmentation	Segmentasi halus antar-beban kerja

Catatan kritis: overlay yang buruk bisa menyembunyikan masalah underlay. Karena itu, troubleshooting harus mampu membaca dua lapisan: **paket logis di overlay dan jalur fisik di underlay**.

8.6 Routing Internal Data Center

Routing internal *data center* harus cepat, sederhana, dan dapat diprediksi. Dalam *spine-leaf*, routing biasanya dibuat agar semua jalur leaf–spine dapat aktif. ECMP digunakan untuk membagi trafik ke beberapa jalur yang setara.

Ada beberapa pilihan protokol routing internal. Yang penting bukan hanya nama protokol, tetapi kesesuaian dengan skala, kemampuan tim, kebutuhan otomasi, dan dukungan perangkat. Untuk desain profesional, routing harus memiliki desain alamat, *loopback*, *route policy*, *failure domain*, dan dokumentasi yang jelas.

Prinsip routing internal:

- Gunakan desain IP yang konsisten.
- Gunakan link point-to-point antar leaf dan spine.
- Gunakan *loopback* untuk identitas stabil.
- Aktifkan ECMP.
- Hindari bridging Layer 2 luas di underlay.
- Gunakan BFD jika butuh deteksi gagal cepat.
- Batasi *failure domain*.
- Dokumentasikan semua peering.

Kesalahan umum: membuat Layer 2 terlalu luas karena ingin “mudah”. Akibatnya, domain gangguan menjadi besar dan troubleshooting sulit.

Kalimat kunci: routing data center yang baik bukan yang paling rumit, tetapi yang paling cepat dipahami saat insiden.

8.7 Data Center Interconnect dan DR Site

Data Center Interconnect atau DCI menghubungkan dua atau lebih *data center*. Tujuannya bisa untuk DR, replikasi data, active-standby, active-active, migrasi beban kerja, atau mendekatkan layanan ke pengguna.

Buku *Cloud Data Center Network Architectures and Technologies* menjelaskan bahwa multi-DC dibutuhkan karena ekspansi skala layanan, reliabilitas, dan kontinuitas. Layanan dapat didistribusikan antar-DC, membentuk model multi-active, dan melayani pengguna dari lokasi terdekat untuk meningkatkan pengalaman pengguna .

DCI harus dirancang hati-hati. Kesalahan DCI dapat memperluas domain gangguan dari satu data center ke data center lain. Jangan membawa Layer 2 antar-site tanpa alasan kuat dan kontrol yang matang. DR yang baik membutuhkan sinkronisasi data, routing failover, keamanan, DNS, kapasitas, prosedur, dan uji berkala.

Pertanyaan desain DCI:

- Apakah modelnya active-standby atau active-active?
- Apakah aplikasi mendukung operasi multi-site?
- Berapa RTO dan RPO?
- Apakah perlu Layer 2 extension?
- Bagaimana routing failover dilakukan?
- Bagaimana replikasi storage dilakukan?
- Bagaimana segmentasi tenant dijaga antar-site?
- Bagaimana firewall policy disinkronkan?
- Apakah kapasitas link cukup saat failover?
- Apakah failover pernah diuji?

Prinsip tajam: DCI bukan kabel antar-gedung; DCI adalah desain kontinuitas layanan.

8.8 Telemetry dan Observability Jaringan

Monitoring tradisional sering berbasis polling berkala. Ini berguna, tetapi tidak selalu cukup untuk jaringan modern yang cepat berubah. *Telemetry* memungkinkan perangkat jaringan mengirim data status secara lebih kontinu ke sistem pengumpul data. Dengan *telemetry*, tim operasi dapat melihat kondisi link, antrian, error, routing, latency, packet drop, dan perubahan konfigurasi secara lebih cepat.

OpenConfig gNMI mendefinisikan protokol berbasis gRPC untuk mengambil dan mengubah konfigurasi, serta mengontrol dan menghasilkan aliran telemetry dari perangkat jaringan ke sistem pengumpul data (openconfig.net).

Observability lebih luas dari monitoring. Ia menggabungkan metrik, log, event, konfigurasi, topologi, dan korelasi insiden. Tujuannya adalah menjawab: **apa yang terjadi, di mana, mengapa, dan apa dampaknya ke layanan?**

Data minimum yang perlu dipantau:

- Status port.
- Utilisasi link.
- Error dan discard.
- Latency.
- Packet drop.
- Status routing neighbor.
- Status VXLAN/EVPN.
- Perubahan konfigurasi.
- Log keamanan.
- Kapasitas VLAN/VRF/VNI.
- Jalur DCI.
- Alarm perangkat.

Catatan sertifikasi: observability yang baik bukan hanya dashboard. Harus ada **prosedur respons, tiket, bukti insiden, dan laporan perbaikan**.

8.9 Prinsip Keamanan Jaringan Data Center

Keamanan jaringan *data center* tidak boleh hanya berada di tepi jaringan. Serangan modern sering bergerak dari satu server ke server lain. Karena itu, segmentasi internal sangat penting.

Buku *Cloud Data Center Network Architectures and Technologies* menjelaskan bahwa pada cloud DCN, switch dan firewall dapat mendukung sistem virtual seperti VRF atau sistem virtual lain; trafik antar-user diblokir secara default, zona keamanan dipersempit, dan kebijakan keamanan dapat dibedakan sesuai karakter layanan .

Prinsip keamanan jaringan:

- Pisahkan jaringan produksi, manajemen, storage, backup, keamanan, dan OT.
- Gunakan VRF untuk isolasi routing.
- Gunakan firewall atau policy enforcement untuk trafik antar-zona.
- Batasi akses manajemen ke perangkat jaringan.
- Gunakan MFA untuk akses admin bila tersedia.
- Log semua akses dan perubahan konfigurasi.
- Gunakan jaringan OOB untuk manajemen kritikal.
- Terapkan prinsip *least privilege*.
- Uji segmentasi secara berkala.

Kalimat tajam: jaringan flat adalah undangan bagi insiden untuk menyebar.

8.10 Dokumentasi dan Validasi Desain Jaringan

Desain jaringan harus bisa dijelaskan, diuji, dan diaudit. Dokumentasi bukan pekerjaan administratif belakangan. Dokumentasi adalah alat operasi.

Dokumen minimum:

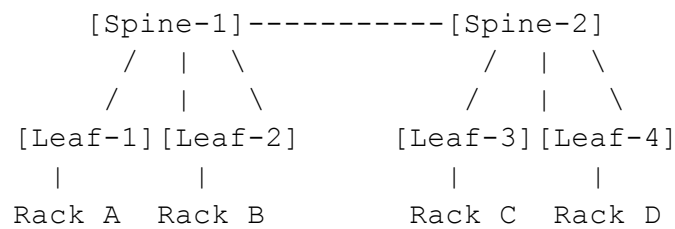
- HLD atau *High-Level Design*.
- LLD atau *Low-Level Design*.
- Diagram fisik.
- Diagram logis.
- Daftar perangkat.
- Daftar port.
- Tabel IP.
- Tabel VLAN.
- Tabel VRF.
- Tabel VNI.
- Routing plan.
- Security zoning.
- DCI plan.
- Telemetry plan.
- Test plan.
- Rollback plan.
- Dokumen *as-built*.

Validasi desain harus dilakukan sebelum produksi. Uji link failure, device failure, routing convergence, segmentasi, DCI failover, kapasitas link, latency, packet loss, dan keamanan akses. Untuk sertifikasi, hasil uji harus disimpan sebagai bukti.

Prinsip audit: desain yang tidak terdokumentasi dianggap tidak dapat dibuktikan; desain yang tidak diuji dianggap belum siap operasi.

Materi Praktek 1: Contoh Desain Jaringan 2 Spine 4 Leaf

Topologi Dasar



Prinsip Desain

- Setiap leaf terhubung ke semua spine.
- Tidak ada koneksi langsung antar-leaf.
- Tidak ada koneksi langsung antar-spine untuk forwarding normal.
- Server terhubung ke leaf.
- Routing underlay berjalan antar leaf dan spine.
- Overlay VXLAN/EVPN berjalan di atas underlay.
- Leaf dapat menjadi VTEP.
- Border leaf dipakai untuk keluar ke WAN, internet, atau DCI.
- Service leaf dapat dipakai untuk firewall, load balancer, atau layanan keamanan.

Contoh Alokasi Fungsi

Perangkat	Fungsi	Catatan
Spine-1	Core fabric	ECMP
Spine-2	Core fabric	Redundansi
Leaf-1	Access rack A	Server produksi
Leaf-2	Access rack B	Server aplikasi
Leaf-3	Access rack C	Storage / backup
Leaf-4	Border / service leaf	Firewall, DCI, uplink

Hal yang Harus Diuji

- Jika satu link leaf-spine putus, trafik tetap berjalan.
- Jika satu spine mati, leaf tetap saling terhubung.
- Jika satu leaf mati, hanya rack terkait terdampak.
- Overlay tetap berjalan setelah failover.
- Segmentasi VLAN/VRF/VNI tetap sesuai.
- Telemetry mencatat kejadian link down.

Catatan: desain ini adalah contoh awal. Desain final harus menyesuaikan kapasitas port, bandwidth, oversubscription, beban aplikasi, keamanan, dan target sertifikasi.

Materi Praktek 2: Contoh Tabel VLAN / VRF / Segmentasi

Zona	VLAN	VRF	VXLAN VNI	Fungsi	Akses Diizinkan
Management	10	VRF-MGMT	10010	Manajemen perangkat	Admin OOB saja
Production App	20	VRF-PROD	10020	Aplikasi produksi	Dari load balancer / firewall
Database	30	VRF-DB	10030	Basis data	Hanya dari aplikasi tertentu
Storage	40	VRF-STORAGE	10040	Storage traffic	Server tertentu
Backup	50	VRF-BACKUP	10050	Backup dan restore	Backup server
Security	60	VRF-SEC	10060	Sensor dan log	SIEM / admin keamanan
DMZ	70	VRF-DMZ	10070	Layanan eksternal	Dari firewall border

Catatan Desain

- Jangan campur jaringan manajemen dengan produksi.
- Jangan campur backup dengan trafik user.
- Database tidak boleh terbuka langsung ke semua zona.
- DMZ harus dikontrol ketat.
- VRF membantu isolasi routing.
- VNI membantu segmentasi overlay.
- Semua aturan harus diuji dan didokumentasikan.

Prinsip: segmentasi yang baik harus menjawab **siapa boleh bicara dengan siapa, lewat jalur mana, dan dengan bukti log apa.**

Materi Praktek 3: Checklist Desain DCI

Area	Pertanyaan Pemeriksaan	Status
Tujuan DCI	Apakah untuk DR, active-active, migrasi, atau replikasi?	Ya / Tidak
RTO/RPO	Apakah target pemulihan sudah jelas?	Ya / Tidak
Kapasitas link	Apakah bandwidth cukup saat failover?	Ya / Tidak
Latency	Apakah latency antar-site sesuai aplikasi?	Ya / Tidak
Routing	Apakah failover routing sudah dirancang?	Ya / Tidak
Layer 2 extension	Apakah benar-benar diperlukan?	Ya / Tidak
Segmentasi	Apakah VRF/VNI/policy konsisten antar-site?	Ya / Tidak
Keamanan	Apakah trafik antar-site terenkripsi bila diperlukan?	Ya / Tidak
Firewall policy	Apakah policy antar-site terdokumentasi?	Ya / Tidak
DNS / service discovery	Apakah perubahan lokasi layanan didukung?	Ya / Tidak
Monitoring	Apakah link DCI dipantau?	Ya / Tidak
Uji failover	Apakah failover pernah diuji?	Ya / Tidak
Rollback	Apakah prosedur rollback tersedia?	Ya / Tidak
Bukti audit	Apakah hasil uji tersimpan?	Ya / Tidak

Catatan tajam: DCI yang tidak pernah diuji adalah asumsi, bukan strategi DR.

Materi Praktek 4: Template *Network Low-Level Design*

1. Informasi Umum

- Nama proyek:
- Lokasi data center:
- Target layanan:
- Target *availability*:
- Target kapasitas:
- Tanggal desain:
- Penanggung jawab:

2. Topologi Fisik

- Daftar spine:
- Daftar leaf:
- Border leaf:
- Service leaf:
- OOB management:
- Diagram fisik:
- Daftar kabel:
- Daftar port:

3. Topologi Logis

- Underlay routing:
- Loopback:
- IP point-to-point:
- ECMP:
- Overlay:
- VXLAN:
- EVPN:
- VRF:
- VNI:

4. Segmentasi

Zona	VLAN	VRF	VNI	Policy

5. Routing Plan

- Protokol routing:
- ASN / area / domain:
- Route policy:

- Default route:
- External route:
- DCI route:
- Failover behavior:

6. Security Plan

- Management access:
- OOB:
- ACL:
- Firewall insertion:
- Logging:
- AAA:
- Change approval:

7. Telemetry dan Monitoring

- Metrik yang dipantau:
- Collector:
- Dashboard:
- Alarm:
- Log retention:
- Laporan operasi:

8. Test Plan

- Link failure:
- Spine failure:
- Leaf failure:
- Routing convergence:
- VXLAN/EVPN validation:
- Segmentasi antar-zona:
- DCI failover:
- Rollback:

9. Dokumen Bukti

- Diagram final.
- Konfigurasi *baseline*.
- Hasil uji.
- Foto instalasi.
- Log perubahan.
- Dokumen *as-built*.

Ringkasan Bab 8

Bab ini menegaskan bahwa jaringan *data center* harus dirancang sebagai **fabric layanan**, bukan sekadar kumpulan switch. Desain modern bergerak dari *three-tier* menuju *spine-leaf* karena kebutuhan trafik *east-west*, virtualisasi, AI, HPC, multi-tenant, dan kebutuhan skalabilitas.

Buku *Cloud Data Center Network Architectures and Technologies* menempatkan desain DCN sebagai rangkaian lengkap: arsitektur fisik, *underlay*, *overlay*, VXLAN, multi-DC, keamanan, deployment, dan operasi. RFC 7348 menjadi rujukan utama VXLAN untuk overlay multi-tenant di data center virtual, sedangkan RFC 7432 menjadi rujukan EVPN sebagai prosedur BGP untuk Ethernet VPN ([IETF Datatracker](#)).

Inti bab: jaringan data center profesional harus rendah latency, redundan, tersegmentasi, terpantau, terdokumentasi, dan terbukti melalui pengujian.

Checklist Akhir Bab 8

Sebelum masuk Bab 9, pembaca harus mampu menjawab:

- Apakah pola trafik aplikasi dominan *north-south*, *east-west*, atau campuran?
- Apakah desain masih cocok dengan *three-tier* atau perlu *spine-leaf*?
- Apakah model ToR, EoR, atau campuran sudah dipilih berdasarkan kebutuhan nyata?
- Apakah *underlay* sederhana, stabil, dan terdokumentasi?
- Apakah *overlay* memakai segmentasi yang jelas?
- Apakah VLAN, VRF, dan VNI sudah dipetakan?
- Apakah routing internal mendukung ECMP dan failover?
- Apakah DCI dirancang sesuai RTO/RPO?
- Apakah DR site pernah diuji?
- Apakah telemetry dan observability sudah dirancang?
- Apakah akses manajemen jaringan dipisahkan dan diamankan?
- Apakah segmentasi antar-zona sudah diuji?
- Apakah HLD, LLD, konfigurasi baseline, test plan, dan *as-built* tersedia?
- Apakah semua hasil uji siap menjadi **bukti audit dan sertifikasi**?

Penutup bab: Data center profesional membutuhkan jaringan yang bukan hanya cepat, tetapi terstruktur, aman, dapat diamati, dapat diuji, dan dapat dipertanggungjawabkan saat terjadi insiden maupun audit.

Bab 9. Secure Data Center: Physical, Network, Cyber, Zero Trust, Audit

Golden Rule: Keamanan *data center* harus berlapis: orang, ruang, perangkat, jaringan, aplikasi, data, proses, dan bukti audit.

Bab ini membahas keamanan *data center* secara menyeluruh. Dalam outline buku, Bab 9 diarahkan untuk membahas keamanan fisik, keamanan ruang, keamanan jaringan, keamanan manajemen, keamanan OT, *Zero Trust*, *patch management*, *vulnerability management*, *backup*, DR, kesiapan ransomware, *audit trail*, kepatuhan, dan *incident response*.

Inti bab ini: **keamanan *data center* bukan satu alat, bukan satu firewall, dan bukan satu SOP. Keamanan adalah sistem berlapis yang harus bisa dibuktikan.**

9.1 Keamanan Fisik: Perimeter, Akses, CCTV, Mantrap

Keamanan *data center* dimulai dari fisik. Sebelum bicara serangan siber, organisasi harus memastikan orang yang tidak berhak tidak bisa masuk ke lokasi, gedung, ruang kritikal, rak, panel listrik, ruang UPS, ruang baterai, ruang cooling, dan ruang operasi.

ISO/IEC 22237 menempatkan **physical security** sebagai salah satu klasifikasi penting dalam desain dan operasi *data center*, bersama *availability* dan *energy efficiency enablement*. Artinya, keamanan fisik bukan tambahan, tetapi bagian dari standar fasilitas ([VDE Verlag](#)).

Lapisan keamanan fisik biasanya mencakup:

- **Perimeter luar:** pagar, pos jaga, lampu, zona parkir, pembatas kendaraan.
- **Akses gedung:** kartu akses, biometrik, daftar tamu, prosedur tamu.
- **Akses ruang kritikal:** kontrol akses bertingkat.
- **CCTV:** area luar, pintu, koridor, ruang komputer, loading area.
- **Mantrap:** ruang perantara untuk mencegah orang masuk beriringan tanpa otorisasi.
- **Alarm pintu:** deteksi pintu dibuka paksa atau terlalu lama terbuka.
- **Patroli dan log keamanan:** bukti kegiatan pengamanan.

Untuk sertifikasi, keamanan fisik tidak cukup dengan “ada CCTV”. Harus ada bukti: denah kamera, area cakupan, masa simpan rekaman, daftar akses, log tamu, prosedur pengawalan, hasil uji alarm, dan catatan insiden.

Notifikasi tajam: akses fisik yang lemah dapat membuat kontrol siber paling mahal menjadi tidak berarti.

9.2 Keamanan Ruang: Rack Lock, Visitor Log, Escort Policy

Setelah perimeter dan pintu utama aman, keamanan harus masuk ke tingkat ruang dan rak. Tidak semua orang yang boleh masuk gedung boleh masuk ruang komputer. Tidak semua orang yang boleh masuk ruang komputer boleh membuka rak. Tidak semua teknisi vendor boleh bekerja tanpa pengawasan.

Kontrol ruang yang penting:

- **Kunci rak** untuk perangkat kritikal.
- **Pembatasan area** berdasarkan fungsi kerja.
- **Visitor log** untuk semua tamu dan vendor.
- **Escort policy**: tamu wajib didampingi.
- **Larangan membawa perangkat tidak sah** ke ruang kritikal.
- **Pemeriksaan barang masuk dan keluar**.
- **Label rak dan perangkat** agar tidak salah tindakan.
- **CCTV mengarah ke area akses**, bukan mengganggu privasi berlebihan.
- **Prosedur pekerjaan di ruang komputer**: siapa, kapan, apa yang dikerjakan, dan siapa yang menyetujui.

Data Center Handbook menekankan pentingnya sistem keamanan seperti akses kontrol dan CCTV dalam operasi fasilitas, bahkan menyarankan sistem tersebut dipasok dari UPS agar tetap berjalan saat gangguan listrik .

Prinsip audit: setiap akses ke ruang kritikal harus meninggalkan jejak: **identitas, waktu, tujuan, pendamping, area yang diakses, dan bukti keluar**.

9.3 Keamanan Jaringan: Firewall, ACL, IDS/IPS, Segmentasi

Keamanan jaringan *data center* harus mencegah, membatasi, mendeteksi, dan mencatat akses yang tidak sah. Model jaringan datar sangat berbahaya karena satu insiden dapat bergerak cepat ke banyak sistem.

Kontrol utama:

- **Firewall** antar-zona.
- **ACL** untuk membatasi akses spesifik.
- **IDS/IPS** untuk deteksi dan pencegahan serangan.
- **Segmentasi VLAN/VRF/VNI**.
- **DMZ** untuk layanan yang menghadap luar.
- **Pemisahan jaringan produksi, storage, backup, management, dan OT**.
- **Logging trafik penting**.
- **Monitoring anomali**.
- **Kontrol akses admin jaringan**.

Buku *Cloud Data Center Network Architectures and Technologies* menekankan bahwa cloud DCN membutuhkan peningkatan menyeluruh pada keamanan jaringan, termasuk ketersediaan tinggi, kemampuan visualisasi aplikasi, otomasi manajemen, dan *troubleshooting* cepat untuk menghadapi tekanan risiko keamanan siber .

Segmentasi juga penting pada arsitektur aplikasi. *Data Centre Management* menjelaskan bahwa model multi-tier dapat meningkatkan keamanan karena web, aplikasi, dan database dipisahkan; firewall dan VLAN dapat digunakan untuk menegakkan pemisahan antar-tier .

Kalimat kunci: segmentasi bukan memperumit jaringan; segmentasi membatasi kerusakan saat insiden terjadi.

9.4 Keamanan Manajemen: OOB, MFA, Bastion, Logging

Jaringan manajemen adalah target bernilai tinggi. Jika penyerang menguasai jalur manajemen, mereka dapat mengubah konfigurasi switch, firewall, server, storage, UPS, cooling, atau sistem monitoring. Karena itu, jaringan manajemen harus dipisahkan dari jaringan produksi.

Kontrol yang disarankan:

- **OOB atau *Out-of-Band Management*** untuk akses darurat dan manajemen perangkat.
- **MFA atau *Multi-Factor Authentication*** untuk admin.
- ***Bastion host*** sebagai titik masuk terkendali.
- **Akses berbasis peran.**
- **Logging semua login dan perubahan konfigurasi.**
- **Session recording** untuk pekerjaan kritis.
- **Akses vendor terbatas waktu.**
- **Tidak ada akses langsung dari jaringan umum ke perangkat manajemen.**
- **Review berkala akun admin.**

NIST SP 800-207 menjelaskan bahwa *Zero Trust Architecture* memindahkan fokus dari perimeter jaringan statis menuju perlindungan pengguna, aset, dan sumber daya; prinsip ini relevan untuk jaringan manajemen karena lokasi jaringan tidak boleh otomatis dianggap tepercaya ([NIST Computer Security Resource Center](#)).

Prinsip tajam: akses admin harus dianggap sebagai akses berisiko tinggi, walaupun berasal dari jaringan internal.

9.5 Keamanan OT: BMS, DCIM, UPS, Cooling Controller

OT atau *Operational Technology* di *data center* mencakup sistem fasilitas: BMS, DCIM, UPS, EMS, generator controller, cooling controller, sensor, akses pintu, CCTV, dan sistem lingkungan. Sistem ini sering diperlakukan sebagai “bukan TI”, padahal jika diserang dapat mematikan layanan.

Data Center Handbook menekankan bahwa sistem OT *data center* harus dilindungi dari ancaman fisik dan siber karena sistem power dan cooling mendukung operasi TI. Buku ini juga membahas risiko OT, termasuk BMS, DCIM, EMS, dan sistem fasilitas lain yang memiliki akses lokal maupun jarak jauh .

Risiko OT yang sering muncul:

- Perangkat memakai protokol lama.
- Password bawaan tidak diganti.
- Akses remote vendor tidak dikontrol.
- Sistem tidak dipatch.
- Tidak ada segmentasi.
- Tidak ada logging.
- Perangkat OT terhubung ke jaringan produksi.
- Tidak ada pemetaan aset.
- Tidak ada prosedur respons insiden OT.

Data Center Handbook menyarankan penggunaan firewall yang kuat untuk jaringan OT, segmentasi, VPN khusus untuk setiap sistem konsol manajemen, dan 2FA untuk sistem penting seperti BMS, DCIM, EMS, dan sistem konsol lainnya .

Kontrol minimum OT:

- Inventaris aset OT.
- Segmentasi OT dari jaringan produksi.
- Firewall khusus OT.
- Akses vendor melalui jalur terkendali.
- MFA untuk konsol penting.
- Logging dan alarm.
- Backup konfigurasi OT.
- Prosedur manual jika otomatisasi gagal.
- Uji pemulihan sistem OT.

Kalimat tajam: serangan ke cooling controller bisa sama berbahaya dengan serangan ke server produksi.

9.6 Zero Trust untuk Data Center

Zero Trust bukan produk. *Zero Trust* adalah prinsip desain keamanan: **jangan percaya hanya karena lokasi jaringan, selalu verifikasi, batasi akses, dan pantau terus-menerus.**

NIST SP 800-207 mendefinisikan *Zero Trust* sebagai pergeseran paradigma keamanan dari pertahanan berbasis perimeter statis menuju fokus pada pengguna, aset, dan sumber daya. *Zero Trust Architecture* digunakan untuk merancang infrastruktur dan alur kerja dengan prinsip *zero trust* ([NIST Computer Security Resource Center](#)).

Penerapan di *data center*:

- Identitas admin diverifikasi dengan kuat.
- Perangkat yang mengakses harus dikenal dan sehat.
- Akses diberikan minimum sesuai kebutuhan.
- Setiap akses dievaluasi berdasarkan konteks.
- Segmentasi dilakukan antar-zona.
- Akses manajemen tidak terbuka langsung.
- Trafik antar-aplikasi dipantau.
- Log dianalisis untuk mendeteksi anomali.
- Akses vendor bersifat terbatas waktu.
- Tidak ada “trusted network” tanpa kontrol.

Contoh sederhana: admin tidak boleh otomatis mengakses semua perangkat hanya karena berada di kantor atau VPN. Ia hanya boleh mengakses perangkat yang relevan, pada waktu yang disetujui, melalui jalur yang tercatat, dengan MFA, dan semua kegiatannya tercatat.

Prinsip praktis: akses harus spesifik, sementara, terverifikasi, dan tercatat.

