

LAPORAN AKHIR

# ANALISA KEBUTUHAN TIK KOTA MAGELANG



# DAFTAR ISI

<b>DAFTAR ISI</b> .....	<b>I</b>
<b>DAFTAR GAMBAR</b> .....	<b>III</b>
<b>DAFTAR TABEL</b> .....	<b>V</b>
<b>BAB I PENDAHULUAN</b> .....	<b>6</b>
1.1 LATAR BELAKANG .....	6
1.2 MAKSUD DAN TUJUAN.....	8
1.3 DASAR HUKUM.....	9
1.4 RUANG LINGKUP.....	10
<b>BAB II PENDEKATAN</b> .....	<