9.7 Patch Management dan Vulnerability Management

Patch management adalah proses mengelola pembaruan keamanan sistem. *Vulnerability management* lebih luas: menemukan kerentanan, menilai risikonya, memprioritaskan perbaikan, melakukan mitigasi, dan membuktikan bahwa risiko sudah ditangani.

Di *data center*, patching tidak boleh sembrono. Banyak sistem kritikal harus tetap berjalan. Karena itu, patch harus mengikuti proses:

- Inventaris aset.
- Klasifikasi kritikalitas.
- Pemantauan advisori keamanan.
- Uji patch di lingkungan terbatas.
- Jadwal maintenance.
- Persetujuan perubahan.
- Backup konfigurasi.
- Rencana rollback.
- Dokumentasi hasil.
- Verifikasi setelah patch.

NIST CSF 2.0 mengelompokkan pengelolaan risiko siber ke dalam fungsi **Govern, Identify, Protect, Detect, Respond, dan Recovery**. Fungsi ini cocok untuk membangun siklus keamanan *data center*: identifikasi aset dan risiko, proteksi, deteksi, respons, pemulihan, dan tata kelola ([NIST Publications](#)).

Catatan kritis: sistem yang tidak bisa di patch harus dikompensasi dengan kontrol lain: segmentasi, pembatasan akses, monitoring, firewall rule, virtual patching, dan prosedur operasi ketat.

9.8 Backup, DR, dan Ransomware Readiness

Backup adalah pertahanan terakhir ketika sistem rusak, data hilang, atau ransomware menyerang. Namun *backup* tidak berguna jika tidak bisa dipulihkan. DR atau *Disaster Recovery* harus diuji, bukan hanya ditulis.

CISA *StopRansomware Guide* menekankan pentingnya membuat, memelihara, dan secara rutin melatih *cyber incident response plan* serta rencana komunikasi, termasuk respons dan notifikasi saat insiden ransomware ([CISA](#)). CISA juga menyediakan panduan untuk mengurangi risiko ransomware melalui Praktek deteksi, pencegahan, respons, dan pemulihan ([CISA](#)).

Kontrol penting ransomware:

- Backup terjadwal.
- Backup offline atau immutable.
- Uji restore berkala.
- Pemisahan kredensial backup.
- Segmentasi jaringan backup.
- Monitoring perubahan file massal.
- Proteksi endpoint dan server.
- MFA untuk admin backup.
- DR drill.
- Salinan prosedur dalam bentuk offline.

Pertanyaan kritis:

- Kapan terakhir restore diuji?
- Berapa RPO nyata?
- Berapa RTO nyata?
- Apakah backup bisa ikut terenkripsi ransomware?
- Siapa yang boleh menghapus backup?
- Apakah kredensial backup terpisah?
- Apakah laporan uji restore tersedia?

Kalimat tajam: backup yang tidak pernah diuji bukan backup; itu hanya harapan.

9.9 Audit Trail dan Bukti Kepatuhan

Dalam sertifikasi, klaim harus berubah menjadi bukti. Keamanan yang tidak terdokumentasi sulit dipercaya. Karena itu, *audit trail* menjadi bagian penting dari *secure data center*.

Bukti kepatuhan minimum:

- Log akses fisik.
- Log tamu.
- Rekaman CCTV sesuai periode retensi.
- Log akses admin.
- Log perubahan konfigurasi.
- Log firewall.
- Log IDS/IPS.
- Log backup dan restore.
- Hasil scan kerentanan.
- Catatan patch.
- Hasil uji DR.
- Hasil uji insiden.
- SOP, MOP, EOP.
- Bukti review akun.
- Bukti review akses vendor.
- Laporan insiden dan tindak lanjut.

ISO/IEC 22237 menekankan desain dan operasi *data center* harus mempertimbangkan analisis risiko bisnis dan biaya operasi, serta klasifikasi ketersediaan, keamanan fisik, dan efisiensi energi selama umur fasilitas ([Iteh Standards](#)). Karena itu, bukti keamanan harus dapat menunjukkan bahwa risiko dikenali, dikontrol, dan ditinjau.

Prinsip audit: yang tidak tercatat dianggap tidak terjadi; yang tidak bisa dibuktikan dianggap belum siap.

9.10 Incident Response Data Center

Incident response adalah kemampuan organisasi merespons insiden secara cepat, terkendali, dan terdokumentasi. Insiden bisa berupa akses fisik tidak sah, kebakaran, cooling failure, serangan jaringan, ransomware, akun admin bocor, OT terganggu, atau kesalahan operator.

NIST CSF 2.0 menempatkan **Respond** dan **Recover** sebagai fungsi inti setelah risiko diidentifikasi, dilindungi, dan dideteksi ([NIST Publications](#)). Untuk *data center*, ini berarti tim harus memiliki prosedur insiden yang menghubungkan TI, fasilitas, keamanan, manajemen, legal, komunikasi, dan vendor.

Tahapan respons:

1. **Detect** — insiden ditemukan melalui alarm, log, sensor, atau laporan.
2. **Triage** — tentukan tingkat keparahan.
3. **Contain** — batasi dampak.
4. **Eradicate** — hilangkan penyebab.
5. **Recover** — pulihkan layanan.
6. **Communicate** — informasikan pihak yang berwenang.
7. **Document** — catat semua tindakan.
8. **Review** — lakukan *lessons learned*.

Kalimat kunci: insiden tidak boleh hanya diselesaikan; insiden harus dipelajari agar tidak terulang.

Materi Praktek 1: Matriks Kontrol Keamanan Data Center

Area	Risiko	Kontrol	Bukti Audit
Perimeter	Orang tidak sah masuk area fasilitas	Pagar, pos, CCTV, patroli	Log patroli, rekaman CCTV
Pintu ruang komputer	Akses tanpa otorisasi	Access control, MFA fisik, alarm pintu	Log akses, hasil uji alarm
Rak	Perangkat dicabut / diubah	Rack lock, label perangkat	Foto rak, daftar kunci
Tamu/vendor	Pekerjaan tanpa pengawasan	Visitor log, escort policy	Daftar tamu, form pekerjaan
Jaringan produksi	Pergerakan lateral	Firewall, ACL, segmentasi	Rulebase, hasil uji segmentasi
Jaringan manajemen	Admin takeover	OOB, MFA, bastion, logging	Log login, daftar admin
OT	BMS/DCIM/UPS diserang	Segmentasi OT, firewall, MFA	Diagram OT, log akses
Patch	Kerentanan tidak ditutup	Patch cycle, maintenance window	Laporan patch
Backup	Backup ikut terenkripsi	Immutable/offline backup, uji restore	Laporan restore
DR	Failover gagal	DR drill	Hasil simulasi
Audit	Tidak ada bukti	Evidence repository	Daftar bukti
Insiden	Respons lambat	IR plan, tabletop exercise	Laporan latihan

Materi Praktek 2: Checklist Audit Akses Fisik

Pertanyaan	Status
Apakah semua pintu ruang kritikal memakai access control?	Ya / Tidak
Apakah daftar pemegang akses diperbarui berkala?	Ya / Tidak
Apakah akses mantan pegawai/vendor sudah dicabut?	Ya / Tidak
Apakah tamu wajib mengisi visitor log?	Ya / Tidak
Apakah tamu/vendor wajib didampingi?	Ya / Tidak
Apakah CCTV mencakup pintu, koridor, dan ruang kritikal?	Ya / Tidak
Apakah rekaman CCTV memiliki masa simpan yang jelas?	Ya / Tidak
Apakah rak kritikal dikunci?	Ya / Tidak
Apakah alarm pintu diuji?	Ya / Tidak
Apakah ada prosedur barang masuk dan keluar?	Ya / Tidak
Apakah akses ruang UPS, baterai, dan cooling dibatasi?	Ya / Tidak
Apakah bukti audit akses tersimpan?	Ya / Tidak

Materi Praktek 3: Checklist *Hardening Management Network*

Kontrol	Status
Jaringan manajemen terpisah dari produksi	Ya / Tidak
OOB tersedia untuk perangkat kritikal	Ya / Tidak
Akses admin memakai MFA	Ya / Tidak
Akses admin melalui bastion	Ya / Tidak
Tidak ada akses langsung dari jaringan umum	Ya / Tidak
Akun admin individual, bukan akun bersama	Ya / Tidak
Hak akses berbasis peran	Ya / Tidak
Login gagal dicatat dan diberi alarm	Ya / Tidak
Semua perubahan konfigurasi tercatat	Ya / Tidak
Backup konfigurasi perangkat tersedia	Ya / Tidak
Akses vendor dibatasi waktu	Ya / Tidak
Protokol tidak aman dinonaktifkan	Ya / Tidak
Log dikirim ke sistem pencatatan terpusat	Ya / Tidak
Review akses dilakukan berkala	Ya / Tidak

Materi Praktek 4: Template Laporan Insiden

Laporan Insiden Data Center

1. Nomor Insiden:

...

2. Tanggal dan Waktu:

...

3. Lokasi / Sistem Terdampak:

...

4. Jenis Insiden:

Akses fisik / jaringan / server / OT / ransomware / cooling / power / lainnya.

5. Deteksi Awal:

Alarm / log / laporan user / CCTV / sensor / monitoring.

6. Ringkasan Kejadian:

Tuliskan singkat, faktual, tanpa spekulasi.

7. Dampak:

- Layanan terdampak: ...
- Durasi gangguan: ...
- Data terdampak: ...
- Risiko keamanan: ...
- Dampak bisnis: ...

8. Akar Masalah Sementara:

...

9. Tindakan Respons:

- Isolasi: ...
- Pemulihan: ...
- Komunikasi: ...
- Eskalasi: ...

10. Bukti yang Dikumpulkan:

Log, screenshot, foto, CCTV, konfigurasi, tiket, laporan vendor.

11. Status Pemulihan:

Pulih / sebagian pulih / masih investigasi.

12. Tindakan Pencegahan:

...

13. Penanggung Jawab:

...

14. Persetujuan Penutupan Insiden:

...

Catatan: laporan insiden harus disimpan sebagai bahan audit, pembelajaran, dan perbaikan kontrol.

Materi Praktek 5: Contoh Desain Segmentasi

Zona	Fungsi	Kontrol Utama	Boleh Akses Ke
User	Akses pengguna internal	Firewall, proxy, policy	Aplikasi tertentu
Server App	Aplikasi produksi	Firewall antar-zona	Database tertentu
Database	Data kritikal	ACL ketat, audit log	Hanya app tertentu
Storage	Penyimpanan utama	Segmentasi khusus	Server tertentu
Backup	Backup dan restore	Isolasi, akun terpisah	Server backup
Managemen t	Admin perangkat	OOB, MFA, bastion	Perangkat terotorisasi
OT	BMS, DCIM, UPS, cooling	Firewall OT, MFA	Konsol OT terbatas
Security	Log, monitoring, sensor	Akses terbatas	Semua log, bukan semua kontrol
DMZ	Layanan publik	Firewall ketat	App gateway tertentu

Prinsip Alur Trafik

- User tidak boleh langsung ke database.
- Produksi tidak boleh langsung ke jaringan backup kecuali melalui server backup.
- Management tidak boleh bercampur dengan user.
- OT tidak boleh bercampur dengan produksi.
- Security boleh menerima log, tetapi tidak otomatis punya akses penuh.
- DMZ harus menjadi zona paling ketat karena berhadapan dengan luar.

Kalimat tajam: segmentasi yang baik membuat insiden berhenti di satu zona, bukan menyebar ke seluruh fasilitas.

Ringkasan Bab 9

Bab ini menegaskan bahwa keamanan *data center* harus dipahami secara berlapis: fisik, ruang, jaringan, manajemen, OT, aplikasi, data, backup, proses, dan bukti audit. *Data Center Handbook* menempatkan cybersecurity dan OT sebagai bagian penting dari desain dan operasi data center modern, khususnya karena sistem power, cooling, BMS, DCIM, dan EMS kini semakin terhubung ke jaringan .

Pertumbuhan data, AI, IoT, dan 5G memperbesar kebutuhan *storage*, *compute*, transfer data, dan koneksi antar-sistem. Semakin banyak koneksi berarti semakin besar permukaan serangan. Karena itu, keamanan harus dirancang sejak awal, bukan ditempel setelah fasilitas berjalan.

Inti bab: data center aman adalah data center yang membatasi akses, memisahkan zona, memantau aktivitas, menguji pemulihan, dan menyimpan bukti.

Checklist Akhir Bab 9

Sebelum masuk Bab 10, pembaca harus mampu menjawab:

- Apakah perimeter, pintu, CCTV, dan *mantrap* sudah dirancang?
- Apakah akses ruang kritikal dicatat dan ditinjau?
- Apakah rak penting dikunci?
- Apakah tamu/vendor wajib didampingi?
- Apakah jaringan produksi, management, storage, backup, dan OT dipisahkan?
- Apakah firewall, ACL, IDS/IPS, dan segmentasi diuji?
- Apakah akses admin memakai MFA dan *bastion*?
- Apakah OOB tersedia untuk perangkat kritikal?
- Apakah BMS, DCIM, UPS, dan cooling controller diamankan?
- Apakah prinsip *Zero Trust* diterapkan pada akses penting?
- Apakah patch dan vulnerability dikelola dengan siklus formal?
- Apakah backup terlindungi dari ransomware?
- Apakah restore pernah diuji?
- Apakah audit trail lengkap?
- Apakah *incident response plan* tersedia dan dilatih?
- Apakah semua kontrol memiliki **bukti audit dan sertifikasi**?

Penutup bab: Secure data center bukan fasilitas yang hanya memiliki banyak alat keamanan, tetapi fasilitas yang **membuktikan bahwa setiap akses dikontrol, setiap risiko dibatasi, setiap insiden dapat direspons, dan setiap keputusan dapat diaudit.**

Bab 10. Deployment, Testing, Commissioning, dan Handover

Golden Rule: Data center belum siap dipakai sampai semua sistem diuji, dibuktikan, didokumentasikan, dan diserahterimakan secara formal.

Bab ini membahas fase paling kritis setelah desain dan instalasi: memastikan bahwa *data center* benar-benar siap beroperasi. Dalam outline buku, Bab 10 diarahkan untuk membahas tahapan *deployment*, FAT, SAT, pengujian power, cooling, network, security, *Integrated System Test*, dokumentasi *as-built*, *handover*, dan *go-live checklist*.

Inti bab ini sederhana: **data center tidak boleh masuk produksi hanya karena perangkat sudah menyala. Ia harus lulus uji, punya bukti, dan diterima oleh tim operasi.**

10.1 Tahapan Deployment

Deployment adalah proses mengubah desain menjadi fasilitas nyata. Tahap ini mencakup pengadaan, pengiriman perangkat, instalasi, konfigurasi, integrasi, pengujian, dokumentasi, pelatihan, dan serah terima.

Urutan umum *deployment*:

1. **Review desain final**
Pastikan gambar, spesifikasi, kapasitas, jalur listrik, jalur cooling, jalur kabel, dan target sertifikasi sudah disetujui.
2. **Pengadaan dan inspeksi perangkat**
Pastikan perangkat yang datang sesuai spesifikasi, jumlah, kapasitas, sertifikat, dan dokumen teknis.
3. **Instalasi fisik**
Rak, kabel, panel, UPS, generator, cooling, sensor, CCTV, akses kontrol, jaringan, dan perangkat pendukung dipasang sesuai desain.
4. **Konfigurasi awal**
Sistem power, cooling, network, monitoring, security, dan DCIM dikonfigurasi.
5. **Pengujian bertahap**
Sistem diuji dari komponen, sistem, antarsistem, hingga kondisi beban nyata.
6. **Dokumentasi *as-built***
Semua perubahan dari desain awal dicatat sebagai kondisi aktual.
7. **Pelatihan operasi**
Tim operasi harus memahami cara menjalankan, memelihara, dan merespons gangguan.
8. ***Handover* formal**
Fasilitas diserahterimakan dengan dokumen, bukti uji, SOP, MOP, EOP, dan daftar isu tersisa.

Prinsip penting: *deployment* yang baik tidak mengejar cepat selesai, tetapi mengejar **siap operasi dan siap audit**.

10.2 Factory Acceptance Test dan Site Acceptance Test

Factory Acceptance Test atau FAT adalah pengujian perangkat sebelum dikirim ke lokasi. Tujuannya memastikan perangkat utama memenuhi spesifikasi teknis sebelum masuk ke proyek. Perangkat yang biasanya melalui FAT adalah UPS, generator, switchgear, panel utama, chiller, CRAC/CRAH, sistem kontrol, dan perangkat kritikal lain.

Site Acceptance Test atau SAT adalah pengujian setelah perangkat dipasang di lokasi. Tujuannya memastikan perangkat tidak hanya baik secara pabrik, tetapi juga **terpasang benar, terhubung benar, dan bekerja dalam lingkungan sebenarnya**.

Data Center Handbook membagi proses commissioning ke lima level: L1 FAT/FWT untuk perangkat kritikal, L2 pengujian instalasi oleh pemasok/subkontraktor, L3 demonstrasi instalasi/peralatan kepada klien atau konsultan, L4 pengujian antarsistem, dan L5 *Integrated Systems Testing* atau IST. TÜV SÜD juga menempatkan FAT, *quality gates*, inspeksi sistem, dan validasi *Integrated Testing & Commissioning* sebagai bagian dari layanan sertifikasi data center berbasis standar internasional seperti ISO/IEC 22237, EN 50600, dan ANSI/TIA-942. ([TÜV SÜD](#))

Perbedaan ringkas:

Jenis Uji	Lokasi	Tujuan	Contoh Bukti
FAT	Pabrik	Membuktikan perangkat sesuai spesifikasi	Laporan FAT, sertifikat, foto, hasil pengukuran
SAT	Lokasi proyek	Membuktikan perangkat terpasang dan bekerja benar	Laporan SAT, checklist instalasi, hasil uji fungsi
IST	Lokasi proyek	Membuktikan semua sistem bekerja bersama	Skenario uji, log, grafik, berita acara

Catatan tajam: FAT yang baik mengurangi risiko barang salah. SAT yang baik mengurangi risiko instalasi salah. IST yang baik mengurangi risiko sistem gagal saat operasi nyata.

10.3 Testing Power: UPS, Generator, ATS, Load Bank

Pengujian power adalah salah satu pengujian paling penting dalam *data center*. Sistem listrik harus dibuktikan mampu menghadapi gangguan nyata: listrik utama padam, UPS mengambil beban, generator menyala, ATS berpindah, dan beban tetap stabil.

Komponen yang harus diuji:

- **UPS:** kapasitas, beban, alarm, *runtime*, baterai, bypass.
- **Generator:** start otomatis, stabilitas tegangan/frekuensi, bahan bakar, durasi operasi.
- **ATS/AMF:** perpindahan dari listrik utama ke generator dan kembali lagi.
- **Load bank:** simulasi beban listrik agar sistem diuji mendekati kondisi nyata.
- **Panel dan breaker:** selektivitas, label, suhu, proteksi.
- **PDU dan rack PDU:** distribusi daya, beban A/B, metering.

Uptime Institute menekankan bahwa *Tier Standard* adalah standar global untuk *availability* dan performa data center, mencakup lingkungan terbangun dan pendekatan operasi tim ([Uptime Institute](https://www.uptimeinstitute.com/)). Artinya, pengujian power bukan hanya verifikasi teknis, tetapi bukti bahwa fasilitas dapat mendukung target ketersediaan layanan.

Skenario minimum pengujian power:

- Utility normal → UPS normal.
- Utility gagal → UPS menahan beban.
- Generator start otomatis.
- ATS pindah ke generator.
- Beban berjalan di generator.
- Utility kembali.
- ATS kembali ke utility.
- UPS kembali ke kondisi normal.
- Alarm dan log tercatat.
- Tidak ada beban kritis mati.

Prinsip audit: setiap pengujian harus punya **tanggal, skenario, beban, hasil, anomali, tindakan koreksi, dan tanda tangan penerimaan.**

10.4 Testing Cooling: Airflow, Thermal Load, Failover Cooling

Cooling harus diuji bukan hanya saat ruangan kosong, tetapi saat ada simulasi beban panas. Banyak data center tampak dingin saat belum penuh, tetapi gagal saat beban IT naik. Karena itu, *thermal load test* penting.

Pengujian cooling mencakup:

- Suhu *supply air*.
- Suhu *return air*.
- Suhu *inlet* rak.
- Suhu *outlet* rak.
- RH dan *dew point*.
- Aliran udara.
- *Bypass air*.
- *Recirculation*.
- Kinerja CRAC/CRAH.
- Kinerja chiller/pump/cooling tower.
- Alarm suhu.
- Sensor kebocoran.
- Failover cooling saat satu unit gagal.

ASHRAE memiliki panduan commissioning yang berbasis Guideline 0 dan Standard 202 untuk membantu pemilik, desainer, dan manajer proyek melakukan commissioning konstruksi baru secara bertahap dan terdokumentasi ([ASHRAE](#)). Untuk data center, prinsip ini penting karena cooling harus memenuhi desain operasi, bukan hanya menyala.

Skenario minimum cooling:

- Semua unit cooling normal.
- Satu unit cooling dimatikan.
- Beban panas dinaikkan dengan *load bank*.
- Alarm suhu diuji.
- Sensor *inlet* rak diverifikasi.
- Kelembaban dan *dew point* dipantau.
- Sistem kembali normal setelah failover.

Catatan tajam: cooling yang belum diuji dengan beban panas belum layak disebut siap produksi.

10.5 Testing Network: Redundansi, Throughput, Failover

Jaringan harus diuji sebagai jalur layanan, bukan hanya dicek “link up”. Pengujian harus memastikan koneksi antar-rak, antar-zona, ke storage, ke backup, ke manajemen, dan ke DCI berjalan sesuai desain.

Pengujian jaringan mencakup:

- Redundansi link.
- Redundansi perangkat.
- *Throughput*.
- *Latency*.
- Packet loss.
- Routing convergence.
- Segmentasi VLAN/VRF/VNI.
- Firewall policy.
- DCI failover.
- OOB management.
- Telemetry dan log.

Untuk jaringan modern, proses *commissioning* juga harus memverifikasi konfigurasi dasar seperti nama perangkat, waktu/NTP, manajemen remote, alamat manajemen, loopback, VTEP, routing underlay, dan koneksi leaf-spine. Buku *Cloud Data Center Network Architectures and Technologies* menempatkan commissioning interkoneksi sebagai bagian dari deployment jaringan data center, termasuk konfigurasi perangkat dasar, interface interkoneksi, loopback/VTEP, routing underlay, dan mekanisme reliabilitas seperti M-LAG .

Kalimat kunci: jaringan yang baik bukan hanya tersambung, tetapi **tetap tersambung saat satu jalur gagal**.

10.6 Testing Security: Akses, Log, Alarm, Incident Drill

Keamanan juga harus diuji. Banyak fasilitas memiliki access control, CCTV, firewall, alarm, dan logging, tetapi tidak pernah menguji apakah semua bekerja saat insiden.

Pengujian security mencakup:

- Kartu akses diterima/ditolak sesuai hak.
- Pintu terbuka terlalu lama menghasilkan alarm.
- CCTV merekam area kritikal.
- Visitor log berjalan.
- Rack lock berfungsi.
- Firewall policy sesuai segmentasi.
- Login admin tercatat.
- Log dikirim ke sistem pencatatan.
- Alarm OT muncul di dashboard.
- Simulasi insiden dilakukan.

Contoh *incident drill*:

- Vendor mencoba masuk ruang komputer tanpa pendamping.
- Alarm pintu ruang UPS berbunyi.
- Satu akun admin gagal login berulang.
- Satu segmen jaringan mencoba akses ke database yang tidak diizinkan.
- Sensor leak detection aktif.
- Cooling alarm muncul.

Prinsip: keamanan yang tidak diuji biasanya terlihat baik sampai insiden pertama terjadi.

10.7 Integrated System Test atau IST

IST adalah pengujian terpenting sebelum *go-live*. Pada IST, sistem tidak diuji sendiri-sendiri, tetapi diuji sebagai satu kesatuan: power, cooling, network, security, monitoring, dan operasi manusia. Tujuannya membuktikan bahwa fasilitas benar-benar bekerja sesuai desain saat menghadapi skenario nyata.

Data Center Handbook menyebut L5 atau IST sebagai tahap yang kini umum pada proyek data center. Namun buku tersebut juga memberi peringatan penting: IST sering masih menjadi domain tim proyek dan hanya sedikit melibatkan tim operasi, sehingga kesempatan transfer pengetahuan dari konstruksi ke operasi dapat hilang .

Contoh skenario IST:

1. **Utility power loss**
Listrik utama diputus secara terkontrol. UPS mengambil beban. Generator menyala. ATS berpindah. Cooling tetap berjalan. Monitoring mencatat semua event.
2. **Generator failure**
Generator utama gagal. Generator cadangan mengambil alih jika desain mendukung. Alarm muncul. Tim operasi menjalankan EOP.
3. **Cooling unit failure**
Satu CRAC/CRAH/chiller dimatikan. Sistem cooling cadangan mengambil alih. Suhu *inlet* rak tetap dalam batas aman.
4. **Network path failure**
Satu link atau satu perangkat jaringan dimatikan. Trafik berpindah ke jalur lain. Tidak ada gangguan layanan kritikal.
5. **Security alarm event**
Akses tidak sah disimulasikan. Alarm muncul. CCTV, access log, dan prosedur respons diverifikasi.

Catatan kritis: IST harus melibatkan tim operasi, bukan hanya kontraktor. Jika tim operasi tidak ikut IST, mereka akan kehilangan pelajaran paling penting: **bagaimana sistem berperilaku saat gagal**.

10.8 Dokumentasi As-Built

Dokumentasi *as-built* adalah catatan kondisi aktual setelah instalasi. Dokumen ini sering berbeda dari desain awal karena perubahan lapangan. Tanpa *as-built*, tim operasi bekerja dengan peta yang salah.

Dokumen *as-built* minimum:

- Layout ruang aktual.
- Posisi rak aktual.
- Jalur kabel data.
- Jalur kabel power.
- *Single line diagram* listrik.
- Diagram cooling.
- Diagram jaringan.
- Daftar panel dan breaker.
- Daftar PDU dan rack PDU.
- Tabel port jaringan.
- Tabel VLAN/VRF/VNI.
- Daftar IP manajemen.
- Daftar sensor.
- Daftar perangkat.
- Foto instalasi.
- Hasil FAT/SAT/IST.
- Daftar *snag list* dan status penyelesaian.

Data Center Handbook mengingatkan bahwa ketiadaan dokumentasi commissioning, IST, SOP/EOP/ARP, dan gambar yang tidak terindeks dapat meningkatkan risiko kegagalan operasi, karena tim tidak tahu bagaimana sistem bekerja atau bagaimana merespons kegagalan .

Kalimat tajam: dokumen *as-built* bukan arsip proyek; ia adalah **alat keselamatan operasi**.

10.9 Handover ke Operasi

Handover adalah proses serah terima formal dari tim proyek ke tim operasi. Fasilitas tidak boleh diserahterimakan hanya dengan kunci ruangan dan dokumen tebal. Tim operasi harus memahami sistem, prosedur, risiko, alarm, batas kapasitas, dan skenario kegagalan.

Isi *handover*:

- Dokumen desain final.
- Dokumen *as-built*.
- Laporan FAT, SAT, IST.
- SOP, MOP, EOP.
- Daftar aset.
- Daftar warranty.
- Kontrak maintenance.
- Jadwal preventive maintenance.
- Daftar vendor dan kontak darurat.
- Daftar akun dan hak akses.
- Training record.
- Daftar isu terbuka.
- Berita acara serah terima.

Data Center Handbook menekankan bahwa pelatihan tidak boleh berhenti setelah pelatihan awal; pembelajaran harus berlangsung sepanjang umur operasi fasilitas dan harus spesifik terhadap sistem yang terpasang di lokasi .

Prinsip penting: *handover* yang gagal akan membuat data center baru menjadi fasilitas lama yang penuh risiko sejak hari pertama.

10.10 Go-Live Checklist

±0,5 halaman

Go-live adalah keputusan manajemen dan teknis bahwa fasilitas siap menanggung beban produksi. Keputusan ini harus berbasis bukti, bukan tekanan jadwal.

Sebelum *go-live*, pastikan:

- FAT selesai.
- SAT selesai.
- IST selesai.
- Semua isu kritikal ditutup.
- *As-built* tersedia.
- SOP/MOP/EOP tersedia.
- Monitoring aktif.
- Alarm diuji.
- Tim operasi dilatih.
- Vendor standby.
- Spare part kritikal tersedia.
- Backup dan DR diuji.
- Security access aktif.
- Kapasitas power dan cooling sesuai desain.
- Persetujuan formal diberikan.

Kalimat kunci: *go-live* bukan akhir proyek; *go-live* adalah awal tanggung jawab operasi.

Materi Praktek 1: Template *Commissioning Plan*

Bagian	Isi yang Harus Disiapkan
Nama proyek	...
Lokasi	...
Pemilik proyek	...
Target sertifikasi	ISO/IEC 22237 / Uptime / TIA-942 / lainnya
Ruang lingkup	Power / cooling / network / security / monitoring / OT
Tim commissioning	Owner, konsultan, kontraktor, vendor, operasi
Daftar sistem kritikal	UPS, generator, ATS, chiller, CRAH, network, security
Level pengujian	L1 FAT, L2 instalasi, L3 SAT, L4 sistem, L5 IST
Skenario uji	Utility failure, cooling failure, network failure, security event
Alat uji	Load bank, thermal sensor, power meter, network tester
Kriteria lulus	Parameter teknis, batas suhu, uptime, alarm, log
Bukti yang dikumpulkan	Foto, log, grafik, hasil ukur, berita acara
Risiko pengujian	Dampak ke perangkat, keselamatan, jadwal, vendor
Rencana rollback	Langkah kembali ke kondisi aman
Jadwal	Tanggal, durasi, penanggung jawab
Persetujuan	Owner, operasi, konsultan, kontraktor

Catatan: commissioning plan harus diperbarui saat proyek berjalan, karena kondisi lapangan dan temuan pengujian dapat berubah. *Data Center Handbook* menekankan bahwa commissioning plan adalah proses iteratif yang perlu ditinjau dan diperbarui secara berkala selama instalasi berlangsung .

Materi Praktek 2: Contoh Skenario *Integrated System Test*

Skenario: Utility Power Failure

Tujuan: membuktikan data center tetap berjalan saat listrik utama gagal.

Langkah	Aksi	Hasil yang Diharapkan	Bukti
1	Pastikan beban simulasi aktif	Beban stabil	Data load bank
2	Putuskan utility secara terkontrol	UPS mengambil beban	Log UPS
3	Generator start otomatis	Generator hidup sesuai waktu desain	Log generator
4	ATS pindah ke generator	Beban kritikal tersuplai	Log ATS
5	Pantau cooling	Suhu tetap aman	Grafik suhu
6	Pantau network	Tidak ada link kritikal down	Log jaringan
7	Pantau security	Alarm dan CCTV tetap aktif	Log security
8	Kembalikan utility	Transfer kembali normal	Log sistem
9	Review semua alarm	Semua event tercatat	Laporan IST
10	Catat anomali	Tindakan koreksi dibuat	Punch list

Kriteria Lulus

- Tidak ada beban kritikal mati.
- UPS bekerja sesuai desain.
- Generator start dan stabil.
- ATS bekerja benar.
- Cooling tetap menjaga suhu aman.
- Monitoring mencatat semua event.
- Tim operasi menjalankan prosedur dengan benar.
- Semua bukti tersimpan.

Catatan: skenario harus dilakukan dengan keselamatan ketat dan disetujui seluruh pihak sebelum dijalankan.

Materi Praktek 3: Checklist FAT/SAT

Area	FAT	SAT
Dokumen teknis tersedia	Ya / Tidak	Ya / Tidak
Spesifikasi sesuai kontrak	Ya / Tidak	Ya / Tidak
Sertifikat perangkat tersedia	Ya / Tidak	Ya / Tidak
Pengujian fungsi dasar	Ya / Tidak	Ya / Tidak
Pengujian alarm	Ya / Tidak	Ya / Tidak
Pengujian proteksi	Ya / Tidak	Ya / Tidak
Label perangkat benar	Ya / Tidak	Ya / Tidak
Kondisi fisik baik	Ya / Tidak	Ya / Tidak
Instalasi sesuai gambar	-	Ya / Tidak
Koneksi kabel benar	-	Ya / Tidak
Grounding benar	-	Ya / Tidak
Integrasi ke monitoring	-	Ya / Tidak
Dokumentasi hasil uji	Ya / Tidak	Ya / Tidak
Daftar temuan dibuat	Ya / Tidak	Ya / Tidak
Temuan kritikal ditutup	Ya / Tidak	Ya / Tidak
Berita acara ditandatangani	Ya / Tidak	Ya / Tidak

Prinsip: FAT mencegah perangkat salah masuk proyek. SAT mencegah perangkat salah masuk operasi.

Materi Praktek 4: Checklist Dokumen *As-Built*

Dokumen	Status
Layout ruang final	Ada / Tidak
Posisi rak final	Ada / Tidak
Jalur kabel data	Ada / Tidak
Jalur kabel power	Ada / Tidak
Single line diagram listrik	Ada / Tidak
Diagram UPS dan baterai	Ada / Tidak
Diagram generator dan ATS	Ada / Tidak
Diagram cooling	Ada / Tidak
Diagram jaringan fisik	Ada / Tidak
Diagram jaringan logis	Ada / Tidak
Daftar VLAN/VRF/VNI	Ada / Tidak
Daftar IP manajemen	Ada / Tidak
Daftar PDU dan beban	Ada / Tidak
Daftar sensor	Ada / Tidak
Foto instalasi	Ada / Tidak
Laporan FAT	Ada / Tidak
Laporan SAT	Ada / Tidak
Laporan IST	Ada / Tidak
SOP/MOP/EOP	Ada / Tidak
Daftar aset	Ada / Tidak
Daftar vendor dan kontak darurat	Ada / Tidak
Daftar isu terbuka	Ada / Tidak

Catatan tajam: tanpa *as-built*, setiap maintenance berubah menjadi investigasi.

Materi Praktek 5: Template Berita Acara Serah Terima

Berita Acara Serah Terima Data Center

1. Nama Proyek:

...

2. Lokasi:

...

3. Tanggal Serah Terima:

...

4. Pihak yang Menyerahkan:

...

5. Pihak yang Menerima:

...

6. Ruang Lingkup Serah Terima:

Power / cooling / network / security / monitoring / ruang / dokumentasi / operasi.

7. Dokumen yang Diserahkan:

- Dokumen desain final
- Dokumen *as-built*
- Laporan FAT
- Laporan SAT
- Laporan IST
- SOP/MOP/EOP
- Daftar aset
- Kontrak maintenance
- Daftar akun dan akses
- Daftar vendor
- Jadwal preventive maintenance

8. Status Pengujian:

FAT: lulus / belum

SAT: lulus / belum

IST: lulus / belum

9. Daftar Isu Tersisa:

No	Isu	Dampak	Target Penyelesaian	PIC
1				

10. Pernyataan:

Fasilitas telah diperiksa, diuji, didokumentasikan, dan diserahkan kepada tim operasi dengan catatan sebagaimana tercantum dalam berita acara ini.

11. Tanda Tangan:

Pihak menyerahkan / pihak menerima / saksi / konsultan.

Ringkasan Bab 10

Bab ini menegaskan bahwa *deployment* data center tidak selesai saat perangkat menyala. Data center baru layak masuk produksi setelah melewati **FAT, SAT, pengujian power, cooling, network, security, IST, dokumentasi as-built, pelatihan operasi, dan handover formal**.

ASHRAE menempatkan commissioning sebagai proses berbasis kualitas untuk memastikan sistem direncanakan, dirancang, dipasang, diuji, dioperasikan, dan dipelihara sesuai kebutuhan pemilik proyek ([ASHRAE](#)). TIA-942 juga menekankan bahwa standar data center mencakup infrastruktur fisik seperti lokasi, arsitektur, elektrik, mekanik, keselamatan kebakaran, telekomunikasi, keamanan, dan persyaratan lain; karena itu testing dan commissioning harus dilihat lintas disiplin, bukan per sistem saja ([TIA Online](#)).

Inti bab: data center siap produksi hanya jika sistemnya sudah diuji, timnya sudah dilatih, dokumennya lengkap, dan risikonya tercatat.

Checklist Akhir Bab 10

Sebelum masuk Bab 11, pembaca harus mampu menjawab:

- Apakah *deployment plan* sudah disetujui?
- Apakah FAT selesai untuk perangkat kritikal?
- Apakah SAT selesai setelah perangkat terpasang?
- Apakah UPS, generator, ATS, dan *load bank* sudah diuji?
- Apakah cooling diuji dengan beban panas?
- Apakah failover cooling diuji?
- Apakah jaringan diuji untuk redundansi dan throughput?
- Apakah segmentasi dan security alarm diuji?
- Apakah IST dilakukan lintas sistem?
- Apakah tim operasi ikut IST?
- Apakah semua alarm dan log tercatat?
- Apakah dokumen *as-built* lengkap?
- Apakah SOP, MOP, dan EOP tersedia?
- Apakah pelatihan operasi selesai?
- Apakah *handover* dilakukan formal?
- Apakah *go-live checklist* ditandatangani?
- Apakah semua bukti siap untuk **audit dan sertifikasi**?

Penutup bab: Data center profesional tidak masuk operasi karena proyek ingin selesai, tetapi karena **sistem telah dibuktikan, risiko telah diuji, dokumen telah lengkap, dan tim operasi telah siap bertanggung jawab.**

Bab 11. Operasi, DCIM, Monitoring, Maintenance, dan Capacity Review

Golden Rule: Data center yang baik bukan hanya yang berhasil dibangun, tetapi yang stabil, terukur, terdokumentasi, dan terus diperbaiki.

Bab ini membahas fase paling panjang dalam hidup *data center*: operasi harian. Dalam outline buku, Bab 11 diarahkan untuk membahas operasi harian, SOP, MOP, EOP, *preventive* dan *predictive maintenance*, DCIM, monitoring, sensor, *capacity management*, *change management*, *incident management*, laporan bulanan, serta review PUE, SLA, risiko, dan kapasitas .

Inti bab ini: **sertifikasi tidak berhenti saat fasilitas selesai dibangun. Sertifikasi yang sehat harus terlihat dalam operasi harian, bukti monitoring, disiplin maintenance, dan laporan berkala.**

11.1 Operasi Harian Data Center

Operasi harian adalah rutinitas kecil yang menjaga fasilitas tetap stabil. Banyak insiden besar berawal dari hal sederhana: suhu naik tidak dicatat, baterai UPS melemah tidak ditindaklanjuti, alarm dianggap biasa, kabel berubah tanpa catatan, atau kapasitas rak penuh tanpa peringatan.

Uptime Institute menekankan bahwa Praktek operasi buruk dapat lebih berisiko daripada desain infrastruktur itu sendiri; *Tier Certification of Operational Sustainability* menilai Praktek organisasi, staffing, maintenance, operasi, manajemen, dan perencanaan agar selaras dengan pengurangan risiko, pengurangan *downtime*, dan efisiensi operasi. ([Uptime Institute](#))

Aktivitas operasi harian mencakup:

- Memeriksa alarm power, cooling, network, security, dan lingkungan.
- Memeriksa suhu, kelembapan, dan *dew point*.
- Memeriksa status UPS, generator, PDU, CRAC/CRAH, chiller, sensor kebocoran.
- Memeriksa akses fisik dan log tamu.
- Memeriksa dashboard kapasitas rak, power, cooling, dan port jaringan.
- Mencatat perubahan, insiden, dan pekerjaan vendor.
- Melakukan eskalasi jika ada parameter melewati ambang batas.

Prinsip operasi: yang penting bukan hanya mengecek, tetapi **mencatat, menganalisis, dan menindaklanjuti.**

11.2 SOP, MOP, EOP

Operasi profesional membutuhkan tiga jenis dokumen utama: SOP, MOP, dan EOP.

SOP atau *Standard Operating Procedure* adalah prosedur rutin. Contohnya pemeriksaan harian, pengecekan suhu, pemeriksaan akses, pencatatan alarm, dan laporan shift.

MOP atau *Method of Procedure* adalah prosedur kerja terencana untuk aktivitas yang berisiko. Contohnya mengganti PDU, memindahkan kabel trunk, melakukan maintenance UPS, menambah rak, atau mengubah konfigurasi jaringan.

EOP atau *Emergency Operating Procedure* adalah prosedur darurat. Contohnya listrik utama mati, UPS alarm, generator gagal start, cooling gagal, suhu ruang naik, kebocoran air, kebakaran, atau insiden keamanan.

Perbedaan ringkas:

Dokumen	Fungsi	Contoh
SOP	Operasi rutin	Pemeriksaan harian suhu, UPS, akses
MOP	Pekerjaan terencana	Maintenance UPS, tambah rack PDU
EOP	Kondisi darurat	Listrik mati, cooling gagal, alarm kebakaran

Aturan praktis: SOP menjaga stabilitas, MOP mengendalikan perubahan, EOP menyelamatkan layanan saat krisis.

Catatan tajam: tim yang hanya mengandalkan pengalaman senior akan rapuh. Saat orang kunci tidak ada, operasi harus tetap berjalan berdasarkan prosedur tertulis.

11.3 Preventive dan Predictive Maintenance

Preventive maintenance adalah perawatan terjadwal untuk mencegah kerusakan. Contohnya membersihkan filter, menguji baterai UPS, memeriksa koneksi panel, menguji generator, mengecek sensor kebocoran, menguji alarm, dan inspeksi thermal panel.

Predictive maintenance lebih maju. Perawatan dilakukan berdasarkan tren data: suhu naik perlahan, getaran motor berubah, arus listrik meningkat, efisiensi cooling menurun, baterai mulai melemah, atau alarm kecil sering muncul. Tujuannya adalah mendeteksi kegagalan sebelum terjadi.

ASHRAE TC 9.9 dibentuk untuk membahas fasilitas *mission critical*, ruang teknologi, desain, operasi, maintenance, dan penggunaan energi yang efisien pada data center dan ruang teknologi modern. ([ASHRAE](#)) Ini menegaskan bahwa maintenance bukan pekerjaan tambahan, tetapi bagian dari operasi kritikal.

Contoh jadwal maintenance:

Sistem	Harian	Bulanan	Triwulanan	Tahunan
UPS	Cek alarm	Cek beban	Uji baterai	Service penuh
Generator	Cek status	Start test	Load test	Overhaul ringan
Cooling	Cek suhu	Bersihkan filter	Cek coil/pump	Service besar
PDU	Cek beban	Cek koneksi	Thermal scan	Audit panel
Sensor	Cek alarm	Uji fungsi	Kalibrasi selektif	Kalibrasi penuh

Prinsip: maintenance harus menghasilkan **bukti**, bukan hanya tanda centang.

11.4 DCIM dan Monitoring

DCIM atau *Data Center Infrastructure Management* adalah sistem untuk mengelola aset, kapasitas, energi, ruang, cooling, sensor, workflow, reporting, dan dashboard. DCIM membantu tim operasi melihat *data center* sebagai sistem terpadu, bukan kumpulan perangkat terpisah.

Data Center Handbook menyebut DCIM sebagai solusi manajemen bisnis untuk perencanaan sumber daya dan kapasitas data center. DCIM mengintegrasikan monitoring, *capacity planning*, basis data konfigurasi, sensor lingkungan, data management, reporting, power management, cooling, BMS alarm, asset configuration, change, dan workflow .

Fungsi utama DCIM mencakup:

- **Asset management:** daftar rak, perangkat, serial number, lokasi, koneksi.
- **Capacity management:** ruang, U, berat, port, power, cooling.
- **Real-time monitoring:** suhu, kelembaban, power, alarm.
- **Reporting:** tren energi, kapasitas, insiden, biaya.
- **Floor visualization:** peta ruang, rak, CRAC/CRAH, status kapasitas.
- **Simulation:** skenario power failure, cooling failure, penambahan perangkat.
- **Workflow:** tiket perubahan dan dokumentasi pekerjaan.
- **API/integrasi:** koneksi ke sistem monitoring, ITSM, BMS, dan sensor.

Brochard dkk. menjelaskan DCIM dapat mencakup *asset management*, *capacity management*, *real-time monitoring and alerting*, *trends and reporting*, visualisasi lantai data center, simulasi, workflow, remote control, API, dan antarmuka berbasis web/mobile .

Kalimat kunci: DCIM bukan sekadar dashboard; DCIM adalah sistem memori operasi data center.

11.5 Sensor: Suhu, Kelembaban, Air Flow, Power, Leak Detection

Sensor adalah mata dan telinga operasi. Tanpa sensor, tim hanya tahu masalah setelah dampaknya terasa. Sensor harus dipasang di lokasi yang tepat, diberi ambang batas, dikalibrasi, dan dihubungkan ke alarm.

Sensor minimum:

- Suhu *inlet* rak.
- Suhu *outlet* rak.
- Kelembaban.
- *Dew point*.
- *Airflow* atau tekanan diferensial.
- Power per rak / PDU.
- Status UPS.
- Status generator.
- Status CRAC/CRAH.
- *Leak detection*.
- Alarm pintu.
- Status CCTV/access control.

ASHRAE mengingatkan bahwa peningkatan temperatur operasi dapat mempengaruhi reliabilitas peralatan, termasuk peralatan daya yang berada pada ruang atau aliran udara yang sama dengan perangkat TI ([ASHRAE](#)). Karena itu, sensor suhu tidak boleh hanya berada di dinding ruang. Sensor harus dekat dengan titik risiko: depan rak, belakang rak, jalur cooling, panel, dan area kebocoran.

Prinsip: sensor tanpa alarm, alarm tanpa prosedur, dan prosedur tanpa tindak lanjut sama-sama tidak cukup.

11.6 Capacity Management

Capacity management adalah proses memastikan data center memiliki kapasitas cukup untuk layanan sekarang dan pertumbuhan masa depan. Kapasitas yang harus dipantau bukan hanya jumlah rak kosong. Kapasitas mencakup **space, power, cooling, network port, storage, UPS, generator, dan SDM operasi**.

DCIM membantu mencegah *stranded capacity*: kapasitas yang terlihat tersedia tetapi tidak bisa dipakai karena bottleneck di sistem lain. Brochard dkk. menjelaskan bahwa DCIM dapat memberi tahu apakah masih ada ruang, port jaringan, soket listrik, kapasitas berat rak, power supply, atau cooling untuk menambah perangkat baru .

Pertanyaan *capacity review*:

- Berapa U kosong yang benar-benar bisa dipakai?
- Berapa kW tersisa per rak?
- Berapa kapasitas cooling tersisa?
- Berapa port jaringan tersisa?
- Berapa kapasitas UPS dan generator tersisa?
- Apakah ada rak kosong tetapi tidak punya daya/cooling?
- Kapan kapasitas akan habis jika tren sekarang berlanjut?

Kalimat tajam: rak kosong bukan berarti kapasitas tersedia.

11.7 Change Management

Setiap perubahan di data center harus dikendalikan. Perubahan kecil seperti memindahkan kabel, menambah server, mengganti PDU, mengubah firewall rule, atau menaikkan set point cooling dapat berdampak besar.

Proses *change management* minimum:

1. Permintaan perubahan.
2. Analisis risiko.
3. Persetujuan.
4. Jadwal kerja.
5. MOP.
6. Rencana rollback.
7. Komunikasi ke pihak terkait.
8. Eksekusi.
9. Validasi.
10. Pembaruan dokumentasi.
11. Penutupan perubahan.

Data Center Virtualization Fundamentals menunjukkan bahwa provisioning server melibatkan banyak domain: fasilitas, power, cooling, kabel, jaringan, storage, firmware, sistem, dan aplikasi. Karena itu, perubahan yang tampak “hanya server” sebenarnya dapat menyentuh banyak tim dan kontrol operasi .

Prinsip: perubahan tanpa MOP adalah eksperimen di fasilitas produksi.

11.8 Incident Management

Insiden adalah kejadian yang mengganggu atau berpotensi mengganggu layanan. Insiden dapat berupa suhu naik, UPS alarm, link down, akses tidak sah, kebocoran air, generator gagal start, atau kesalahan operator.

Siklus *incident management*:

- Deteksi.
- Klasifikasi prioritas.
- Eskalasi.
- Tindakan sementara.
- Pemulihan.
- Komunikasi.
- Dokumentasi.
- Analisis akar masalah.
- Perbaikan permanen.
- *Lessons learned*.

Uptime Institute menyatakan *Management and Operations Guideline* menilai perilaku operasi yang berdampak pada kemampuan data center memenuhi tujuan bisnis dan performa, mencakup aktivitas harian serta perencanaan dan pengambilan keputusan di tingkat hulu ([Uptime Institute](#)).

Kalimat kunci: insiden yang tidak dianalisis akan kembali sebagai insiden yang lebih mahal.

11.9 Laporan Bulanan Operasi

Laporan bulanan adalah alat manajemen. Laporan ini menunjukkan apakah data center stabil, efisien, aman, dan siap tumbuh. Laporan tidak boleh hanya berisi narasi umum. Ia harus berisi angka, tren, temuan, risiko, dan keputusan yang dibutuhkan.

Isi laporan bulanan:

- Ringkasan SLA.
- Insiden dan durasi.
- Alarm kritikal.
- Perubahan yang dilakukan.
- PUE bulanan.
- Konsumsi energi.
- Suhu dan kelembaban.
- Kapasitas rak, power, cooling, port.
- Maintenance yang selesai.
- Maintenance yang terlambat.
- Temuan keamanan.
- Risiko baru.
- Rekomendasi.
- Keputusan yang dibutuhkan manajemen.

DCIM memiliki peran penting dalam reporting. *Data Center Handbook* menjelaskan bahwa reporting mengubah data mentah menjadi informasi berdampak bisnis, sedangkan dashboard menyajikan informasi besar secara ringkas agar cepat dipahami dan dapat ditindaklanjuti .

Prinsip: laporan operasi harus membantu manajemen mengambil keputusan, bukan hanya memenuhi administrasi.

11.10 Review PUE, SLA, Risiko, dan Kapasitas

Review berkala memastikan data center tidak berjalan dengan asumsi lama. Beban berubah. Perangkat berubah. Risiko berubah. Tarif listrik berubah. Tim berubah. Standar berubah.

ISO/IEC 22237 menjelaskan prinsip umum fasilitas data center dan klasifikasi berdasarkan *availability*, *security*, dan *energy-efficiency* sepanjang umur rencana fasilitas ([ISO](#)). Artinya, review operasi harus melihat ketiganya: ketersediaan, keamanan, dan efisiensi.

Review minimum:

- **PUE**: apakah efisiensi membaik atau memburuk?
- **SLA**: apakah layanan memenuhi target?
- **Risiko**: apakah ada risiko baru?
- **Kapasitas**: kapan power/cooling/space/network habis?
- **Maintenance**: apakah ada pekerjaan tertunda?
- **Security**: apakah akses dan log ditinjau?
- **Incident trend**: apakah ada pola berulang?
- **Audit evidence**: apakah bukti siap diperiksa?

Kalimat tajam: data center yang tidak direview akan menua diam-diam sampai gagal.

Materi Praktek 1: Template SOP Operasi Harian

SOP Operasi Harian Data Center

Tujuan: memastikan kondisi fasilitas stabil, aman, dan terdokumentasi setiap hari.

No	Aktivitas	Parameter	Batas Aman	Bukti
1	Cek alarm utama	Power/cooling/network/security	Tidak ada alarm kritikal	Screenshot dashboard
2	Cek suhu inlet rak	°C	Sesuai standar internal	Log sensor
3	Cek kelembapan	RH / dew point	Sesuai batas operasi	Log sensor
4	Cek UPS	Beban, baterai, alarm	Normal	Log UPS
5	Cek generator	Status, bahan bakar	Siap operasi	Checklist
6	Cek PDU/rack PDU	Beban per jalur	Tidak overload	Log PDU
7	Cek CRAC/CRAH	Status unit	Normal	Dashboard cooling
8	Cek leak detection	Alarm air	Tidak ada alarm	Log sensor
9	Cek access log	Akses ruang kritikal	Sesuai izin	Log akses
10	Catat kejadian shift	Insiden/perubahan/vendor	Lengkap	Shift report

Output: laporan shift harian, daftar alarm, daftar tindakan, dan eskalasi jika ada anomali.

Materi Praktek 2: Template MOP Pekerjaan Kritis

MOP — Method of Procedure

Nama pekerjaan:

Contoh: penggantian rack PDU jalur A pada Rack DC1-A03.

Tujuan:

...

Tanggal dan waktu:

...

PIC:

...

Tim terkait:

Facility / network / server / security / vendor / operasi.

Risiko utama:

- Beban mati.
- Salah cabut kabel.
- Jalur A/B tidak seimbang.
- Alarm tidak ditangani.
- Dokumentasi tidak diperbarui.

Persiapan:

- Cek beban perangkat.
- Pastikan perangkat memiliki jalur B aktif.
- Backup konfigurasi jika terkait perangkat aktif.
- Siapkan alat dan label.
- Komunikasikan jadwal.
- Siapkan rollback.

Langkah kerja:

No	Langkah	PIC	Status
1	Validasi beban jalur A/B		
2	Konfirmasi perangkat aman di jalur B		
3	Lepas beban dari PDU lama		
4	Pasang PDU baru		
5	Sambungkan perangkat sesuai label		
6	Verifikasi beban		
7	Update dokumentasi		

Rollback:

...

Validasi setelah pekerjaan:

Alarm normal, beban seimbang, perangkat hidup, dokumentasi diperbarui.

Persetujuan penutupan:

...

Materi Praktek 3: Template EOP Ketika Listrik Mati, UPS Alarm, Cooling Gagal

EOP 1 — Listrik Utama Mati

Tanda awal: utility alarm, UPS on battery, generator start.

Langkah:

1. Pastikan UPS mengambil beban.
2. Pantau *runtime* UPS.
3. Pastikan generator start.
4. Pastikan ATS berpindah.
5. Pantau cooling.
6. Eskalasi ke facility lead.
7. Komunikasikan status ke manajemen.
8. Catat waktu kejadian.
9. Setelah utility kembali, pantau transfer balik.
10. Buat laporan insiden.

EOP 2 — UPS Alarm

Tanda awal: alarm baterai, overload, bypass, fault.

Langkah:

1. Identifikasi jenis alarm.
2. Cek beban UPS.
3. Cek status baterai.
4. Cek apakah beban kritis terdampak.
5. Jangan melakukan bypass tanpa persetujuan.
6. Eskalasi ke teknisi listrik/vendor.
7. Siapkan rencana pengurangan beban jika overload.
8. Catat tindakan dan waktu.
9. Setelah normal, lakukan RCA.

EOP 3 — Cooling Gagal

Tanda awal: suhu *inlet* naik, CRAC/CRAH alarm, chiller/pump alarm.

Langkah:

1. Identifikasi zona terdampak.
2. Cek suhu *inlet* rak kritikal.
3. Cek unit cooling cadangan.
4. Kurangi beban non-kritikal jika perlu.
5. Pastikan airflow tidak terhalang.
6. Eskalasi ke facility lead.
7. Pantau suhu setiap 5 menit.
8. Siapkan shutdown terkontrol jika suhu melewati batas.
9. Setelah normal, dokumentasikan penyebab dan perbaikan.

Prinsip EOP: cepat, aman, tercatat, dan tidak spekulatif.

Materi Praktek 4: Dashboard Minimum Operasi

Dashboard minimum harus mampu menunjukkan kondisi fasilitas secara cepat.

Area	Metrik Minimum	Tujuan
Power	Utility status, UPS load, battery, generator, PDU load	Mengetahui kesiapan listrik
Cooling	CRAC/CRAH status, chiller, supply/return temp	Menjaga termal
Temperature	Inlet rack atas/tengah/bawah	Deteksi hot spot
Humidity	RH dan dew point	Cegah ESD/kondensasi
Rack Capacity	U kosong, kW/rack, berat, port	Cegah kapasitas semu
Network	Link status, latency, error, DCI	Jaga konektivitas
Security	Access log, door alarm, CCTV status	Kontrol akses
Incident	Alarm aktif, tiket terbuka, SLA	Fokus tindakan
Energy	PUE, kWh, biaya energi	Efisiensi operasi
Maintenance	Jadwal dan overdue task	Cegah perawatan tertunda

Catatan: dashboard harus memiliki ambang batas, alarm, pemilik tindakan, dan histori. Tanpa itu, dashboard hanya tampilan.

Materi Praktek 5: Checklist *Capacity Review* Triwulanan

Area	Pertanyaan Review	Status
Space	Berapa rack kosong yang benar-benar bisa dipakai?	Aman / Waspada / Kritis
Rack U	Berapa U tersedia per zona?	Aman / Waspada / Kritis
Power	Berapa kW tersedia per rak dan per jalur?	Aman / Waspada / Kritis
UPS	Berapa kapasitas UPS tersisa?	Aman / Waspada / Kritis
Generator	Apakah generator cukup untuk beban terbaru?	Aman / Waspada / Kritis
Cooling	Berapa kapasitas cooling tersisa?	Aman / Waspada / Kritis
Thermal	Apakah ada hot spot berulang?	Aman / Waspada / Kritis
Network	Apakah port dan bandwidth cukup?	Aman / Waspada / Kritis
Storage	Apakah kapasitas storage dan backup cukup?	Aman / Waspada / Kritis
PUE	Apakah PUE membaik atau memburuk?	Aman / Waspada / Kritis
SLA	Apakah target layanan tercapai?	Aman / Waspada / Kritis
Incident	Apakah ada pola insiden berulang?	Aman / Waspada / Kritis
Maintenance	Apakah ada pekerjaan tertunda?	Aman / Waspada / Kritis
Security	Apakah akses dan akun sudah direview?	Aman / Waspada / Kritis
Risiko	Risiko baru apa yang muncul?	Catatan
Keputusan	Ekspansi / optimasi / mitigasi apa yang perlu dilakukan?	Catatan

Output review: daftar risiko kapasitas, estimasi waktu kapasitas habis, keputusan ekspansi, dan kebutuhan anggaran.

Ringkasan Bab 11

Bab ini menegaskan bahwa operasi *data center* adalah disiplin jangka panjang. Fasilitas yang bagus saat serah terima bisa cepat menjadi rapuh jika SOP tidak dijalankan, MOP tidak dipakai, EOP tidak dilatih, maintenance tertunda, sensor tidak dikalibrasi, kapasitas tidak di review, dan dokumentasi tidak diperbarui.

DCIM menjadi alat penting karena dapat menggabungkan asset management, capacity planning, monitoring, reporting, visualisasi ruang, simulasi, workflow, dan integrasi data. *Data Center Handbook* menempatkan DCIM sebagai sistem strategis untuk mengelola kapasitas, aset, energi, operasi, dan kepatuhan. Brochard dkk. juga menekankan pentingnya mengintegrasikan data infrastruktur dan perangkat IT untuk optimasi operasi dinamis, termasuk konsumsi daya server, storage, dan perangkat jaringan.

Inti bab: operasi profesional berarti semua kondisi penting dipantau, semua perubahan dikendalikan, semua insiden dicatat, semua kapasitas di review, dan semua bukti siap diaudit.

Checklist Akhir Bab 11

Sebelum masuk Bab 12, pembaca harus mampu menjawab:

- Apakah SOP operasi harian tersedia dan dijalankan?
- Apakah MOP wajib untuk pekerjaan kritikal?
- Apakah EOP tersedia untuk listrik mati, UPS alarm, cooling gagal, kebocoran, dan insiden keamanan?
- Apakah preventive maintenance berjalan sesuai jadwal?
- Apakah predictive maintenance mulai memakai tren data?
- Apakah DCIM atau sistem setara mencatat aset, power, cooling, kapasitas, dan workflow?
- Apakah sensor suhu, kelembaban, air flow, power, dan leak detection aktif?
- Apakah alarm memiliki pemilik tindakan?
- Apakah kapasitas space, power, cooling, network, dan storage direview triwulanan?
- Apakah semua perubahan melewati *change management*?
- Apakah insiden dianalisis sampai akar masalah?
- Apakah laporan bulanan operasi dibuat?
- Apakah PUE, SLA, risiko, dan kapasitas direview?
- Apakah semua bukti operasi siap untuk **audit dan sertifikasi**?

Penutup bab: *Data center* professional tidak hanya kuat karena desainnya, tetapi karena operasinya disiplin, datanya akurat, maintenance-nya konsisten, dan perbaikannya tidak pernah berhenti.

Bab 12. Studi Kasus, Checklist Sertifikasi, dan Roadmap Profesional

Golden Rule: Professional data center dinilai bukan dari hafalan istilah, tetapi dari kemampuan mendesain, menghitung, membuktikan, mengoperasikan, dan mempertanggungjawabkan keputusan teknis.

Bab ini adalah penutup utama buku. Setelah pembaca mempelajari desain ruang, power, cooling, jaringan, keamanan, deployment, commissioning, dan operasi, Bab 12 menyatukan semuanya dalam bentuk **studi kasus, checklist sertifikasi, roadmap kompetensi, dan portofolio profesional**.

Dalam outline buku, Bab 12 memang diarahkan sebagai bab praktis yang memuat studi kasus 10 rack, retrofit data center lama, desain *edge data center*, checklist sertifikasi, peta kompetensi, roadmap belajar 6 bulan, serta kesalahan fatal yang sering menggagalkan sertifikasi. Fokusnya bukan menambah teori, tetapi membantu pembaca **berpikir seperti profesional yang siap diuji di lapangan**.

Standar yang perlu dijadikan rujukan lintas bab adalah ISO/IEC 22237, Uptime Tier, TIA-942, dan ASHRAE. ISO/IEC 22237 menekankan klasifikasi *availability*, *physical security*, dan *energy efficiency enablement*; Uptime Tier digunakan untuk menilai ketersediaan dan performa fasilitas; TIA-942 mencakup lokasi, telekomunikasi, arsitektur, listrik, mekanikal, keselamatan kebakaran, dan keamanan fisik; sedangkan ASHRAE TC 9.9 menjadi rujukan penting untuk lingkungan termal dan operasi ruang teknologi. ([Iteh Standards](#))

12.1 Studi Kasus 1: Membangun Data Center Kecil 10 Rack

Studi kasus pertama adalah membangun *data center* kecil 10 rack untuk organisasi profesional. Walaupun kecil, fasilitas ini tidak boleh diperlakukan seperti ruang server biasa. Justru pada skala kecil, disiplin desain harus dibangun sejak awal agar fasilitas tidak tumbuh liar.

Asumsi awal:

- Jumlah rack: **10 rack**
- Beban rata-rata: **5 kW/rack**
- Total *IT load*: **50 kW**
- Target PUE awal: **1,7**
- Total facility power: **85 kW**
- Margin desain: **20%**
- Daya desain awal: **±102 kW**
- Cooling awal: **±17 TR** setelah margin
- Target operasi: layanan internal penting, sebagian 24×7

Keputusan desain utama:

- Gunakan layout **hot aisle / cold aisle**.
- Siapkan UPS sesuai beban kritikal dan pertumbuhan.
- Siapkan generator jika layanan harus tetap hidup saat listrik utama mati.
- Gunakan monitoring suhu di *inlet* rack.
- Pisahkan jaringan produksi, manajemen, backup, dan keamanan.
- Siapkan SOP, MOP, EOP sejak hari pertama.
- Dokumentasikan rack, PDU, patch panel, kabel, IP, dan akses.

Bukti minimum untuk sertifikasi internal:

- *Data Center Design Brief*
- Perhitungan *IT load*
- Layout rack
- *Single line diagram*
- Diagram cooling
- Diagram jaringan
- Matriks risiko
- Checklist keamanan fisik
- Hasil FAT/SAT sederhana
- SOP operasi harian
- Log inspeksi

Pelajaran utama: data center kecil tetap harus punya disiplin besar. Jika dari 10 rack sudah tidak rapi, maka saat tumbuh menjadi 30 rack atau 50 rack, masalahnya akan berlipat.

12.2 Studi Kasus 2: Retrofit Data Center Lama agar Lebih Efisien

Studi kasus kedua adalah *retrofit* data center lama. Fasilitas lama biasanya masih berjalan, tetapi penuh masalah: kabel menumpuk, airflow buruk, PUE tinggi, dokumentasi lemah, sensor minim, dan kapasitas tidak jelas. Tujuan retrofit bukan membongkar semua, tetapi **memperbaiki risiko terbesar dengan gangguan minimum**.

Kondisi awal:

- Jumlah rack: 30 rack
- Beban rata-rata: 4–6 kW/rack
- PUE sekitar 2,0
- Banyak U kosong tanpa *blanking panel*
- Celah kabel terbuka
- Tidak ada sensor suhu per rack
- Dokumentasi kabel tidak akurat
- UPS belum diuji penuh
- Tidak ada review kapasitas triwulanan

Program perbaikan 6–12 bulan:

Tahap	Fokus	Tindakan
0–1 bulan	Baseline	Hitung PUE, IT load, suhu, rack density, kapasitas UPS/cooling
1–3 bulan	Airflow	Pasang blanking panel, tutup celah kabel, rapikan kabel
3–6 bulan	Monitoring	Tambah sensor suhu, power meter, leak detection
6–9 bulan	Dokumentasi	Update layout, SLD, kabel, IP, PDU, aset
9–12 bulan	Operasi	SOP/MOP/EOP, capacity review, audit internal

Data Center Handbook menekankan pentingnya *capacity planning* dan utilisasi sumber daya karena fasilitas data center sering tidak memenuhi kebutuhan operasi dan kapasitas awalnya; kapasitas yang tidak terpakai dapat menjadi modal yang terjebak pada UPS, generator, chiller, dan peralatan fasilitas lain .

Target retrofit:

- PUE turun bertahap dari **2,0 ke 1,6–1,7**
- Alarm suhu berkurang
- Kapasitas nyata terlihat
- Dokumentasi sesuai kondisi aktual
- SOP/MOP/EOP aktif
- Bukti audit tersedia

Pelajaran utama: retrofit terbaik bukan selalu mengganti perangkat besar, tetapi memperbaiki airflow, dokumentasi, monitoring, kapasitas, dan disiplin operasi.

12.3 Studi Kasus 3: Desain Edge Data Center

±0,75 halaman

Edge data center dibangun dekat sumber data atau pengguna. Fasilitas ini cocok untuk IoT, 5G, kota cerdas, pabrik, pelabuhan, kampus, pertambangan, perkebunan, rumah sakit, atau layanan yang membutuhkan *latency* rendah. Tantangannya adalah fasilitas kecil ini tetap harus aman, stabil, dan dapat dimonitor dari pusat.

Asumsi desain:

- Jumlah rack: 2–6 rack
- Beban: 3–8 kW/rack
- Lokasi: jauh dari pusat operasi
- Koneksi: minimal dua jalur jika layanan kritikal
- Operasi: remote monitoring
- Risiko: listrik tidak stabil, suhu lingkungan, keamanan fisik, akses vendor lambat

Buku *Cloud Data Center Network Architectures and Technologies* menjelaskan bahwa layanan 5G mendorong deployment ke *edge DC*, karena layanan perlu dipindahkan lebih dekat ke pengguna dan dikelola secara terpadu; tantangannya mencakup skalabilitas, reliabilitas, dan gangguan layanan yang harus sangat rendah pada skenario tertentu .

Keputusan desain *edge*:

- Gunakan rack tertutup bila lingkungan kurang ideal.
- Siapkan UPS dengan *runtime* cukup untuk gangguan singkat.
- Siapkan generator atau sumber cadangan jika lokasi kritikal.
- Gunakan cooling sederhana tetapi terukur.
- Pasang sensor suhu, kelembaban, power, pintu, dan kebocoran.
- Gunakan monitoring terpusat.
- Batasi akses fisik.
- Buat prosedur remote hands.
- Dokumentasikan semua aset dan konfigurasi.
- Siapkan skenario operasi saat koneksi pusat terputus.

Pelajaran utama: *edge data center* boleh kecil, tapi risikonya tidak kecil. **Semakin jauh lokasi, semakin penting monitoring, otomasi, keamanan fisik, dan prosedur lokal.**

12.4 Checklist Kesiapan Sertifikasi

Checklist ini digunakan sebelum audit internal atau audit pihak ketiga.

Area	Bukti Minimum	Status
Kebutuhan bisnis	BRD, RTO, RPO, SLA	Siap / Belum
Risiko	Risk register, mitigasi, bukti kontrol	Siap / Belum
Site & ruang	Layout, akses, jalur evakuasi, ruang MEP	Siap / Belum
Rack & cabling	Label, jalur kabel, patching record	Siap / Belum
Power	SLD, UPS, generator, PDU, grounding, hasil test	Siap / Belum
Cooling	Thermal map, sensor, cooling capacity, alarm	Siap / Belum
Jaringan	HLD, LLD, VLAN/VRF, DCI, hasil failover test	Siap / Belum
Security	Access log, CCTV, segmentation test, audit trail	Siap / Belum
Deployment	FAT, SAT, IST, commissioning report	Siap / Belum
Operasi	SOP, MOP, EOP, maintenance log	Siap / Belum
Monitoring	Dashboard, alarm, log, escalation path	Siap / Belum
Kapasitas	Review space, power, cooling, network, storage	Siap / Belum
Efisiensi	PUE, energi, air, karbon bila tersedia	Siap / Belum
Handover	As-built, training, BA serah terima	Siap / Belum

TIA-942 secara resmi mencakup infrastruktur fisik data center, termasuk lokasi, arsitektur, electrical, mechanical, *fire safety*, telekomunikasi, keamanan, dan persyaratan lain; skema sertifikasinya dilakukan oleh *Licensed Certification Bodies* yang memverifikasi kesesuaian fasilitas dengan standar. ([TIA Online](#))

Prinsip: sertifikasi bukan mencari dokumen yang indah, tetapi mencari **kesesuaian antara desain, kondisi lapangan, operasi, dan bukti**.

12.5 Peta Kompetensi Profesional Data Center

Profesional data center harus menguasai banyak disiplin. Ia tidak harus menjadi ahli terdalam di semua bidang, tetapi harus mampu membaca hubungan antar-domain.

Peta kompetensi inti:

Kompetensi	Yang Harus dikuasai
Bisnis & risiko	SLA, RTO, RPO, dampak downtime, risk register
Space & rack	Layout, white space, gray space, cable pathway
Power	UPS, generator, PDU, grounding, redundancy
Cooling	Airflow, containment, chiller, ASHRAE, thermal map
Network	Spine-leaf, underlay, overlay, segmentation, DCI
Security	Physical, network, OT, Zero Trust, audit trail
Deployment	FAT, SAT, IST, commissioning, handover
Operasi	SOP, MOP, EOP, DCIM, maintenance, incident
Sustainability	PUE, WUE, CUE, energy audit, green retrofit
Dokumentasi	HLD, LLD, as-built, checklist, evidence pack

Data Center Handbook menempatkan arsitektur data center sebagai gabungan sistem mekanikal, distribusi listrik, backup, rack-cabling, DCIM, DR/BC, perangkat lunak, dan layanan digital; rencana strategis juga harus mempertimbangkan agility, resiliency, modularity, availability, TCO, dan sustainability .

Kalimat kunci: profesional data center yang kuat mampu menjembatani bahasa bisnis, fasilitas, jaringan, keamanan, dan operasi.

12.6 Roadmap Belajar 6 Bulan

Roadmap ini ditujukan untuk profesional yang ingin menyiapkan diri menuju sertifikasi atau audit internal data center.

Bulan	Fokus	Output
1	Fondasi & standar	Ringkasan ISO/IEC 22237, Uptime, TIA-942, ASHRAE
2	Perhitungan kapasitas	Kalkulasi IT load, rack, power, UPS, generator, cooling
3	Space, power, cooling	Layout, SLD awal, thermal checklist, airflow audit
4	Network & security	HLD/LLD jaringan, segmentasi, checklist keamanan
5	Deployment & operasi	FAT/SAT/IST plan, SOP, MOP, EOP, monitoring
6	Audit readiness	Gap analysis, evidence pack, simulasi audit, portofolio

Aktivitas mingguan yang disarankan:

- Minggu 1: baca standar dan ringkas dalam 2 halaman.
- Minggu 2: buat template hitungan kapasitas.
- Minggu 3: audit mini ruang atau lab yang tersedia.
- Minggu 4: buat checklist dan bukti.
- Ulangi pola ini untuk setiap domain.

Uptime Institute menyatakan *Tier Certification* dapat mencakup desain, konstruksi, dan operasi; daftar penghargaan Uptime menunjukkan lebih dari 4.000 penghargaan di lebih dari 122 negara, sehingga disiplin bukti dan standar global menjadi penting untuk profesional data center. ([Uptime Institute](#))

Prinsip belajar: jangan hanya membaca; buat dokumen, hitung angka, gambar desain, dan simulasikan audit.

12.7 Kesalahan Fatal yang Sering Menggagalkan Sertifikasi

Kesalahan pertama adalah **tidak punya bukti**. Fasilitas bisa saja baik, tetapi tanpa dokumen, hasil uji, log, foto, laporan, dan *as-built*, auditor sulit memverifikasi klaim.

Kesalahan kedua adalah **desain dan kondisi lapangan berbeda**. Gambar menunjukkan jalur A/B, tetapi di lapangan kabel bercampur. Dokumen menunjukkan kapasitas UPS cukup, tetapi beban aktual melebihi batas aman.

Kesalahan ketiga adalah **operasi tidak disiplin**. SOP ada, tetapi tidak dipakai. MOP ada, tetapi perubahan tetap dilakukan spontan. EOP ada, tetapi tim belum pernah latihan.

Kesalahan keempat adalah **hanya mengejar perangkat, bukan sistem**. Perangkat mahal tidak otomatis menghasilkan data center andal jika airflow salah, grounding buruk, monitoring lemah, dan tim operasi tidak siap.

Kesalahan kelima adalah **tidak melakukan testing terpadu**. Power diuji sendiri, cooling diuji sendiri, network diuji sendiri, tetapi tidak pernah dilakukan *Integrated System Test*.

Kesalahan keenam adalah **tidak memahami kapasitas nyata**. Masih ada rack kosong, tetapi power habis. UPS cukup, tetapi cooling tidak cukup. Port jaringan ada, tetapi jalur kabel penuh.

Kalimat tajam: sertifikasi gagal bukan karena auditor terlalu ketat, tetapi karena desain, operasi, dan bukti tidak bertemu.

Materi Praktek 1: Checklist Final Sebelum Audit

Pertanyaan Final	Status
Apakah target sertifikasi sudah jelas?	Ya / Tidak
Apakah kebutuhan bisnis dan SLA terdokumentasi?	Ya / Tidak
Apakah RTO/RPO aplikasi kritikal tersedia?	Ya / Tidak
Apakah risk register lengkap?	Ya / Tidak
Apakah layout dan as-built sesuai lapangan?	Ya / Tidak
Apakah SLD listrik sesuai kondisi aktual?	Ya / Tidak
Apakah UPS, generator, ATS, dan PDU sudah diuji?	Ya / Tidak
Apakah thermal map tersedia?	Ya / Tidak
Apakah sensor dan alarm diuji?	Ya / Tidak
Apakah segmentasi jaringan diuji?	Ya / Tidak
Apakah akses fisik memiliki log dan review?	Ya / Tidak
Apakah FAT/SAT/IST terdokumentasi?	Ya / Tidak
Apakah SOP/MOP/EOP tersedia dan dilatih?	Ya / Tidak
Apakah maintenance log lengkap?	Ya / Tidak
Apakah capacity review terbaru tersedia?	Ya / Tidak
Apakah evidence pack sudah tersusun rapi?	Ya / Tidak

Materi Praktek 2: Template Gap Analysis

Domain	Kondisi Saat Ini	Target Sertifikasi	Gap	Risiko	Prioritas	PIC	Target Selesai
Space					Tinggi / Sedang / Rendah		
Power							
Cooling							
Network							
Security							
Monitoring							
Operations							
Documentation							
Sustainability							
Audit Evidence							

Cara membaca: gap yang berdampak langsung ke *availability*, keselamatan, keamanan, atau bukti audit harus mendapat prioritas tinggi.

Materi Praktek 3: Template Roadmap Peningkatan dari Kondisi Existing ke Target Sertifikasi

Tahap	Waktu	Fokus	Output
Tahap 1	0–30 hari	Baseline	Inventaris aset, kapasitas, risiko, dokumen existing
Tahap 2	31–60 hari	Perbaikan cepat	Labeling, dokumentasi, airflow, akses fisik
Tahap 3	61–90 hari	Pengujian	UPS test, generator test, cooling test, network failover
Tahap 4	91–120 hari	Operasi	SOP/MOP/EOP, maintenance plan, incident log
Tahap 5	121–150 hari	Evidence pack	As-built, laporan test, audit trail, checklist
Tahap 6	151–180 hari	Simulasi audit	Internal audit, gap closure, management review

Output akhir: fasilitas tidak hanya “lebih baik”, tetapi memiliki **bukti kesiapan** untuk audit.

Materi Praktek 4: Contoh Portofolio Professional Data Center

Portofolio profesional bukan hanya CV. Portofolio menunjukkan bahwa seseorang mampu bekerja dengan standar, angka, desain, operasi, dan bukti.

Isi portofolio yang disarankan:

- Ringkasan pengalaman proyek.
- Contoh *Data Center Design Brief*.
- Contoh perhitungan *IT load*, rack, power, cooling.
- Contoh layout *hot aisle/cold aisle*.
- Contoh *single line diagram* sederhana.
- Contoh HLD/LLD jaringan.
- Contoh matriks risiko.
- Contoh checklist keamanan fisik.
- Contoh commissioning plan.
- Contoh SOP/MOP/EOP.
- Contoh laporan insiden.
- Contoh capacity review.
- Contoh audit energi/PUE.
- Contoh gap analysis sertifikasi.
- Daftar pelatihan dan sertifikasi yang diikuti.
- Daftar standar yang dipahami.

Catatan penting: hilangkan informasi rahasia organisasi. Gunakan versi anonim, contoh sintetis, atau lab pribadi.

Kalimat kunci: portofolio yang baik membuktikan cara berpikir profesional, bukan membocorkan rahasia proyek.

Ringkasan Bab 12

Bab ini menutup buku dengan pesan utama: professional data center harus mampu **mendesain, menghitung, menguji, mengoperasikan, dan membuktikan**. Sertifikasi tidak cukup didekati dengan hafalan. Sertifikasi membutuhkan disiplin dokumen, disiplin pengujian, disiplin operasi, dan disiplin bukti.

Tiga studi kasus menunjukkan skala yang berbeda: 10 rack untuk membangun disiplin dasar, retrofit untuk memperbaiki fasilitas lama, dan *edge data center* untuk menjawab kebutuhan latency rendah serta operasi terdistribusi. Ketiganya memiliki pesan yang sama: **setiap keputusan teknis harus terkait dengan risiko, kapasitas, operasi, dan bukti audit**.

Inti bab: professional data center tidak diukur dari seberapa banyak istilah yang dihafal, tetapi dari seberapa kuat ia mempertanggungjawabkan keputusan teknis dengan angka, prosedur, pengujian, dan bukti.

Checklist Akhir Bab 12

Pembaca dinyatakan siap melanjutkan ke lampiran dan penyusunan portofolio bila mampu menjawab:

- Apakah saya bisa membuat studi kasus 10 rack dari nol?
- Apakah saya bisa menghitung *IT load*, power, UPS, generator, dan cooling?
- Apakah saya bisa menilai data center lama dan membuat roadmap retrofit?
- Apakah saya memahami risiko *edge data center*?
- Apakah saya bisa menyusun checklist kesiapan sertifikasi?
- Apakah saya bisa membuat *gap analysis*?
- Apakah saya bisa menyusun roadmap peningkatan 6 bulan?
- Apakah saya bisa membedakan desain, operasi, dan bukti audit?
- Apakah saya punya contoh portofolio profesional?
- Apakah saya siap menjelaskan keputusan teknis kepada auditor, manajemen, dan tim operasi?

Penutup bab: Data center yang baik lahir dari desain yang benar, tetapi sertifikasi yang kuat lahir dari bukti yang lengkap, operasi yang disiplin, dan profesional yang berani mempertanggungjawabkan setiap keputusan teknis.

Lampiran A. Template Data Center Design Brief

Tujuan:

Template ini digunakan sebagai dokumen awal sebelum desain teknis *data center* dibuat. Fungsinya adalah menyatukan kebutuhan bisnis, risiko, kapasitas, target keamanan, efisiensi energi, dan standar acuan agar seluruh tim memiliki pemahaman yang sama.

A.1 Informasi Umum Proyek

Item	Keterangan
Nama Proyek	
Nama Organisasi	
Lokasi Rencana Data Center	
Pemilik Bisnis	
Pemilik Teknis	
Tim Penyusun	
Tanggal Dokumen	
Versi Dokumen	

A.2 Tujuan Bisnis

Jelaskan alasan utama pembangunan atau pengembangan *data center*. Bagian ini harus menjawab **mengapa data center ini dibutuhkan** dan **layanan bisnis apa yang harus dijaga**.

Pertanyaan	Jawaban
Apa tujuan utama data center ini?	
Layanan bisnis apa yang akan didukung?	
Siapa pengguna utama layanan?	Internal / Publik / Pelanggan / Mitra / Cabang
Apakah layanan harus berjalan 24×7?	Ya / Tidak
Apa dampak jika layanan berhenti?	Finansial / Reputasi / Operasional / Hukum / Keselamatan
Apakah ada kebutuhan audit atau sertifikasi?	Ya / Tidak

Catatan:

Tujuan bisnis harus menjadi dasar semua keputusan teknis. Jangan mulai dari perangkat. Mulailah dari **layanan, risiko, dan dampak bisnis**.

A.3 Aplikasi Kritikal

Daftar aplikasi atau layanan utama yang akan berjalan di *data center*. Fokuskan pada aplikasi yang berdampak besar jika berhenti.

No	Aplikasi / Layanan	Fungsi Utama	Tingkat Kritikal	Jam Operasi	Dampak Jika Gagal
1			Rendah / Sedang / Tinggi / Kritikal		
2			Rendah / Sedang / Tinggi / Kritikal		
3			Rendah / Sedang / Tinggi / Kritikal		
4			Rendah / Sedang / Tinggi / Kritikal		

A.4 Target Availability

Bagian ini menetapkan target ketersediaan layanan. Target harus realistis terhadap risiko, anggaran, desain, dan kemampuan operasi.

Item	Target
Target uptime	
Jam operasi layanan	8×5 / 12×6 / 24×7
RTO — Recovery Time Objective	
RPO — Recovery Point Objective	
Apakah layanan boleh mati saat maintenance?	Ya / Tidak
Apakah dibutuhkan redundansi power?	N / N+1 / 2N
Apakah dibutuhkan redundansi cooling?	N / N+1 / 2N
Apakah dibutuhkan DR site?	Ya / Tidak
Model operasi DR	Active-Standby / Active-Active / Backup-Restore

Catatan:

Semakin tinggi target *availability*, semakin tinggi kebutuhan redundansi, pengujian, dokumentasi, dan disiplin operasi.

A.5 Target Keamanan

Bagian ini menjelaskan kebutuhan keamanan fisik, jaringan, sistem manajemen, data, dan bukti audit.

Area Keamanan	Target / Kebutuhan
Keamanan perimeter	
Kontrol akses ruang data center	
CCTV dan rekaman	
Visitor log dan escort policy	
Kunci rack	
Segmentasi jaringan	
Jaringan manajemen terpisah	Ya / Tidak
MFA untuk akses admin	Ya / Tidak
Logging dan audit trail	
Backup terlindungi ransomware	Ya / Tidak
Keamanan OT: BMS, DCIM, UPS, cooling controller	

Catatan:

Keamanan *data center* harus berlapis: **orang, ruang, rack, jaringan, sistem, data, proses, dan bukti audit.**

A.6 Target PUE dan Efisiensi Energi

Bagian ini menetapkan target efisiensi energi dan indikator keberlanjutan.

Item	Target / Keterangan
Target PUE awal	
Target PUE tahun ke-3	
Target PUE tahun ke-5	
Apakah energi IT dan fasilitas akan diukur terpisah?	Ya / Tidak
Apakah WUE akan dihitung?	Ya / Tidak
Apakah CUE akan dihitung?	Ya / Tidak
Apakah ada target energi terbarukan?	Ya / Tidak
Apakah ada rencana audit energi berkala?	Ya / Tidak
Apakah ada rencana green retrofit?	Ya / Tidak

Catatan:

PUE rendah penting, tetapi **data center hijau** juga harus memperhatikan energi, air, karbon, panas buangan, dan operasi berkelanjutan.

A.7 Kapasitas Awal dan Kapasitas 5 Tahun

Bagian ini menjadi dasar perhitungan ruang, rack, listrik, UPS, generator, cooling, jaringan, dan biaya energi.

Komponen	Kapasitas Awal	Proyeksi Tahun ke-3	Proyeksi Tahun ke-5
Jumlah rack			
Rata-rata kW/rack			
Total IT load			
Total facility power			
Kapasitas UPS			
Kapasitas generator			
Kapasitas cooling			
Luas white space			
Kapasitas storage			
Kapasitas jaringan			
Jumlah port jaringan			
Kapasitas backup			

A.8 Lokasi

Bagian ini menilai kelayakan lokasi dari sisi operasional, risiko, akses, energi, konektivitas, dan keamanan.

Faktor Lokasi	Keterangan
Alamat / area lokasi	
Kepemilikan lokasi	Milik sendiri / sewa / colocation / lainnya
Risiko banjir	Rendah / Sedang / Tinggi
Risiko gempa	Rendah / Sedang / Tinggi
Risiko kebakaran sekitar	Rendah / Sedang / Tinggi
Ketersediaan listrik	
Ketersediaan generator / bahan bakar	
Ketersediaan konektivitas	
Akses kendaraan barang	
Keamanan lingkungan	
Ketersediaan SDM operasi	
Potensi ekspansi	

Catatan:

Lokasi yang salah dapat membuat desain terbaik menjadi mahal, sulit dioperasikan, dan berisiko tinggi.

A.9 Risiko Utama

Identifikasi risiko sejak awal. Setiap risiko harus memiliki dampak, kontrol, dan bukti audit.

Risiko	Dampak	Kontrol yang Direncanakan	Bukti Audit
Listrik utama padam		UPS, generator, ATS/AMF	Log test, SLD, laporan maintenance
UPS gagal		Redundansi, bypass, uji baterai	Laporan uji UPS
Cooling gagal		Cooling cadangan, sensor suhu	Thermal map, log alarm
Kebakaran		Deteksi dini, sistem pemadaman	Sertifikat inspeksi
Banjir / kebocoran air		Leak detection, desain elevasi	Log sensor
Akses fisik tidak sah		Access control, CCTV, visitor log	Log akses
Serangan jaringan		Segmentasi, firewall, logging	Rulebase, log keamanan
Ransomware		Backup immutable/offline, uji restore	Laporan restore
SDM tidak siap		SOP, MOP, EOP, training	Daftar pelatihan
Vendor lambat		SLA, spare part, escalation path	Kontrak SLA
Kapasitas habis		Capacity review berkala	Laporan kapasitas

A.10 Standar Acuan

Pilih standar yang menjadi acuan desain, sertifikasi, audit, dan operasi.

Standar / Kerangka	Digunakan?	Fokus Penggunaan
ISO/IEC 22237	Ya / Tidak	Fasilitas, availability, keamanan fisik, efisiensi energi
Uptime Tier	Ya / Tidak	Ketersediaan infrastruktur dan operasi
TIA-942	Ya / Tidak	Telekomunikasi, fasilitas, power, cooling, keamanan
ASHRAE TC 9.9	Ya / Tidak	Thermal, humidity, cooling, energy efficiency
The Green Grid PUE	Ya / Tidak	Efisiensi energi
NIST Cybersecurity Framework	Ya / Tidak	Tata kelola keamanan siber
NIST Zero Trust Architecture	Ya / Tidak	Prinsip akses dan segmentasi
Standar internal organisasi	Ya / Tidak	Kepatuhan internal

A.11 Keputusan Manajemen yang Dibutuhkan

Bagian ini mencatat keputusan strategis yang harus disetujui sebelum desain detail.

Keputusan	Pilihan / Catatan	Status
Target sertifikasi		Disetujui / Belum
Target availability		Disetujui / Belum
Target PUE		Disetujui / Belum
Kapasitas 5 tahun		Disetujui / Belum
Lokasi		Disetujui / Belum
Model redundansi power	N / N+1 / 2N	Disetujui / Belum
Model redundansi cooling	N / N+1 / 2N	Disetujui / Belum
Model operasi	Internal / managed service / hybrid	Disetujui / Belum
Anggaran awal		Disetujui / Belum
Roadmap ekspansi		Disetujui / Belum

A.12 Ringkasan Eksekutif Design Brief

Isi bagian ini dalam 1–2 paragraf pendek.

Ringkasan:

Data center ini dirancang untuk mendukung layanan: _____.

Layanan paling kritikal adalah: _____.

Target *availability* adalah: _____.

Target keamanan utama adalah: _____.

Target PUE adalah: _____.

Kapasitas awal adalah: _____ rack / _____ kW *IT load*.

Kapasitas tahun ke-5 adalah: _____ rack / _____ kW *IT load*.

Risiko utama yang harus dikendalikan adalah: _____.

Standar acuan utama adalah: _____.

A.13 Persetujuan

Nama	Jabatan	Peran	Tanda Tangan	Tanggal
		Pemilik Bisnis		
		Pemilik Teknis		
		Fasilitas / MEP		
		Jaringan		
		Keamanan		
		Operasi		
		Manajemen		

Catatan Penutup:

Data Center Design Brief harus dibuat sebelum desain detail. Dokumen ini menjadi **jembatan antara kebutuhan bisnis dan keputusan teknis**, sekaligus menjadi dasar awal untuk audit, sertifikasi, perencanaan kapasitas, dan pengendalian risiko.

Lampiran B. Template Perhitungan Kapasitas

Tujuan:

Template ini digunakan untuk menghitung kebutuhan kapasitas awal *data center*, memproyeksikan pertumbuhan 3 tahun dan 5 tahun, serta menjadi dasar perhitungan **rack, power, UPS, generator, cooling, jaringan, dan ruang ekspansi**.

Prinsip utama: **semua desain kapasitas harus dimulai dari angka beban perangkat, bukan dari perkiraan umum.**

B.1 Template Utama Perhitungan Kapasitas Perangkat

Jenis Perangkat	Jumlah	Watt per Perangkat	Total Watt	Rack Target	Growth 3 Tahun	Growth 5 Tahun	Catatan Desain
Server aplikasi							
Server database							
Server virtualisasi							
Server AI / GPU							
Storage array							
Backup appliance							
Core switch							
Leaf switch							
Firewall							
IDS/IPS							
Load balancer							
Perangkat manajemen							
Perangkat monitoring							
Perangkat keamanan fisik							
Perangkat OT / BMS / DCIM							

Lainnya							
Total			0 W				

B.2 Rumus Dasar

Gunakan rumus berikut untuk mengisi tabel.

Komponen	Rumus
Total Watt per jenis perangkat	Jumlah × Watt per perangkat
Total IT Load watt	Jumlah seluruh total watt perangkat TI
Total IT Load kW	Total watt / 1.000
Growth 3 Tahun	Kapasitas awal × faktor pertumbuhan 3 tahun
Growth 5 Tahun	Kapasitas awal × faktor pertumbuhan 5 tahun
Total Facility Power	IT Load × PUE
Cooling BTU/h	IT Load kW × 3.412
Cooling TR	BTU/h / 12.000

B.3 Contoh Pengisian

Jenis Perangkat	Jumlah	Watt per Perangkat	Total Watt	Rack Target	Growth 3 Tahun	Growth 5 Tahun	Catatan Desain
Server aplikasi	20	500 W	10.000 W	Rack A01–A03	30 unit	40 unit	Beban produksi utama
Server database	6	700 W	4.200 W	Rack A04	8 unit	10 unit	Perlu storage cepat
Server AI / GPU	4	2.500 W	10.000 W	Rack B01	8 unit	12 unit	Perlu perhatian cooling
Storage array	3	1.200 W	3.600 W	Rack B02	4 unit	5 unit	Perlu jalur storage khusus
Core switch	2	600 W	1.200 W	Rack N01	2 unit	2 unit	Redundansi
Leaf switch	4	400 W	1.600 W	Rack N02–N03	6 unit	8 unit	Sesuaikan jumlah rack
Firewall	2	350 W	700 W	Rack S01	2 unit	2 unit	HA pair
Perangkat monitoring	2	300 W	600 W	Rack M01	3 unit	4 unit	Monitoring dan logging
Total			31.900 W				

Total IT Load awal:

$$31.900 \text{ W} / 1.000 = \mathbf{31,9 \text{ kW}}$$

Jika ditambah margin desain 20%:

$$31,9 \text{ kW} \times 1,2 = \mathbf{38,28 \text{ kW}}$$

B.4 Template Ringkasan Kapasitas

Item	Kapasitas Awal	Proyeksi 3 Tahun	Proyeksi 5 Tahun	Catatan
Total perangkat				
Total IT Load				kW
Jumlah rack				
Rata-rata kW/rack				
Rack density tertinggi				kW/rack
Total Facility Power				IT Load × PUE
Kapasitas UPS				Tambahkan margin
Kapasitas generator				Termasuk beban pendukung
Kapasitas cooling				BTU/h atau TR
Kebutuhan port jaringan				
Kebutuhan storage				TB/PB
Kapasitas backup				
Risiko bottleneck				Power / cooling / space / network

B.5 Template Perhitungan Rack Target

Rack Target	Jenis Perangkat	Total U Terpakai	Total Watt	kW/Rack	Status Kapasitas	Catatan
Rack A01					Aman / Waspada / Kritis	
Rack A02					Aman / Waspada / Kritis	
Rack A03					Aman / Waspada / Kritis	
Rack B01					Aman / Waspada / Kritis	
Rack B02					Aman / Waspada / Kritis	
Rack N01					Aman / Waspada / Kritis	
Rack S01					Aman / Waspada / Kritis	
Total						

Catatan:

Rack dengan beban tinggi, terutama untuk *server* AI/GPU, storage padat, atau perangkat jaringan besar, harus diberi perhatian khusus pada **power, airflow, PDU, kabel, dan sensor suhu**.

B.6 Template Growth 3 Tahun dan 5 Tahun

Jenis Perangkat	Kapasitas Awal	Growth per Tahun	Estimasi Tahun ke-3	Estimasi Tahun ke-5	Dampak ke Desain
Server aplikasi					Rack / power / cooling
Server database					Storage / backup
Server AI / GPU					Power tinggi / liquid cooling
Storage					Space / backup / power
Perangkat jaringan					Port / bandwidth
Perangkat keamanan					Segmentasi / logging
Perangkat monitoring					Dashboard / sensor
Total IT Load					UPS / generator / cooling

B.7 Catatan Desain yang Wajib Diisi

Gunakan kolom **Catatan Desain** untuk mencatat hal-hal penting yang mempengaruhi keputusan teknis.

Contoh catatan:

- Perangkat memiliki **dual power supply**.
- Perlu jalur power A dan B.
- Perlu koneksi jaringan redundant.
- Perlu cooling khusus karena kW/rack tinggi.
- Perlu sensor suhu di depan rack.
- Perlu rack dengan kapasitas berat lebih tinggi.
- Perlu segmentasi jaringan khusus.
- Perlu backup dan DR.
- Perlu koneksi storage berkecepatan tinggi.
- Perlu ruang ekspansi 3–5 tahun.
- Berisiko menjadi *stranded capacity* jika power/cooling tidak ditambah.

B.8 Checklist Validasi Perhitungan Kapasitas

Pertanyaan Validasi	Status
Apakah semua perangkat utama sudah masuk tabel?	Ya / Tidak
Apakah watt per perangkat memakai data yang realistis?	Ya / Tidak
Apakah total IT Load sudah dihitung dalam kW?	Ya / Tidak
Apakah margin desain sudah ditambahkan?	Ya / Tidak
Apakah growth 3 tahun sudah dihitung?	Ya / Tidak
Apakah growth 5 tahun sudah dihitung?	Ya / Tidak
Apakah rack target sudah ditentukan?	Ya / Tidak
Apakah kW/rack sudah dihitung?	Ya / Tidak
Apakah ada rack dengan densitas tinggi?	Ya / Tidak
Apakah kapasitas UPS cukup untuk growth?	Ya / Tidak
Apakah kapasitas generator memperhitungkan beban pendukung?	Ya / Tidak
Apakah kapasitas cooling cukup untuk beban aktual dan growth?	Ya / Tidak
Apakah kebutuhan port jaringan sudah dihitung?	Ya / Tidak
Apakah risiko stranded capacity sudah diperiksa?	Ya / Tidak
Apakah hasil perhitungan siap menjadi bukti audit?	Ya / Tidak

B.9 Ringkasan Akhir Perhitungan

Isi ringkasan ini setelah semua tabel selesai.

Item	Nilai
Total IT Load awal	
Total IT Load dengan margin	
Total IT Load tahun ke-3	
Total IT Load tahun ke-5	
Jumlah rack awal	
Jumlah rack tahun ke-3	
Jumlah rack tahun ke-5	
Rata-rata kW/rack awal	
Rack density tertinggi	
Target PUE	
Total Facility Power awal	
Kapasitas UPS minimum	
Kapasitas generator minimum	
Kapasitas cooling minimum	
Risiko kapasitas terbesar	

Catatan Penutup:

Template ini harus diperbarui setiap kali ada penambahan perangkat, perubahan desain, ekspansi layanan, atau perubahan target sertifikasi. **Perhitungan kapasitas yang tidak diperbarui akan membuat desain terlihat cukup di dokumen, tetapi gagal di lapangan.**

Lampiran C. Rumus-Rumus Penting

Tujuan:

Lampiran ini merangkum rumus dasar yang sering dipakai dalam perencanaan, desain, audit, dan operasi *data center*. Rumus ini membantu profesional menghitung **beban TI, daya fasilitas, efisiensi energi, kapasitas pendinginan, biaya energi, densitas rack, UPS, generator, dan pertumbuhan kapasitas**.

Catatan penting: rumus di bawah ini adalah **rumus awal untuk perencanaan dan estimasi**. Untuk desain final, terutama listrik, UPS, generator, grounding, proteksi, dan cooling, hasil harus divalidasi oleh engineer profesional sesuai standar, kondisi lokasi, dan spesifikasi perangkat.

C.1 IT Load

IT Load adalah total beban daya perangkat TI yang benar-benar menjalankan layanan, seperti *server, storage*, perangkat jaringan, perangkat keamanan, perangkat monitoring, dan GPU.

Rumus Dasar

$$\text{IT Load} = \text{Jumlah Perangkat} \times \text{Watt per Perangkat}$$

Jika ada banyak jenis perangkat:

$$\text{Total IT Load} = \text{Total Watt semua perangkat} / 1.000$$

Contoh

Jenis Perangkat	Jumlah	Watt per Perangkat	Total Watt
Server aplikasi	20	500 W	10.000 W
Storage	4	800 W	3.200 W
Network switch	4	400 W	1.600 W
Firewall	2	300 W	600 W
Total			15.400 W

$$\text{Total IT Load} = 15.400 / 1.000 = 15,4 \text{ kW}$$

Jika memakai margin desain 20%:

$$\text{IT Load Desain} = 15,4 \times 1,2 = 18,48 \text{ kW}$$

C.2 Facility Load

Facility Load adalah total beban daya fasilitas, yaitu beban TI ditambah beban pendukung seperti cooling, UPS losses, PDU losses, lampu, keamanan, monitoring, fan, pump, dan sistem fasilitas lain.

Rumus Dasar

$$\text{Facility Load} = \text{IT Load} \times \text{PUE}$$

Contoh

- IT Load = 200 kW
- Target PUE = 1,6

$$\text{Facility Load} = 200 \times 1,6 = 320 \text{ kW}$$

Jika ditambah margin desain 20%:

$$\text{Facility Load Desain} = 320 \times 1,2 = 384 \text{ kW}$$

Catatan: angka ini dapat digunakan sebagai estimasi awal untuk melihat kebutuhan daya fasilitas, tetapi desain final harus memperhitungkan faktor daya, *inrush current*, beban motor, UPS recharge, cooling, dan ekspansi.

C.3 PUE — Power Usage Effectiveness

PUE adalah ukuran efisiensi energi *data center*. PUE menunjukkan perbandingan antara total energi fasilitas dan energi yang benar-benar dipakai perangkat TI.

Rumus

$$\text{PUE} = \text{Total Energi Fasilitas} / \text{Energi Perangkat IT}$$

Atau untuk estimasi daya:

$$\text{PUE} = \text{Total Facility Power} / \text{IT Load}$$

Contoh

- Total energi fasilitas = 240.000 kWh/bulan
- Energi perangkat IT = 150.000 kWh/bulan

$$\text{PUE} = 240.000 / 150.000 = 1,6$$

Interpretasi

PUE	Makna Umum
1,1–1,3	Sangat efisien, biasanya fasilitas modern dan sangat optimal
1,4–1,6	Baik untuk banyak fasilitas profesional
1,7–2,0	Masih dapat diterima, tetapi perlu optimasi
>2,0	Boros, perlu audit energi serius

Catatan: PUE tidak boleh dibaca sendirian. PUE harus dilihat bersama *IT load*, suhu lingkungan, usia fasilitas, pola beban, strategi cooling, dan biaya energi.

C.4 DCiE — Data Center Infrastructure Efficiency

DCiE adalah kebalikan dari PUE. Jika PUE menunjukkan rasio total fasilitas terhadap energi TI, DCiE menunjukkan persentase energi yang benar-benar dipakai perangkat TI.

Rumus

$$\text{DCiE} = \text{Energi Perangkat IT} / \text{Total Energi Fasilitas} \times 100\%$$

Atau:

$$\text{DCiE} = 1 / \text{PUE} \times 100\%$$

Contoh

Jika PUE = 1,6:

$$\text{DCiE} = 1 / 1,6 \times 100\% = 62,5\%$$

Artinya, sekitar **62,5% energi** dipakai perangkat TI, sedangkan sisanya dipakai sistem pendukung seperti cooling, UPS losses, distribusi listrik, dan fasilitas lain.

C.5 Cooling BTU/h

Kapasitas cooling harus dihitung dari *IT Load*, karena hampir seluruh energi listrik yang dipakai perangkat TI akan berubah menjadi panas.

Rumus

$$\text{Cooling Capacity BTU/h} = \text{IT Load kW} \times 3.412$$

Untuk konversi ke TR:

$$\text{Cooling TR} = \text{BTU/h} / 12.000$$

Contoh

- IT Load = 100 kW

$$\text{Cooling BTU/h} = 100 \times 3.412 = 341.200 \text{ BTU/h}$$

$$\text{Cooling TR} = 341.200 / 12.000 = 28,43 \text{ TR}$$

Jika ditambah margin 20%:

$$\text{Cooling Design} = 28,43 \times 1,2 = 34,1 \text{ TR}$$

Catatan: kapasitas TR saja tidak cukup. Cooling harus benar-benar sampai ke *inlet* rack. Karena itu, *airflow*, *hot aisle*, *cold aisle*, *containment*, *sensor*, dan *thermal map* tetap wajib diperiksa.

C.6 Energy Cost

Biaya energi membantu manajemen memahami dampak finansial dari desain *data center*. Perhitungan ini penting untuk menilai PUE, efisiensi cooling, dan investasi penghematan energi.

Rumus

$$\text{Energy Cost per Year} = \text{kW} \times 24 \times 365 \times \text{Tarif Listrik}$$

Jika memakai energi bulanan:

$$\text{Energy Cost per Month} = \text{kW} \times 24 \times 30 \times \text{Tarif Listrik}$$

Contoh Tahunan

- Total Facility Power = 320 kW
- Tarif listrik = Rp1.500/kWh

$$\text{Energy Cost per Year} = 320 \times 24 \times 365 \times 1.500$$

$$\text{Energy Cost per Year} = \text{Rp}4.204.800.000$$

Contoh Penghematan PUE

- IT Load = 200 kW
- PUE awal = 2,0
- PUE target = 1,6
- Tarif listrik = Rp1.500/kWh

Facility power awal:

$$200 \times 2,0 = 400 \text{ kW}$$

Facility power target:

$$200 \times 1,6 = 320 \text{ kW}$$

Penghematan daya:

$$400 - 320 = 80 \text{ kW}$$

Penghematan tahunan:

$$80 \times 24 \times 365 \times 1.500 = \text{Rp}1.051.200.000$$

Catatan: efisiensi energi bukan hanya isu teknis. Efisiensi energi adalah **isu biaya operasi jangka panjang**.

C.7 Rack Density

Rack density menunjukkan rata-rata beban daya per rack. Ini penting untuk menentukan kebutuhan PDU, kabel power, airflow, cooling, sensor, dan risiko *hot spot*.

Rumus

$$\text{Rack Density} = \text{Total IT Load} / \text{Jumlah Rack}$$

Atau per rack:

$$\text{Rack Density per Rack} = \text{Total Watt dalam Rack} / 1.000$$

Contoh

- Total IT Load = 180 kW
- Jumlah rack = 30

$$\text{Rack Density} = 180 / 30 = 6 \text{ kW/rack}$$

Kategori Awal

Rack Density	Kategori	Implikasi Desain
1–3 kW/rack	Rendah	Cooling sederhana, risiko rendah
4–6 kW/rack	Menengah	Perlu airflow baik dan monitoring
7–12 kW/rack	Tinggi	Perlu containment dan distribusi daya kuat
>12 kW/rack	Sangat tinggi	Perlu desain khusus, mungkin liquid cooling

Catatan: rack GPU, AI, HPC, dan storage padat harus diperiksa khusus. Jangan hanya memakai rata-rata seluruh ruangan.

\

C.8 UPS Sizing

UPS melindungi beban kritikal saat listrik utama terganggu. Perhitungan awal UPS harus berbasis *critical IT load*, margin pertumbuhan, faktor daya, dan target redundansi.

Rumus Dasar

$$\text{UPS kW} = \text{Critical IT Load} \times \text{Margin}$$

Jika perlu konversi ke kVA:

$$\text{UPS kVA} = \text{UPS kW} / \text{Power Factor}$$

Contoh

- Critical IT Load = 200 kW
- Margin desain = 20%
- Power factor = 0,9

$$\text{UPS kW} = 200 \times 1,2 = 240 \text{ kW}$$

$$\text{UPS kVA} = 240 / 0,9 = 266,7 \text{ kVA}$$

Maka kapasitas praktis awal dapat diarahkan ke:

$$\pm 300 \text{ kVA}$$

Jika Menggunakan N+1

Misal modul UPS = 100 kW.

- Beban desain = 240 kW
- Modul aktif minimum = 3 modul = 300 kW
- Tambah 1 modul cadangan = 4 modul
- Total terpasang = **400 kW**, dengan kapasitas aktif aman **300 kW**

Catatan: UPS final harus memperhitungkan efisiensi UPS, harmonisa, *bypass*, baterai, suhu ruang, *runtime*, dan prosedur maintenance.

C.9 Generator Sizing

Generator harus dihitung dari beban kritikal fasilitas, bukan dari IT Load saja. Generator harus mampu mendukung perangkat TI, cooling kritikal, UPS recharge, keamanan, monitoring, lampu darurat, dan sistem penting lain.

Rumus Awal

$$\text{Generator Capacity kW} = \text{Beban Kritis Fasilitas} \times \text{Margin}$$

Jika memakai faktor daya:

$$\text{Generator Capacity kVA} = \text{Generator kW} / \text{Power Factor}$$

Contoh

- IT Load = 200 kW
- Target PUE = 1,6
- Total Facility Load = $200 \times 1,6 = 320$ kW
- Margin desain = 20%

$$\text{Generator kW} = 320 \times 1,2 = 384 \text{ kW}$$

Jika power factor = 0,8:

$$\text{Generator kVA} = 384 / 0,8 = 480 \text{ kVA}$$

Maka kapasitas praktis awal:

$$\pm 500 \text{ kVA}$$

Hal yang Wajib Diperiksa

- Beban motor cooling.
- *Inrush current*.
- UPS recharge.
- Beban pompa dan fan.
- Suhu lingkungan.
- Ketinggian lokasi.
- Durasi bahan bakar.
- Kapasitas tangki.
- Redundansi N, N+1, atau 2N.
- Jadwal *load test*.

Catatan: generator besar tanpa *load test*, bahan bakar cukup, ATS/AMF yang diuji, dan SOP operasi tetap merupakan risiko besar.

C.10 Growth Capacity

Growth capacity digunakan untuk menghitung pertumbuhan kapasitas dalam beberapa tahun. Ini penting agar desain tidak hanya cukup untuk hari pertama.

Rumus Pertumbuhan Majemuk

$$\text{Kapasitas Tahun ke-}n = \text{Kapasitas Awal} \times (1 + \text{Growth Rate})^n$$

Contoh

- IT Load awal = 100 kW
- Growth rate = 15% per tahun
- Periode = 5 tahun

$$\text{IT Load Tahun ke-5} = 100 \times (1 + 0,15)^5$$

$$\text{IT Load Tahun ke-5} = 100 \times 2,011 = 201,1 \text{ kW}$$

Artinya, dengan pertumbuhan 15% per tahun, beban bisa menjadi sekitar **dua kali lipat dalam 5 tahun**.

Tabel Contoh

Tahun	Rumus	IT Load
0	Awal	100 kW
1	$100 \times 1,15$	115 kW
2	$100 \times 1,15^2$	132,25 kW
3	$100 \times 1,15^3$	152,09 kW
4	$100 \times 1,15^4$	174,90 kW
5	$100 \times 1,15^5$	201,14 kW

Catatan: growth tidak harus langsung dibeli semua, tetapi **jalur ekspansinya harus disiapkan**: ruang, panel, breaker, UPS, generator, cooling, cable tray, port jaringan, monitoring, dan prosedur operasi.

C.11 Ringkasan Rumus Cepat

Kebutuhan	Rumus
IT Load	Jumlah perangkat × watt per perangkat
Total IT Load kW	Total watt / 1.000
Facility Load	IT Load × PUE
PUE	Total energi fasilitas / energi IT
DCiE	Energi IT / total energi fasilitas × 100%
Cooling BTU/h	IT Load kW × 3.412
Cooling TR	BTU/h / 12.000
Energy Cost per Year	kW × 24 × 365 × tarif listrik
Rack Density	Total IT Load / jumlah rack
UPS kW	Critical IT Load × margin
UPS kVA	UPS kW / power factor
Generator kW	Beban kritis fasilitas × margin
Generator kVA	Generator kW / power factor
Growth Capacity	Kapasitas awal × (1 + growth rate) ⁿ

C.12 Contoh Ringkas Satu Kasus Lengkap

Asumsi

- Jumlah rack = 30
- Beban per rack = 6 kW
- PUE target = 1,6
- Margin desain = 20%
- Tarif listrik = Rp1.500/kWh
- Power factor generator = 0,8

Perhitungan

1. IT Load

$$30 \times 6 = 180 \text{ kW}$$

2. Facility Load

$$180 \times 1,6 = 288 \text{ kW}$$

3. Facility Load dengan margin

$$288 \times 1,2 = 345,6 \text{ kW}$$

4. Cooling BTU/h

$$180 \times 3.412 = 614.160 \text{ BTU/h}$$

5. Cooling TR

$$614.160 / 12.000 = 51,18 \text{ TR}$$

Dengan margin 20%:

$$51,18 \times 1,2 = 61,4 \text{ TR}$$

6. Energy Cost per Year

$$288 \times 24 \times 365 \times 1.500 = \text{Rp}3.784.320.000$$

7. Rack Density

$$180 / 30 = 6 \text{ kW/rack}$$

8. Generator kVA estimasi

$$345,6 / 0,8 = 432 \text{ kVA}$$

Kapasitas praktis awal dapat diarahkan ke sekitar **450–500 kVA**, sebelum validasi desain final.

C.13 Checklist Validasi Rumus

Pertanyaan	Status
Apakah semua perangkat masuk dalam perhitungan IT Load?	Ya / Tidak
Apakah watt per perangkat realistis?	Ya / Tidak
Apakah margin desain sudah ditambahkan?	Ya / Tidak
Apakah PUE yang dipakai realistis untuk fasilitas tersebut?	Ya / Tidak
Apakah cooling dihitung dari IT Load?	Ya / Tidak
Apakah biaya energi dihitung tahunan?	Ya / Tidak
Apakah rack density dihitung per rack, bukan hanya rata-rata ruangan?	Ya / Tidak
Apakah UPS memperhitungkan faktor daya dan runtime?	Ya / Tidak
Apakah generator memperhitungkan beban cooling dan UPS recharge?	Ya / Tidak
Apakah growth 3–5 tahun dihitung?	Ya / Tidak
Apakah risiko stranded capacity diperiksa?	Ya / Tidak

Catatan Penutup:

Rumus membantu membuat desain lebih rasional, tetapi **angka tanpa validasi lapangan tetap berbahaya**. Professional *data center* harus mampu menghitung, menjelaskan asumsi, memeriksa risiko, dan membuktikan hasil perhitungan melalui desain, pengujian, dokumentasi, dan operasi.

Lampiran D. Checklist Desain Data Center

Tujuan:

Checklist ini digunakan untuk memeriksa kesiapan desain *data center* sebelum masuk tahap detail engineering, pengadaan, deployment, commissioning, dan audit sertifikasi.

Prinsip utama: **desain yang baik harus dapat dibuktikan melalui gambar, perhitungan, dokumen, pengujian, dan kesiapan operasi.**

D.1 Checklist Site

Area Pemeriksaan	Pertanyaan Desain	Status	Catatan
Lokasi	Apakah lokasi sudah dipilih berdasarkan kebutuhan bisnis dan risiko?	Ya / Tidak	
Risiko banjir	Apakah risiko banjir sudah dianalisis?	Ya / Tidak	
Risiko gempa	Apakah risiko gempa sudah dipertimbangkan?	Ya / Tidak	
Risiko kebakaran sekitar	Apakah ada resiko kebakaran dari lingkungan sekitar?	Ya / Tidak	
Akses kendaraan	Apakah akses untuk pengiriman perangkat besar tersedia?	Ya / Tidak	
Akses darurat	Apakah akses pemadam, ambulance, dan evakuasi tersedia?	Ya / Tidak	
Ketersediaan listrik	Apakah pasokan listrik utama cukup dan stabil?	Ya / Tidak	
Ketersediaan bahan bakar	Apakah pasokan bahan bakar generator tersedia dan aman?	Ya / Tidak	
Konektivitas	Apakah tersedia lebih dari satu jalur koneksi?	Ya / Tidak	
Keamanan lingkungan	Apakah area sekitar cukup aman untuk fasilitas kritikal?	Ya / Tidak	
Potensi ekspansi	Apakah lokasi mendukung ekspansi 3–5 tahun?	Ya / Tidak	
Kepatuhan lokal	Apakah perizinan dan aturan lokal sudah dipetakan?	Ya / Tidak	

D.2 Checklist Space

Area Pemeriksaan	Pertanyaan Desain	Status	Catatan
White space	Apakah luas ruang rack cukup untuk kapasitas awal?	Ya / Tidak	
Ekspansi ruang	Apakah tersedia ruang untuk kapasitas 5 tahun?	Ya / Tidak	
Gray space	Apakah ruang UPS, baterai, panel, cooling, dan MEP tersedia?	Ya / Tidak	
Ruang staging	Apakah tersedia ruang bongkar, staging, dan persiapan perangkat?	Ya / Tidak	
Jalur barang	Apakah jalur masuk perangkat besar aman dan cukup lebar?	Ya / Tidak	
Jalur evakuasi	Apakah jalur evakuasi jelas dan tidak terhalang?	Ya / Tidak	
Beban lantai	Apakah kapasitas lantai cukup untuk rack, UPS, baterai, dan cooling?	Ya / Tidak	
Ketinggian ruang	Apakah tinggi ruang cukup untuk rack, cable tray, dan airflow?	Ya / Tidak	
Hot/cold aisle	Apakah layout mendukung hot aisle dan cold aisle?	Ya / Tidak	
Area kerja	Apakah tersedia ruang kerja maintenance di depan dan belakang rack?	Ya / Tidak	
Kebersihan	Apakah desain mencegah debu, air, dan barang tidak perlu masuk ruang kritikal?	Ya / Tidak	

D.3 Checklist Rack

Area Pemeriksaan	Pertanyaan Desain	Status	Catatan
Jumlah rack	Apakah jumlah rack awal sudah dihitung?	Ya / Tidak	
Kapasitas 5 tahun	Apakah jumlah rack 5 tahun sudah diproyeksikan?	Ya / Tidak	
Ukuran rack	Apakah tinggi, lebar, dan kedalaman rack sesuai perangkat?	Ya / Tidak	
Beban berat	Apakah kapasitas berat rack cukup?	Ya / Tidak	
Rack density	Apakah kW/rack sudah dihitung?	Ya / Tidak	
Rack GPU/HPC	Apakah rack densitas tinggi diberi desain khusus?	Ya / Tidak	
Jalur power A/B	Apakah setiap rack mendukung jalur listrik A dan B?	Ya / Tidak	
Rack PDU	Apakah kapasitas rack PDU sesuai beban?	Ya / Tidak	
Blanking panel	Apakah U kosong wajib ditutup blanking panel?	Ya / Tidak	
Manajemen kabel	Apakah tersedia vertical/horizontal cable manager?	Ya / Tidak	
Label rack	Apakah penamaan rack sudah distandarkan?	Ya / Tidak	
Kunci rack	Apakah rack kritikal memiliki rack lock?	Ya / Tidak	
Sensor rack	Apakah rack kritikal memiliki sensor suhu inlet?	Ya / Tidak	

D.4 Checklist Power

Area Pemeriksaan	Pertanyaan Desain	Status	Catatan
IT load	Apakah total IT load sudah dihitung?	Ya / Tidak	
Facility load	Apakah total beban fasilitas sudah dihitung?	Ya / Tidak	
Margin desain	Apakah margin pertumbuhan sudah dimasukkan?	Ya / Tidak	
SLD	Apakah single line diagram tersedia?	Ya / Tidak	
Utility feed	Apakah pasokan listrik utama cukup?	Ya / Tidak	
Panel utama	Apakah kapasitas panel dan breaker sesuai desain?	Ya / Tidak	
UPS	Apakah kapasitas UPS sesuai beban kritis?	Ya / Tidak	
Runtime UPS	Apakah runtime UPS sudah ditentukan?	Ya / Tidak	
Redundansi UPS	Apakah model N, N+1, atau 2N sudah dipilih?	Ya / Tidak	
Generator	Apakah generator menghitung IT load dan beban pendukung?	Ya / Tidak	
ATS/AMF	Apakah ATS/AMF dirancang dan diuji?	Ya / Tidak	
PDU/RPP	Apakah distribusi daya ke rack jelas?	Ya / Tidak	
Rack PDU	Apakah rack PDU memiliki kapasitas dan metering yang cukup?	Ya / Tidak	
Grounding	Apakah grounding dan bonding dirancang?	Ya / Tidak	
Proteksi petir	Apakah proteksi petir dan surge protection tersedia?	Ya / Tidak	
Jalur A/B	Apakah jalur A dan B benar-benar terpisah?	Ya / Tidak	
Metering	Apakah energi IT dan fasilitas dapat diukur terpisah?	Ya / Tidak	

D.5 Checklist Cooling

Area Pemeriksaan	Pertanyaan Desain	Status	Catatan
Cooling load	Apakah kebutuhan cooling dihitung dari IT load?	Ya / Tidak	
BTU/h dan TR	Apakah kapasitas cooling dihitung dalam BTU/h dan TR?	Ya / Tidak	
Margin cooling	Apakah margin pertumbuhan sudah dimasukkan?	Ya / Tidak	
Airflow	Apakah jalur udara dingin dan panas dipisahkan?	Ya / Tidak	
Hot/cold aisle	Apakah rack disusun sesuai hot aisle dan cold aisle?	Ya / Tidak	
Containment	Apakah HAC atau CAC diperlukan?	Ya / Tidak	
CRAC/CRAH	Apakah kapasitas dan jumlah unit cooling cukup?	Ya / Tidak	
Chiller/pump	Apakah sistem chilled water sudah dihitung?	Ya / Tidak	
Cooling redundancy	Apakah model N, N+1, atau 2N sudah dipilih?	Ya / Tidak	
Inlet temperature	Apakah suhu inlet rack akan dipantau?	Ya / Tidak	
Kelembapan	Apakah RH dan dew point akan dipantau?	Ya / Tidak	
Leak detection	Apakah sensor kebocoran tersedia?	Ya / Tidak	
Rack density tinggi	Apakah rack GPU/HPC butuh liquid cooling?	Ya / Tidak	
Free cooling	Apakah free cooling atau economizer layak dikaji?	Ya / Tidak	
Thermal map	Apakah rencana thermal mapping tersedia?	Ya / Tidak	
Filter dan maintenance	Apakah akses maintenance cooling tersedia?	Ya / Tidak	

D.6 Checklist Network

Area Pemeriksaan	Pertanyaan Desain	Status	Catatan
Arsitektur	Apakah desain jaringan memakai three-tier atau spine-leaf?	Ya / Tidak	
ToR/EoR	Apakah model ToR, EoR, atau campuran sudah dipilih?	Ya / Tidak	
Underlay	Apakah desain underlay network sudah jelas?	Ya / Tidak	
Overlay	Apakah VXLAN/EVPN atau overlay lain diperlukan?	Ya / Tidak	
VLAN/VRF	Apakah segmentasi VLAN/VRF sudah dipetakan?	Ya / Tidak	
IP plan	Apakah perencanaan IP tersedia?	Ya / Tidak	
Routing	Apakah routing internal dan failover sudah dirancang?	Ya / Tidak	
Redundansi link	Apakah link kritikal memiliki jalur cadangan?	Ya / Tidak	
Bandwidth	Apakah kebutuhan bandwidth awal dan 5 tahun dihitung?	Ya / Tidak	
DCI	Apakah Data Center Interconnect diperlukan?	Ya / Tidak	
DR site	Apakah koneksi ke DR site sudah dirancang?	Ya / Tidak	
OOB	Apakah jaringan out-of-band management tersedia?	Ya / Tidak	
Telemetry	Apakah monitoring jaringan dan telemetry disiapkan?	Ya / Tidak	
Dokumentasi port	Apakah tabel port dan koneksi tersedia?	Ya / Tidak	

D.7 Checklist Security

Area Pemeriksaan	Pertanyaan Desain	Status	Catatan
Perimeter	Apakah perimeter fisik diamankan?	Ya / Tidak	
Access control	Apakah akses ruang kritikal dikendalikan?	Ya / Tidak	
CCTV	Apakah CCTV mencakup area kritikal?	Ya / Tidak	
Mantrap	Apakah mantrap diperlukan?	Ya / Tidak	
Visitor log	Apakah tamu dan vendor wajib tercatat?	Ya / Tidak	
Escort policy	Apakah tamu/vendor wajib didampingi?	Ya / Tidak	
Rack lock	Apakah rack kritikal dikunci?	Ya / Tidak	
Segmentasi jaringan	Apakah jaringan dipisah berdasarkan zona risiko?	Ya / Tidak	
Firewall/ACL	Apakah kontrol antar-zona tersedia?	Ya / Tidak	
IDS/IPS	Apakah deteksi/pencegahan intrusi diperlukan?	Ya / Tidak	
MFA	Apakah akses admin memakai MFA?	Ya / Tidak	
Bastion	Apakah akses admin melalui bastion?	Ya / Tidak	
Logging	Apakah semua akses penting tercatat?	Ya / Tidak	
OT security	Apakah BMS, DCIM, UPS, dan cooling controller dipisah?	Ya / Tidak	
Backup security	Apakah backup terlindungi dari ransomware?	Ya / Tidak	
Audit trail	Apakah bukti keamanan siap diaudit?	Ya / Tidak	

D.8 Checklist Fire Protection

Area Pemeriksaan	Pertanyaan Desain	Status	Catatan
Fire risk	Apakah risiko kebakaran sudah dianalisis?	Ya / Tidak	
Deteksi dini	Apakah sistem deteksi asap dini tersedia?	Ya / Tidak	
Alarm kebakaran	Apakah alarm terhubung ke sistem monitoring?	Ya / Tidak	
Sistem pemadaman	Apakah sistem pemadaman sesuai ruang kritikal?	Ya / Tidak	
Zonasi	Apakah ruang kritikal memiliki zonasi proteksi?	Ya / Tidak	
Panel listrik	Apakah panel dan baterai memiliki proteksi sesuai risiko?	Ya / Tidak	
Jalur evakuasi	Apakah jalur evakuasi jelas dan bebas hambatan?	Ya / Tidak	
Material ruang	Apakah material ruang mendukung keselamatan kebakaran?	Ya / Tidak	
Integrasi HVAC	Apakah shutdown/isolasi HVAC saat kebakaran dirancang?	Ya / Tidak	
Integrasi akses	Apakah pintu dan akses darurat sesuai prosedur keselamatan?	Ya / Tidak	
Uji sistem	Apakah fire alarm dan sistem pemadaman dijadwalkan diuji?	Ya / Tidak	
SOP darurat	Apakah EOP kebakaran tersedia?	Ya / Tidak	
Bukti inspeksi	Apakah sertifikat inspeksi dan maintenance tersedia?	Ya / Tidak	

D.9 Checklist Monitoring

Area Pemeriksaan	Pertanyaan Desain	Status	Catatan
DCIM	Apakah DCIM atau sistem setara diperlukan?	Ya / Tidak	
Dashboard power	Apakah status utility, UPS, generator, PDU dipantau?	Ya / Tidak	
Dashboard cooling	Apakah CRAC/CRAH, chiller, suhu, airflow dipantau?	Ya / Tidak	
Sensor suhu	Apakah suhu inlet rack dipantau?	Ya / Tidak	
Sensor kelembaban	Apakah RH dan dew point dipantau?	Ya / Tidak	
Leak detection	Apakah kebocoran air dipantau?	Ya / Tidak	
Network monitoring	Apakah link, latency, error, dan routing dipantau?	Ya / Tidak	
Security monitoring	Apakah akses fisik dan log keamanan dipantau?	Ya / Tidak	
Capacity dashboard	Apakah space, power, cooling, dan port dipantau?	Ya / Tidak	
Alarm threshold	Apakah ambang batas alarm ditentukan?	Ya / Tidak	
Eskalasi	Apakah jalur eskalasi alarm jelas?	Ya / Tidak	
Retensi log	Apakah masa simpan log ditentukan?	Ya / Tidak	
Laporan berkala	Apakah laporan operasi bulanan dirancang?	Ya / Tidak	

D.10 Checklist Documentation

Area Pemeriksaan	Dokumen yang Dibutuhkan	Status	Catatan
Design brief	Tujuan bisnis, risiko, kapasitas, target sertifikasi	Ada / Tidak	
BRD	Kebutuhan bisnis, SLA, RTO, RPO	Ada / Tidak	
Risk register	Risiko utama dan kontrol	Ada / Tidak	
Layout site	Denah lokasi dan ruang	Ada / Tidak	
Layout rack	Posisi rack dan lorong	Ada / Tidak	
SLD power	Single line diagram listrik	Ada / Tidak	
Diagram cooling	CRAC/CRAH, chiller, airflow	Ada / Tidak	
Diagram network	Fisik dan logis	Ada / Tidak	
Tabel VLAN/VRF	Segmentasi jaringan	Ada / Tidak	
IP plan	Alamat IP dan manajemen	Ada / Tidak	
Security zoning	Zona keamanan dan kontrol akses	Ada / Tidak	
Fire protection plan	Deteksi dan pemadaman kebakaran	Ada / Tidak	
Monitoring plan	Sensor, dashboard, alarm, eskalasi	Ada / Tidak	
Capacity plan	Kapasitas awal, 3 tahun, 5 tahun	Ada / Tidak	
Commissioning plan	FAT, SAT, IST	Ada / Tidak	
SOP	Operasi rutin	Ada / Tidak	
MOP	Pekerjaan kritis	Ada / Tidak	
EOP	Kondisi darurat	Ada / Tidak	
As-built	Kondisi aktual setelah deployment	Ada / Tidak	
Evidence pack	Bukti audit dan sertifikasi	Ada / Tidak	

D.11 Ringkasan Status Desain

Domain	Status Umum	Risiko Utama	Tindakan Lanjut
Site	Siap / Belum		
Space	Siap / Belum		
Rack	Siap / Belum		
Power	Siap / Belum		
Cooling	Siap / Belum		
Network	Siap / Belum		
Security	Siap / Belum		
Fire protection	Siap / Belum		
Monitoring	Siap / Belum		
Documentation	Siap / Belum		

D.12 Persetujuan Review Desain

Nama	Peran	Tanda Tangan	Tanggal
	Pemilik Bisnis		
	Data Center Architect		
	Facility / MEP Engineer		
	Network Engineer		
	Security Officer		
	Operations Lead		
	Auditor / Reviewer		

Catatan Penutup:

Checklist desain ini harus digunakan sebelum pengadaan dan deployment. **Semakin banyak gap ditemukan di tahap desain, semakin murah dan aman perbaikannya.** Gap yang baru ditemukan saat commissioning atau operasi biasanya jauh lebih mahal, lebih berisiko, dan lebih sulit dipertanggungjawabkan saat audit.

Lampiran E. Checklist Deployment dan Commissioning

Tujuan:

Checklist ini digunakan untuk memastikan seluruh proses *deployment*, pengujian, *commissioning*, dan *handover data center* dilakukan secara **terstruktur, terdokumentasi, aman, dan siap audit**.

Prinsip utama: **data center belum siap produksi sampai semua sistem kritikal diuji, dibuktikan, dan diserahterimakan secara formal.**

E.1 Checklist FAT — Factory Acceptance Test

FAT dilakukan sebelum perangkat dikirim ke lokasi proyek. Tujuannya memastikan perangkat sesuai spesifikasi kontrak dan layak dikirim.

Area Pemeriksaan	Pertanyaan / Aktivitas	Status	Catatan
Dokumen teknis	Apakah datasheet, manual, dan sertifikat tersedia?	Ya / Tidak	
Kesesuaian spesifikasi	Apakah perangkat sesuai BoQ dan spesifikasi teknis?	Ya / Tidak	
Kapasitas perangkat	Apakah kapasitas sesuai desain?	Ya / Tidak	
Nomor seri	Apakah serial number dicatat?	Ya / Tidak	
Pemeriksaan fisik	Apakah kondisi fisik baik?	Ya / Tidak	
Pengujian fungsi dasar	Apakah fungsi utama berhasil diuji?	Ya / Tidak	
Pengujian alarm	Apakah alarm lokal bekerja?	Ya / Tidak	
Pengujian proteksi	Apakah proteksi dasar bekerja?	Ya / Tidak	
Pengujian kontrol	Apakah panel kontrol / interface bekerja?	Ya / Tidak	
Label perangkat	Apakah label perangkat sesuai?	Ya / Tidak	
Aksesori	Apakah aksesori, kabel, modul, dan komponen pendukung lengkap?	Ya / Tidak	
Laporan FAT	Apakah laporan FAT dibuat?	Ya / Tidak	
Temuan FAT	Apakah semua temuan kritikal ditutup?	Ya / Tidak	
Persetujuan pengiriman	Apakah perangkat disetujui untuk dikirim?	Ya / Tidak	

Catatan: FAT sebaiknya dilakukan untuk perangkat kritikal seperti **UPS, generator, ATS/AMF, panel listrik, chiller, CRAC/CRAH, sistem fire protection, switch utama, firewall, DCIM, dan access control**.

E.2 Checklist SAT — Site Acceptance Test

SAT dilakukan setelah perangkat terpasang di lokasi. Tujuannya memastikan perangkat bekerja dalam kondisi instalasi aktual.

Area Pemeriksaan	Pertanyaan / Aktivitas	Status	Catatan
Penerimaan barang	Apakah perangkat diterima dalam kondisi baik?	Ya / Tidak	
Kesesuaian lokasi	Apakah perangkat dipasang di lokasi yang benar?	Ya / Tidak	
Instalasi mekanikal	Apakah pemasangan fisik kuat dan rapi?	Ya / Tidak	
Instalasi listrik	Apakah koneksi listrik sesuai desain?	Ya / Tidak	
Grounding	Apakah grounding dan bonding terpasang benar?	Ya / Tidak	
Kabel data	Apakah kabel data sesuai jalur dan label?	Ya / Tidak	
Kabel power	Apakah kabel power sesuai jalur A/B?	Ya / Tidak	
Labeling	Apakah semua perangkat, kabel, port, dan panel diberi label?	Ya / Tidak	
Konfigurasi awal	Apakah konfigurasi dasar selesai?	Ya / Tidak	
Integrasi monitoring	Apakah perangkat terbaca di dashboard monitoring/DCIM?	Ya / Tidak	
Pengujian alarm	Apakah alarm muncul di sistem monitoring?	Ya / Tidak	
Pengujian fungsi	Apakah fungsi utama berjalan normal?	Ya / Tidak	
Dokumentasi SAT	Apakah laporan SAT dibuat?	Ya / Tidak	
Temuan SAT	Apakah temuan kritis ditutup?	Ya / Tidak	
Persetujuan SAT	Apakah SAT ditandatangani pihak terkait?	Ya / Tidak	

Catatan: SAT tidak hanya memeriksa perangkat menyala. SAT harus membuktikan bahwa perangkat **terpasang benar, terhubung benar, terpantau, dan aman digunakan**.

E.3 Checklist Load Bank Test

Load bank test digunakan untuk menguji sistem listrik dan cooling dengan beban simulasi. Ini penting karena data center kosong sering terlihat normal, tetapi gagal saat beban meningkat.

Area Pemeriksaan	Pertanyaan / Aktivitas	Status	Catatan
Rencana uji	Apakah skenario load bank test disetujui?	Ya / Tidak	
Kapasitas load bank	Apakah kapasitas load bank sesuai target uji?	Ya / Tidak	
Keselamatan kerja	Apakah prosedur keselamatan tersedia?	Ya / Tidak	
Area uji	Apakah lokasi load bank aman dan cukup ventilasi?	Ya / Tidak	
Beban bertahap	Apakah pengujian dilakukan bertahap?	Ya / Tidak	
Beban 25%	Apakah sistem stabil pada beban 25%?	Ya / Tidak	
Beban 50%	Apakah sistem stabil pada beban 50%?	Ya / Tidak	
Beban 75%	Apakah sistem stabil pada beban 75%?	Ya / Tidak	
Beban 100%	Apakah sistem stabil pada beban 100% desain?	Ya / Tidak	
UPS	Apakah UPS stabil saat diberi beban?	Ya / Tidak	
Generator	Apakah generator stabil saat load test?	Ya / Tidak	
ATS/AMF	Apakah transfer berjalan benar?	Ya / Tidak	
PDU/RPP	Apakah distribusi daya stabil?	Ya / Tidak	
Cooling	Apakah cooling mampu membuang panas load bank?	Ya / Tidak	
Suhu inlet rack	Apakah suhu tetap dalam batas aman?	Ya / Tidak	
Alarm	Apakah alarm muncul sesuai kondisi?	Ya / Tidak	
Data logging	Apakah tegangan, arus, frekuensi, suhu, dan alarm dicatat?	Ya / Tidak	
Laporan uji	Apakah laporan load bank test dibuat?	Ya / Tidak	

Catatan penting: *load bank test* harus dirancang hati-hati agar tidak merusak perangkat, membahayakan personel, atau menimbulkan panas berlebih di area uji.

E.4 Checklist Integrated System Test — IST

IST adalah pengujian lintas sistem. Tujuannya membuktikan bahwa **power, cooling, network, security, monitoring, dan operasi manusia** bekerja bersama saat terjadi skenario nyata.

Area Pemeriksaan	Pertanyaan / Aktivitas	Status	Catatan
Rencana IST	Apakah skenario IST disetujui semua pihak?	Ya / Tidak	
Tim operasi	Apakah tim operasi ikut dalam IST?	Ya / Tidak	
Tim vendor	Apakah vendor sistem kritikal hadir?	Ya / Tidak	
Keselamatan	Apakah risiko pengujian sudah dianalisis?	Ya / Tidak	
Rollback plan	Apakah rencana rollback tersedia?	Ya / Tidak	
Skenario utility failure	Apakah listrik utama diputus secara terkontrol?	Ya / Tidak	
UPS response	Apakah UPS mengambil beban sesuai desain?	Ya / Tidak	
Generator response	Apakah generator menyala dan stabil?	Ya / Tidak	
ATS transfer	Apakah ATS berpindah sesuai desain?	Ya / Tidak	
Cooling continuity	Apakah cooling tetap bekerja saat skenario berjalan?	Ya / Tidak	
Network continuity	Apakah jaringan tetap berjalan?	Ya / Tidak	
Security continuity	Apakah CCTV, access control, dan alarm tetap aktif?	Ya / Tidak	
Monitoring	Apakah semua event terekam di dashboard/log?	Ya / Tidak	
EOP execution	Apakah tim menjalankan EOP dengan benar?	Ya / Tidak	
Komunikasi	Apakah jalur komunikasi insiden berjalan?	Ya / Tidak	
Catatan waktu	Apakah waktu tiap event dicatat?	Ya / Tidak	
Temuan IST	Apakah semua temuan dicatat dalam punch list?	Ya / Tidak	
Persetujuan IST	Apakah hasil IST ditandatangani?	Ya / Tidak	

Prinsip: IST bukan sekadar uji teknis. IST adalah **latihan nyata operasi data center saat sistem mengalami gangguan**.

E.5 Checklist Failover Test

Failover test memastikan sistem cadangan benar-benar bekerja saat sistem utama gagal.

Sistem	Skenario Uji	Hasil yang Diharapkan	Status	Catatan
Utility ke UPS	Listrik utama diputus	UPS mengambil beban tanpa gangguan	Ya / Tidak	
UPS ke generator	Utility gagal lebih lama	Generator menyala dan ATS berpindah	Ya / Tidak	
Generator utama gagal	Generator utama dimatikan	Generator cadangan mengambil alih jika tersedia	Ya / Tidak	
UPS module failure	Satu modul UPS gagal	Beban tetap tersuplai	Ya / Tidak	
Cooling unit failure	Satu CRAC/CRAH dimatikan	Cooling cadangan menjaga suhu aman	Ya / Tidak	
Chiller failure	Satu chiller gagal	Chiller cadangan mengambil beban	Ya / Tidak	
Pump failure	Satu pump dimatikan	Pump cadangan bekerja	Ya / Tidak	
Network link failure	Satu uplink putus	Trafik berpindah ke link lain	Ya / Tidak	
Spine/leaf failure	Satu perangkat jaringan mati	Trafik tetap berjalan sesuai desain	Ya / Tidak	
Firewall failover	Firewall utama dimatikan	Firewall pasangan mengambil alih	Ya / Tidak	
DCI failover	Jalur antar-site utama putus	Jalur cadangan aktif	Ya / Tidak	
Monitoring failure	Salah satu collector gagal	Monitoring tetap tersedia jika dirancang redundant	Ya / Tidak	

Catatan: hasil *failover test* harus mencatat **durasi perpindahan, dampak layanan, alarm yang muncul, log yang terbentuk, dan tindakan koreksi.**

E.6 Checklist Security Test

Pengujian keamanan memastikan kontrol akses, segmentasi, logging, alarm, dan respons insiden bekerja sesuai desain.

Area Pemeriksaan	Pertanyaan / Aktivitas	Status	Catatan
Access control	Apakah kartu akses hanya berlaku untuk personel berwenang?	Ya / Tidak	
Akses ditolak	Apakah akses tidak sah ditolak dan tercatat?	Ya / Tidak	
Door alarm	Apakah pintu terbuka terlalu lama memicu alarm?	Ya / Tidak	
CCTV	Apakah kamera merekam area kritis?	Ya / Tidak	
Rekaman CCTV	Apakah rekaman dapat diputar ulang?	Ya / Tidak	
Visitor log	Apakah tamu/vendor tercatat?	Ya / Tidak	
Escort policy	Apakah tamu/vendor didampingi?	Ya / Tidak	
Rack lock	Apakah rack kritis terkunci?	Ya / Tidak	
Network segmentation	Apakah zona user, server, storage, backup, management, dan OT terpisah?	Ya / Tidak	
Firewall rule	Apakah akses antar-zona sesuai policy?	Ya / Tidak	
IDS/IPS	Apakah deteksi/pencegahan intrusi diuji?	Ya / Tidak	
MFA admin	Apakah akses admin memakai MFA?	Ya / Tidak	
Bastion	Apakah akses manajemen melalui bastion?	Ya / Tidak	
Logging admin	Apakah login dan perubahan konfigurasi tercatat?	Ya / Tidak	
OT security	Apakah BMS, DCIM, UPS, cooling controller tersegmentasi?	Ya / Tidak	
Backup access	Apakah akses backup dibatasi?	Ya / Tidak	
Incident drill	Apakah simulasi insiden keamanan dilakukan?	Ya / Tidak	
Laporan security test	Apakah laporan pengujian keamanan dibuat?	Ya / Tidak	

Catatan: keamanan yang tidak diuji hanya berupa asumsi. Untuk sertifikasi, yang dibutuhkan adalah **bukti kontrol bekerja**.

E.7 Checklist Handover Document

Dokumen *handover* memastikan tim operasi menerima fasilitas dalam kondisi siap dijalankan, dipelihara, diaudit, dan dikembangkan.

Dokumen / Bukti	Status	Catatan
Dokumen Data Center Design Brief	Ada / Tidak	
Dokumen HLD	Ada / Tidak	
Dokumen LLD	Ada / Tidak	
Layout ruang final	Ada / Tidak	
Layout rack final	Ada / Tidak	
Single line diagram listrik	Ada / Tidak	
Diagram cooling	Ada / Tidak	
Diagram jaringan fisik	Ada / Tidak	
Diagram jaringan logis	Ada / Tidak	
Tabel VLAN/VRF/VNI	Ada / Tidak	
IP address plan	Ada / Tidak	
Tabel port dan patching	Ada / Tidak	
Daftar aset	Ada / Tidak	
Daftar serial number	Ada / Tidak	
Daftar warranty	Ada / Tidak	
Daftar vendor dan kontak darurat	Ada / Tidak	
Manual perangkat	Ada / Tidak	
Laporan FAT	Ada / Tidak	
Laporan SAT	Ada / Tidak	
Laporan load bank test	Ada / Tidak	
Laporan integrated system test	Ada / Tidak	
Laporan failover test	Ada / Tidak	
Laporan security test	Ada / Tidak	
Punch list dan status penyelesaian	Ada / Tidak	
SOP operasi harian	Ada / Tidak	

MOP pekerjaan kritikal	Ada / Tidak	
EOP kondisi darurat	Ada / Tidak	
Jadwal preventive maintenance	Ada / Tidak	
Baseline konfigurasi	Ada / Tidak	
Backup konfigurasi perangkat	Ada / Tidak	
Daftar akun dan hak akses	Ada / Tidak	
Training record tim operasi	Ada / Tidak	
Berita acara serah terima	Ada / Tidak	

Catatan: *handover* tidak sah secara operasional jika dokumen, akses, pelatihan, hasil uji, dan daftar isu belum jelas.

E.8 Template Ringkasan Status Commissioning

Area	Status	Temuan Kritisal	PIC	Target Penyelesaian
FAT	Lulus / Belum			
SAT	Lulus / Belum			
Load bank test	Lulus / Belum			
Integrated system test	Lulus / Belum			
Failover test	Lulus / Belum			
Security test	Lulus / Belum			
Handover document	Lengkap / Belum			

E.9 Template Persetujuan Commissioning

Nama	Peran	Persetujuan	Tanda Tangan	Tanggal
	Pemilik Proyek	Setuju / Tidak		
	Konsultan Desain	Setuju / Tidak		
	Facility / MEP Lead	Setuju / Tidak		
	Network Lead	Setuju / Tidak		
	Security Lead	Setuju / Tidak		
	Operations Lead	Setuju / Tidak		
	Vendor / Kontraktor	Setuju / Tidak		
	Auditor / Reviewer	Setuju / Tidak		

E.10 Checklist Final Sebelum Go-Live

Pertanyaan Final	Status
Apakah semua FAT perangkat kritikal lulus?	Ya / Tidak
Apakah semua SAT perangkat terpasang lulus?	Ya / Tidak
Apakah load bank test selesai dan terdokumentasi?	Ya / Tidak
Apakah integrated system test selesai dan terdokumentasi?	Ya / Tidak
Apakah failover test selesai dan berhasil?	Ya / Tidak
Apakah security test selesai dan temuan kritikal ditutup?	Ya / Tidak
Apakah semua alarm masuk ke dashboard monitoring?	Ya / Tidak
Apakah tim operasi ikut dalam commissioning?	Ya / Tidak
Apakah SOP, MOP, dan EOP tersedia?	Ya / Tidak
Apakah training tim operasi selesai?	Ya / Tidak
Apakah dokumen as-built lengkap?	Ya / Tidak
Apakah punch list kritikal sudah ditutup?	Ya / Tidak
Apakah punch list non-kritikal memiliki target penyelesaian?	Ya / Tidak
Apakah handover document lengkap?	Ya / Tidak
Apakah berita acara serah terima ditandatangani?	Ya / Tidak
Apakah fasilitas disetujui untuk go-live?	Ya / Tidak

Catatan Penutup:

Checklist ini harus digunakan sebagai **evidence pack** untuk audit dan sertifikasi. Fasilitas yang sudah menyala belum tentu siap operasi. *Data center* baru benar-benar siap ketika **semua sistem kritikal lulus uji, semua temuan tercatat, semua dokumen lengkap, dan tim operasi siap mengambil alih tanggung jawab.**

Lampiran F. Checklist Operasi Harian Data Center

Tujuan:

Checklist ini digunakan oleh tim operasi untuk memastikan kondisi *data center* tetap **stabil, aman, terukur, dan terdokumentasi** setiap hari.

Prinsip utama: **operasi harian bukan sekadar melihat dashboard, tetapi memastikan setiap anomali dicatat, eskalasi, dan ditindaklanjuti.**

F.1 Informasi Shift Operasi

Item	Keterangan
Tanggal	
Shift	Pagi / Siang / Malam
Petugas Operasi	
Supervisor	
Jam Pemeriksaan	
Status Umum Data Center	Normal / Waspada / Kritis
Catatan Umum	

F.2 Checklist Suhu

Area Pemeriksaan	Parameter	Batas Aman	Status	Catatan
Suhu ruang data center	°C	Sesuai standar internal	Normal / Waspada / Kritis	
Suhu cold aisle	°C		Normal / Waspada / Kritis	
Suhu hot aisle	°C		Normal / Waspada / Kritis	
Suhu inlet rack tertinggi	°C		Normal / Waspada / Kritis	
Suhu outlet rack tertinggi	°C		Normal / Waspada / Kritis	
Rack dengan suhu tertinggi	Nama rack		Normal / Waspada / Kritis	
Perubahan suhu mendadak	Ada / Tidak	Tidak ada	Normal / Waspada / Kritis	

Catatan tindakan:

Jika suhu *inlet* rack naik tidak normal, segera cek **airflow**, **CRAC/CRAH**, celah kabel, **blanking panel**, dan beban rack.

F.3 Checklist Kelembaban

Area Pemeriksaan	Parameter	Batas Aman	Status	Catatan
Kelembaban ruang	RH %	Sesuai standar internal	Normal / Waspada / Kritis	
Dew point	°C	Sesuai standar internal	Normal / Waspada / Kritis	
Risiko kondensasi	Ada / Tidak	Tidak ada	Normal / Waspada / Kritis	
Risiko ESD	Ada / Tidak	Tidak ada	Normal / Waspada / Kritis	
Alarm kelembapan	Ada / Tidak	Tidak ada	Normal / Waspada / Kritis	

Catatan tindakan:

Kelembapan terlalu tinggi meningkatkan risiko **kondensasi dan korosi**. Kelembapan terlalu rendah meningkatkan risiko **ESD**.

F.4 Checklist Alarm

Jenis Alarm	Status	Waktu Muncul	Dampak	Tindakan	PIC
Alarm power	Ada / Tidak				
Alarm UPS	Ada / Tidak				
Alarm generator	Ada / Tidak				
Alarm cooling	Ada / Tidak				
Alarm suhu	Ada / Tidak				
Alarm kelembaban	Ada / Tidak				
Alarm kebocoran air	Ada / Tidak				
Alarm fire protection	Ada / Tidak				
Alarm access control	Ada / Tidak				
Alarm jaringan	Ada / Tidak				
Alarm keamanan	Ada / Tidak				

Catatan penting:

Alarm tidak boleh hanya di-*acknowledge*. Alarm harus memiliki **analisis, tindakan, PIC, dan status penyelesaian**.

F.5 Checklist UPS

Area Pemeriksaan	Parameter	Status	Catatan
Status UPS utama	Normal / Alarm / Bypass / Fault		
Beban UPS	% / kW	Normal / Waspada / Kritis	
Kapasitas tersisa	%	Normal / Waspada / Kritis	
Status baterai	Normal / Alarm / Lemah		
Estimasi runtime	Menit	Normal / Waspada / Kritis	
Suhu ruang UPS / baterai	°C	Normal / Waspada / Kritis	
Status bypass	Aktif / Tidak aktif	Normal / Waspada / Kritis	
Alarm UPS	Ada / Tidak		
Log event UPS	Ada / Tidak		

Catatan tindakan:

Jika UPS masuk mode *bypass*, *overload*, atau baterai alarm, segera eskalasi ke **facility lead** dan ikuti EOP UPS.

F.6 Checklist Generator

Area Pemeriksaan	Parameter	Status	Catatan
Status generator	Ready / Running / Alarm / Fault		
Mode operasi	Auto / Manual		
Level bahan bakar	% / liter	Normal / Waspada / Kritis	
Tegangan baterai starter	Volt	Normal / Waspada / Kritis	
Oli / coolant	Normal / Kurang / Alarm		
Suhu mesin	°C	Normal / Waspada / Kritis	
Alarm generator	Ada / Tidak		
Status ATS/AMF	Normal / Alarm / Fault		
Area generator bersih dan aman	Ya / Tidak		
Jadwal test terakhir	Tanggal		

Catatan tindakan:

Generator harus selalu berada dalam kondisi **siap start otomatis**. Mode manual tanpa alasan jelas adalah risiko operasional.

F.7 Checklist PDU / Rack PDU

Area Pemeriksaan	Parameter	Status	Catatan
PDU utama	Normal / Alarm / Fault		
Beban PDU A	Ampere / kW	Normal / Waspada / Kritis	
Beban PDU B	Ampere / kW	Normal / Waspada / Kritis	
Keseimbangan jalur A/B	Seimbang / Tidak seimbang		
Rack PDU overload	Ada / Tidak		
Breaker trip	Ada / Tidak		
Suhu panel/PDU	Normal / Panas		
Label PDU jelas	Ya / Tidak		
Log PDU tersedia	Ya / Tidak		

Catatan tindakan:

Jika jalur A/B tidak seimbang, jangan langsung memindahkan kabel. Buat **MOP**, cek dampak perangkat, dan pastikan tidak mematikan beban kritikal.

F.8 Checklist CRAC / CRAH

Area Pemeriksaan	Parameter	Status	Catatan
Status CRAC/CRAH utama	Normal / Alarm / Fault		
Unit aktif	Jumlah unit		
Unit standby	Jumlah unit		
Suhu supply air	°C	Normal / Waspada / Kritis	
Suhu return air	°C	Normal / Waspada / Kritis	
Fan status	Normal / Alarm		
Filter	Bersih / Kotor / Perlu ganti		
Kondisi coil	Normal / Perlu inspeksi		
Drain / kondensat	Normal / Tersumbat		
Alarm cooling	Ada / Tidak		
Leak detection sekitar unit	Normal / Alarm		

Catatan tindakan:

Jika satu unit cooling gagal, segera cek **suhu inlet rack**, status unit cadangan, dan jalankan EOP cooling jika suhu naik.

F.9 Checklist Access Log

Area Pemeriksaan	Pertanyaan	Status	Catatan
Log akses ruang data center tersedia	Ya / Tidak		
Semua akses hari ini sesuai izin	Ya / Tidak		
Ada akses ditolak	Ya / Tidak		
Ada pintu terbuka terlalu lama	Ya / Tidak		
Ada tamu/vendor masuk	Ya / Tidak		
Tamu/vendor mengisi visitor log	Ya / Tidak		
Tamu/vendor didampingi	Ya / Tidak		
Akses ruang UPS/baterai tercatat	Ya / Tidak		
Akses ruang cooling tercatat	Ya / Tidak		
CCTV area akses aktif	Ya / Tidak		

Log Tamu / Vendor

Waktu Masuk	Nama	Instansi	Tujuan	Area Diakses	Pendamping	Waktu Keluar	Tanda Tangan

Catatan penting:

Setiap akses fisik ke area kritikal harus bisa dijelaskan melalui **identitas, waktu, tujuan, pendamping, dan area yang diakses**.

F.10 Checklist Incident Log

No	Waktu	Jenis Insiden	Area Terdampak	Dampak	Tindakan Awal	Status	PIC
1		Power / Cooling / Network / Security / Access / Fire / Leak / Lainnya				Open / Closed	
2							
3							

Detail Insiden

Item	Keterangan
Nomor insiden	
Waktu mulai	
Waktu selesai	
Deteksi awal	Alarm / Sensor / Petugas / User / Vendor
Sistem terdampak	
Dampak layanan	
Akar masalah sementara	
Tindakan pemulihan	
Eskalasi ke	
Bukti yang dikumpulkan	Log / Foto / Screenshot / CCTV / Tiket
Perlu RCA?	Ya / Tidak
Status akhir	Open / Monitoring / Closed

Catatan tindakan:

Insiden kecil yang berulang harus diperlakukan sebagai **sinyal risiko besar**.

F.11 Checklist Capacity Log

Area Kapasitas	Parameter	Nilai Hari Ini	Status	Catatan
Rack space	U kosong total		Aman / Waspada / Kritis	
Rack tersedia	Jumlah rack kosong		Aman / Waspada / Kritis	
Power per rack	kW/rack tertinggi		Aman / Waspada / Kritis	
PDU capacity	Kapasitas tersisa		Aman / Waspada / Kritis	
UPS capacity	Kapasitas tersisa		Aman / Waspada / Kritis	
Generator capacity	Kapasitas tersisa		Aman / Waspada / Kritis	
Cooling capacity	Kapasitas tersisa		Aman / Waspada / Kritis	
Port jaringan	Port tersedia		Aman / Waspada / Kritis	
Storage capacity	Kapasitas tersedia		Aman / Waspada / Kritis	
Backup capacity	Kapasitas tersedia		Aman / Waspada / Kritis	

Perubahan Kapasitas Hari Ini

Perubahan	Perangkat / Area	Dampak ke Rack	Dampak ke Power	Dampak ke Cooling	Dampak ke Network	Catatan
Penambahan						
Pengurangan						
Pemindahan						

Catatan penting:

Kapasitas tidak boleh hanya dilihat dari rack kosong. Kapasitas harus dilihat dari **space, power, cooling, port, berat rack, dan jalur kabel**.

F.12 Ringkasan Harian Operasi

Area	Status	Catatan Penting
Suhu	Normal / Waspada / Kritis	
Kelembapan	Normal / Waspada / Kritis	
Alarm	Normal / Waspada / Kritis	
UPS	Normal / Waspada / Kritis	
Generator	Normal / Waspada / Kritis	
PDU	Normal / Waspada / Kritis	
CRAC/CRAH	Normal / Waspada / Kritis	
Access log	Normal / Waspada / Kritis	
Incident log	Normal / Waspada / Kritis	
Capacity log	Normal / Waspada / Kritis	

F.13 Eskalasi

Kondisi	Eskalasi ke	Waktu Maksimum
Alarm kritikal power	Facility Lead	Segera
UPS masuk bypass/fault	Facility Lead + Vendor	Segera
Generator gagal start	Facility Lead + Vendor	Segera
Suhu rack kritikal naik	Facility Lead + Operations Lead	Segera
Cooling unit gagal	Facility Lead	Segera
Leak detection aktif	Facility Lead + Security	Segera
Akses tidak sah	Security Lead	Segera
Insiden jaringan kritikal	Network Lead	Segera
Kapasitas power/cooling kritis	Data Center Manager	Hari yang sama
Insiden berdampak layanan	Management + Incident Manager	Segera

F.14 Persetujuan Shift

Nama	Peran	Tanda Tangan	Waktu
	Petugas Shift		
	Supervisor Shift		
	Operations Lead		

Catatan Penutup:

Checklist operasi harian ini harus disimpan sebagai **bukti audit operasi**. Data center yang baik bukan hanya yang tidak mengalami gangguan, tetapi yang mampu menunjukkan bahwa kondisi kritikalnya **dipantau, dicatat, dianalisis, dan ditindaklanjuti setiap hari**.

Glosarium

Istilah	Arti / Penjelasan
<i>Access Control</i>	Sistem untuk mengatur siapa yang boleh masuk ke area tertentu, misalnya ruang data center, ruang UPS, ruang baterai, atau ruang jaringan.
<i>Airflow</i>	Aliran udara di dalam data center, terutama aliran udara dingin ke depan rack dan udara panas keluar dari belakang rack.
Alarm	Peringatan dari sistem monitoring ketika terjadi kondisi tidak normal, misalnya suhu tinggi, UPS fault, pintu terbuka, atau kebocoran air.
ASHRAE TC 9.9	Komite teknis ASHRAE yang banyak menjadi rujukan untuk lingkungan termal, kelembaban, cooling, dan efisiensi energi data center.
<i>As-Built Document</i>	Dokumen kondisi aktual setelah instalasi selesai, mencakup layout, kabel, power, cooling, jaringan, sensor, dan perangkat yang benar-benar terpasang.
<i>ATS (Automatic Transfer Switch)</i>	Perangkat untuk memindahkan sumber listrik dari utility ke generator atau sebaliknya secara otomatis.
<i>Availability</i>	Tingkat ketersediaan layanan atau infrastruktur agar tetap dapat digunakan sesuai target bisnis.
<i>Backup</i>	Salinan data atau sistem yang digunakan untuk pemulihan saat terjadi kerusakan, kesalahan, kehilangan data, atau serangan ransomware.
<i>BMS (Building Management System)</i>	Sistem untuk memantau dan mengendalikan fasilitas gedung, seperti HVAC, listrik, sensor, alarm, dan sistem pendukung lainnya.
<i>Bastion Host</i>	Titik akses terkendali untuk administrator sebelum masuk ke sistem atau jaringan manajemen yang sensitif.
<i>Blanking Panel</i>	Panel penutup ruang kosong di rack untuk mencegah udara panas kembali ke sisi depan perangkat.
BTU/h	Satuan kapasitas panas atau pendinginan. Dalam data center, digunakan untuk menghitung kebutuhan cooling.
<i>Bypass Air</i>	Udara dingin yang kembali ke unit cooling tanpa melewati perangkat IT. Ini menyebabkan pemborosan energi.

<i>CAC (Cold Aisle Containment)</i>	Sistem pengurungan lorong dingin agar udara dingin langsung masuk ke sisi depan rack dan tidak bercampur dengan udara panas.
<i>Capacity Management</i>	Proses mengelola kapasitas space, power, cooling, rack, port jaringan, storage, dan backup agar cukup untuk kebutuhan sekarang dan masa depan.
<i>Capacity Review</i>	Evaluasi berkala untuk menilai sisa kapasitas data center dan memprediksi kapan kapasitas akan habis.
<i>CCTV</i>	Sistem kamera pengawas untuk memantau area kritikal, akses fisik, perimeter, ruang komputer, dan jalur masuk.
<i>Chiller</i>	Mesin pendingin yang menghasilkan air dingin untuk sistem cooling, biasanya digunakan bersama CRAH.
<i>Cold Aisle</i>	Lorong dingin di depan rack, tempat udara dingin masuk ke perangkat IT.
<i>Cold Plate</i>	Teknologi <i>liquid cooling</i> yang menempelkan pelat pendingin langsung ke komponen panas seperti CPU atau GPU.
<i>Commissioning</i>	Proses pengujian, verifikasi, dokumentasi, dan pembuktian bahwa sistem data center bekerja sesuai desain.
<i>Containment</i>	Teknik memisahkan udara panas dan dingin agar cooling lebih efisien dan risiko <i>hotspot</i> berkurang.
<i>Cooling</i>	Sistem pendinginan data center untuk membuang panas dari perangkat IT dan menjaga kondisi operasi tetap aman.
<i>Cooling Tower</i>	Perangkat untuk membuang panas dari sistem chilled water ke lingkungan luar.
<i>CRAH (Computer Room Air Handler)</i>	Unit pendingin ruang data center yang biasanya memakai chilled water untuk mendinginkan udara.
<i>CRAC (Computer Room Air Conditioner)</i>	Unit pendingin ruang data center yang biasanya memakai refrigerant langsung.
<i>CUE (Carbon Usage Effectiveness)</i>	Metrik intensitas karbon data center, yaitu emisi karbon dibanding energi IT.
<i>DCiE (Data Center Infrastructure Efficiency)</i>	Kebalikan dari PUE. Menunjukkan persentase energi fasilitas yang benar-benar dipakai oleh perangkat IT.
<i>DCI (Data Center Interconnect)</i>	Koneksi antar data center untuk DR, replikasi, migrasi beban kerja, atau operasi multi-site.

DCIM (<i>Data Center Infrastructure Management</i>)	Sistem untuk mengelola aset, kapasitas, power, cooling, sensor, rack, monitoring, reporting, dan workflow data center.
<i>Delta T</i>	Selisih suhu antara <i>outlet temperature</i> dan <i>inlet temperature</i> . Digunakan untuk memahami efektivitas perpindahan panas.
<i>Design Brief</i>	Dokumen awal yang merangkum tujuan bisnis, aplikasi kritikal, target availability, kapasitas, risiko, lokasi, keamanan, PUE, dan standar acuan.
<i>Dew Point</i>	Titik embun, yaitu suhu ketika uap air mulai mengembun. Penting untuk mencegah kondensasi di data center.
DR (<i>Disaster Recovery</i>)	Strategi pemulihan layanan setelah gangguan besar seperti bencana, kegagalan sistem, atau serangan siber.
EOP (<i>Emergency Operating Procedure</i>)	Prosedur darurat untuk menghadapi kondisi kritikal seperti listrik mati, UPS alarm, cooling gagal, kebakaran, atau kebocoran air.
ERE (<i>Energy Reuse Effectiveness</i>)	Metrik yang memperhitungkan pemanfaatan kembali energi, misalnya panas buangan data center.
ESD (<i>Electrostatic Discharge</i>)	Pelepasan listrik statis yang dapat merusak perangkat elektronik, terutama jika kelembapan terlalu rendah.
EVPN (<i>Ethernet VPN</i>)	Teknologi <i>control plane</i> berbasis BGP yang sering digunakan bersama VXLAN untuk segmentasi dan overlay data center.
<i>Failover Test</i>	Pengujian untuk memastikan sistem cadangan mengambil alih saat sistem utama gagal.
FAT (<i>Factory Acceptance Test</i>)	Pengujian perangkat di pabrik sebelum dikirim ke lokasi proyek.
<i>Fire Protection</i>	Sistem perlindungan kebakaran, mencakup deteksi, alarm, pemadaman, evakuasi, dan prosedur darurat.
<i>Free Cooling</i>	Pemanfaatan kondisi lingkungan luar untuk mengurangi beban kerja chiller atau sistem cooling mekanis.
Generator	Sumber listrik cadangan yang menyuplai data center saat listrik utama gagal.
<i>Ghost Server</i>	Server yang masih menyala tetapi tidak lagi memiliki fungsi jelas. Tetap mengonsumsi listrik, cooling, ruang, dan port.
<i>Gray Space</i>	Area pendukung data center seperti ruang UPS, panel listrik, baterai, generator, cooling plant, dan ruang MEP.

<i>Green Data Center</i>	Data center yang dirancang dan dioperasikan untuk efisiensi energi, pengurangan karbon, efisiensi air, pemanfaatan panas, dan keberlanjutan.
<i>Grounding</i>	Sistem pentanahan untuk keselamatan listrik, proteksi perangkat, dan stabilitas sistem.
<i>HAC (Hot Aisle Containment)</i>	Sistem pengurungan lorong panas agar udara panas tidak bercampur dengan udara dingin.
<i>HLD (High-Level Design)</i>	Dokumen desain tingkat tinggi yang menjelaskan arsitektur utama, prinsip desain, dan hubungan antar-sistem.
<i>Hot Aisle</i>	Lorong panas di belakang rack, tempat udara panas keluar dari perangkat IT.
<i>Hot Spot</i>	Titik panas lokal di data center, biasanya terjadi karena airflow buruk, beban rack tinggi, atau recirculation.
<i>Immersion Cooling</i>	Metode pendinginan dengan merendam perangkat ke dalam cairan dielektrik khusus.
<i>Incident Log</i>	Catatan kejadian insiden, termasuk waktu, dampak, tindakan, PIC, dan status penyelesaian.
<i>Incident Management</i>	Proses menangani insiden mulai dari deteksi, eskalasi, pemulihan, dokumentasi, hingga analisis akar masalah.
<i>Incident Response</i>	Tindakan terstruktur untuk merespons insiden agar dampak dapat dibatasi dan layanan dipulihkan.
<i>Inlet Temperature</i>	Suhu udara yang masuk ke perangkat IT, biasanya di bagian depan server atau rack.
<i>Integrated System Test</i>	Pengujian terpadu untuk membuktikan power, cooling, network, security, monitoring, dan operasi manusia bekerja bersama.
<i>IPS/IDS</i>	Sistem deteksi atau pencegahan intrusi jaringan untuk memantau dan merespons aktivitas mencurigakan.
<i>ISO/IEC 22237</i>	Standar internasional untuk fasilitas dan infrastruktur data center, mencakup konsep umum, availability, keamanan fisik, dan efisiensi energi.
<i>IT Load</i>	Total beban daya perangkat IT seperti server, storage, jaringan, keamanan, dan perangkat komputasi lain.
<i>kW (Kilowatt)</i>	Satuan daya listrik. Dalam data center digunakan untuk mengukur beban IT, facility load, UPS, generator, dan rack density.

<i>kWh (Kilowatt-hour)</i>	Satuan energi listrik. Digunakan untuk menghitung konsumsi energi dan biaya listrik.
<i>Latency</i>	Waktu tunda dalam pengiriman data. Penting untuk aplikasi real-time, storage, AI, HPC, dan edge data center.
<i>Leaf Switch</i>	Switch pada arsitektur spine-leaf yang menghubungkan server atau rack ke jaringan fabric.
<i>Leak Detection</i>	Sistem sensor untuk mendeteksi kebocoran air di area kritikal data center.
<i>Liquid Cooling</i>	Teknologi pendinginan yang memakai cairan untuk membawa panas dari perangkat IT, cocok untuk rack density tinggi.
<i>LLD (Low-Level Design)</i>	Dokumen desain detail yang memuat konfigurasi, port, IP, VLAN/VRF, kabel, parameter teknis, dan detail implementasi.
<i>Load Bank Test</i>	Pengujian dengan beban listrik simulasi untuk memvalidasi UPS, generator, distribusi power, dan cooling.
<i>Management Network</i>	Jaringan khusus untuk akses administrasi perangkat, monitoring, konfigurasi, dan troubleshooting.
<i>Mantrap</i>	Ruang perantara dengan kontrol akses bertingkat untuk mencegah orang tidak sah masuk bersama personel berwenang.
<i>MFA (Multi-Factor Authentication)</i>	Metode autentikasi dengan lebih dari satu faktor, misalnya password ditambah token atau biometrik.
<i>MOP (Method of Procedure)</i>	Prosedur kerja terencana untuk pekerjaan kritikal seperti maintenance, perubahan konfigurasi, atau penggantian perangkat.
<i>MTTR (Mean Time to Repair)</i>	Rata-rata waktu yang dibutuhkan untuk memperbaiki gangguan.
<i>N</i>	Kapasitas minimum yang dibutuhkan agar sistem berjalan tanpa cadangan tambahan.
<i>N+1</i>	Desain redundansi dengan satu unit cadangan tambahan di atas kebutuhan minimum.
<i>2N</i>	Desain redundansi dengan dua sistem penuh yang masing-masing mampu menanggung seluruh beban.
<i>NOC (Network Operations Center)</i>	Pusat pemantauan dan operasi jaringan atau layanan digital.

<i>OOB (Out-of-Band Management)</i>	Jalur manajemen terpisah untuk mengakses perangkat saat jaringan produksi bermasalah.
<i>Outlet Temperature</i>	Suhu udara panas yang keluar dari perangkat IT, biasanya di belakang server atau rack.
<i>Overlay Network</i>	Jaringan logis yang berjalan di atas jaringan fisik, misalnya VXLAN.
<i>PDU (Power Distribution Unit)</i>	Perangkat distribusi listrik ke rack atau perangkat IT.
<i>Physical Security</i>	Keamanan fisik data center, termasuk perimeter, akses, CCTV, mantrap, rack lock, dan visitor log.
<i>PUE (Power Usage Effectiveness)</i>	Metrik efisiensi energi data center: total energi fasilitas dibagi energi perangkat IT.
<i>Predictive Maintenance</i>	Perawatan berbasis tren data dan prediksi kegagalan sebelum kerusakan terjadi.
<i>Preventive Maintenance</i>	Perawatan terjadwal untuk mencegah kerusakan perangkat atau sistem.
<i>Rack</i>	Lemari standar untuk menempatkan server, storage, switch, firewall, PDU, dan perangkat data center lainnya.
<i>Rack Density</i>	Beban daya per rack, biasanya dalam kW/rack.
<i>Rack Lock</i>	Kunci rack untuk mencegah akses fisik tidak sah ke perangkat.
<i>Rack PDU</i>	PDU yang dipasang di rack untuk mendistribusikan listrik ke perangkat dalam rack.
<i>Raised Floor</i>	Lantai semu yang ditinggikan, biasanya digunakan untuk airflow, kabel, atau distribusi tertentu.
<i>Rear-Door Heat Exchanger</i>	Teknologi cooling di pintu belakang rack untuk menyerap panas dari udara keluar perangkat.
<i>Recirculation</i>	Udara panas yang kembali masuk ke sisi depan perangkat, menyebabkan suhu inlet naik.
<i>Renewable Matching</i>	Upaya mencocokkan konsumsi energi data center dengan pasokan energi terbarukan.
<i>Right-Sizing</i>	Menyesuaikan kapasitas perangkat dan layanan dengan kebutuhan nyata agar tidak boros.

RPO (<i>Recovery Point Objective</i>)	Batas maksimal kehilangan data yang dapat diterima setelah gangguan.
RTO (<i>Recovery Time Objective</i>)	Batas maksimal waktu pemulihan layanan setelah gangguan.
SAT (<i>Site Acceptance Test</i>)	Pengujian perangkat setelah dipasang di lokasi proyek untuk memastikan instalasi dan fungsi sesuai desain.
SDM Operasi	Tim manusia yang menjalankan, memelihara, memantau, dan merespons kondisi data center.
SLA (<i>Service Level Agreement</i>)	Perjanjian tingkat layanan, misalnya target availability, waktu respons, dan pemulihan.
SLD (<i>Single Line Diagram</i>)	Diagram satu garis yang menggambarkan sistem distribusi listrik data center.
SOP (<i>Standard Operating Procedure</i>)	Prosedur standar untuk pekerjaan rutin operasi harian data center.
Spine Switch	Switch inti pada arsitektur spine-leaf yang menghubungkan semua leaf switch.
Spine-Leaf Architecture	Arsitektur jaringan dua lapis yang dirancang untuk latency rendah, jalur redundan, dan skalabilitas tinggi.
Staging Area	Area untuk penerimaan, pengecekan, dan persiapan perangkat sebelum masuk ruang data center.
Stranded Capacity	Kapasitas yang terlihat tersedia tetapi tidak bisa dipakai karena bottleneck, misalnya rack kosong tetapi power atau cooling tidak cukup.
Telemetry	Pengiriman data monitoring secara kontinu dari perangkat ke sistem pengumpul data untuk observability.
TIA-942	Standar infrastruktur telekomunikasi untuk data center, mencakup site, arsitektur, electrical, mechanical, keamanan, dan cabling.
ToR (<i>Top-of-Rack</i>)	Desain penempatan switch di atas atau dekat rack, sehingga kabel server lebih pendek.
TR (<i>Ton of Refrigeration</i>)	Satuan kapasitas pendinginan. 1 TR setara sekitar 12.000 BTU/h.
UPS (<i>Uninterruptible Power Supply</i>)	Sistem catu daya tanpa putus yang menjaga perangkat tetap menyala saat listrik utama terganggu.

Uptime Tier	Klasifikasi tingkat ketersediaan infrastruktur data center yang banyak digunakan sebagai acuan desain dan sertifikasi.
Utility Power	Sumber listrik utama dari penyedia listrik.
VDI	Lingkungan desktop virtual yang berjalan di infrastruktur data center.
VLAN	Segmentasi jaringan Layer 2 untuk memisahkan trafik.
VNI (<i>VXLAN Network Identifier</i>)	Identitas segmen pada VXLAN.
VRF (<i>Virtual Routing and Forwarding</i>)	Pemisahan tabel routing untuk isolasi jaringan.
VTEP (<i>VXLAN Tunnel Endpoint</i>)	Titik awal dan akhir enkapsulasi VXLAN pada jaringan overlay.
VXLAN (<i>Virtual eXtensible LAN</i>)	Teknologi overlay untuk memperluas jaringan logis di atas jaringan IP.
Waste Heat Reuse	Pemanfaatan panas buangan data center untuk kebutuhan lain, seperti pemanas gedung atau proses industri ringan.
White Space	Area utama data center tempat rack dan perangkat IT ditempatkan.
WUE (<i>Water Usage Effectiveness</i>)	Metrik efisiensi penggunaan air data center dibanding energi IT.
Zero Trust	Prinsip keamanan yang tidak otomatis mempercayai pengguna, perangkat, atau jaringan; semua akses harus diverifikasi dan dibatasi.

Daftar Referensi

- Aitsaadi, N. (Ed.). (2021). *Management of data center networks*. Wiley-IEEE Press.
- ASHRAE. (2016). *Data center power equipment thermal guidelines and best practices*. ASHRAE Technical Committee 9.9.
https://www.ashrae.org/file%20library/technical%20resources/bookstore/ashrae_tc0909_power_white_paper_22_june_2016_revised.pdf
- ASHRAE. (2021). *Thermal guidelines for data processing environments* (5th ed.). ASHRAE Technical Committee 9.9.
<https://www.ashrae.org/file%20library/technical%20resources/bookstore/supplemental%20files/therm-gdlns-5th-r-e-refcard.pdf>
- ASHRAE. (n.d.). *ASHRAE TC 9.9: Mission critical facilities, data centers, technology spaces, and electronic equipment*. Retrieved May 8, 2026, from
<https://tpc.ashrae.org/?cmtKey=fd4a4ee6-96a3-4f61-8b85-43418dfa988d>
- Avramov, L., & Portolani, M. (2015). *The policy driven data center with ACI: Architecture, concepts, and methodology*. Cisco Press.
- Bibliotex Digital Library. (2023). *Data centre management* (3rd ed.). 3G E-Learning LLC.
- Brochard, L., Kamath, V., Corbalán, J., Holland, S., Mittelbach, W., & Ott, M. (2019). *Energy-efficient computing and data centers*. ISTE Ltd. / Wiley.
- Cybersecurity and Infrastructure Security Agency. (2025). *#StopRansomware guide*.
<https://www.cisa.gov/sites/default/files/2025-03/StopRansomware-Guide%20508.pdf>
- Geng, H. (Ed.). (2021). *Data center handbook: Plan, design, build, and operations of a smart data center* (2nd ed.). Wiley.
- International Organization for Standardization. (2021). *ISO/IEC 22237-1:2021: Information technology—Data centre facilities and infrastructures—Part 1: General concepts*.
<https://www.iso.org/standard/78550.html>
- Lammle, T., & Swartz, J. (2013). *CCNA data center: Introducing Cisco data center networking study guide*. Sybex.
- Lin, J., & Aitkenhead, G. (2023). *Data centers of the future: Reaching sustainability*. O'Reilly Media.
- Mahalingam, M., Dutt, D., Duda, K., Agarwal, P., Kreeger, L., Sridhar, T., Bursell, M., & Wright, C. (2014). *Virtual eXtensible Local Area Network (VXLAN): A framework for overlaying virtualized Layer 2 networks over Layer 3 networks* (RFC 7348). Internet Engineering Task Force. <https://datatracker.ietf.org/doc/html/rfc7348>
- National Institute of Standards and Technology. (2024). *The NIST cybersecurity framework (CSF) 2.0*. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>

- Odom, W., & Hintz, C. (2015). *CCNA data center DCICN 640-911 official cert guide*. Cisco Press.
- OpenConfig. (n.d.). *OpenConfig: Vendor-neutral network management and telemetry*. Retrieved May 8, 2026, from <https://www.openconfig.net/>
- Purbo, O. W. (2026). *Onno W. Purbo, Data Center Handbook, 2026* [Dokumen outline buku tidak dipublikasikan].
- Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture* (NIST Special Publication 800-207). National Institute of Standards and Technology. <https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf>
- Sajassi, A., Aggarwal, R., Bitar, N., Isaac, A., Uttaro, J., Drake, J., & Henderickx, W. (2015). *BGP MPLS-based Ethernet VPN* (RFC 7432). Internet Engineering Task Force. <https://www.rfc-editor.org/rfc/rfc7432.html>
- Santana, G. A. A. (2014). *Data center virtualization fundamentals: Understanding techniques and designs for highly efficient data centers*. Cisco Press.
- Telecommunications Industry Association. (n.d.). *ANSI/TIA-942 standard: Telecommunications infrastructure standard for data centers*. Retrieved May 8, 2026, from <https://tiaonline.org/products-and-services/tia942certification/ansi-tia-942-standard/>
- Telecommunications Industry Association. (n.d.). *TIA-942 certification program*. Retrieved May 8, 2026, from <https://tiaonline.org/products-and-services/tia942certification/>
- The Green Grid. (2012). *PUE: A comprehensive examination of the metric*. https://datacenters.lbl.gov/sites/default/files/WP49-PUE%20A%20Comprehensive%20Examination%20of%20the%20Metric_v6.pdf
- The Green Grid. (2011). *Water usage effectiveness (WUE): A green grid data center sustainability metric*. https://www.thegreengrid.org/system/files/store/WUE_v1.pdf
- U.S. Department of Energy. (2024). *Best practices guide for energy-efficient data center design*. <https://www.energy.gov/sites/default/files/2024-07/best-practice-guide-data-center-design.pdf>
- Uptime Institute. (n.d.). *Tier classification system*. Retrieved May 8, 2026, from <https://uptimeinstitute.com/tiers>
- Uptime Institute. (n.d.). *Tier certification*. Retrieved May 8, 2026, from <https://uptimeinstitute.com/tier-certification>
- Uptime Institute. (n.d.). *Tier certification of operational sustainability*. Retrieved May 8, 2026, from <https://uptimeinstitute.com/tier-certification/operations>
- Zhang, L., & Chen, L. (2021). *Cloud data center network architectures and technologies*. CRC Press.

Tentang Penulis



Onno W. Purbo, saat ini bertugas sebagai rektor di Institut Teknologi Tangerang Selatan (ITTS). Onno memperoleh gelar Ph.D bidang Electrical Engineering dari University of Waterloo, Canada, adalah seorang copyleft, educator dan ICT evangelist. Dia sudah mempublikasikan 50++ buku, termasuk free ICT ebook untuk sekolah tahun 2008. Beberapa buku terakhirnya adalah "Internet-TCP/IP: Konsep Dan Implementasi", 2018; "Sistem Operasi, Konsep Dan Membuat Linux OpenWRT Dan ROM Android", 2019; "IPv6 Untuk Mendukung Operasi Jaringan Dan Domain Name System", 2019; "Kubernetes untuk Pemula", 2024 dan "Membuat Operator Seluler 5G Sendiri", 2024.

Dia memimpin sambungan pertama Internet di Institut Teknologi Bandung, tahun 1993-2000, dan menggunakannya untuk membuat jaringan Internet pendidikan yang pertama di Indonesia. Dia membebaskan frekuensi WiFi, memperkenalkan RT/RW-net, antenna Wajanbolic dan jaringan selular OpenBTS dan private 5G sendiri. Dia memimpin jaringan telepon pertama di atas Internet, VoIP Merdeka, yang kemudian hari dikenal sebagai VoIP Rakyat berbasis SIP dan menggunakan kode area +62520 dan +62521. Dia saat ini aktif memperkenalkan e-Learning, dan menjalankan server e-Learning di <http://lms.onnocenter.or.id/moodle/> 66,000++ siswa / mahasiswa dan <https://opencourse.itts.ac.id> 39.000+ mahasiswa secara gratis. Email: onno@indo.net.id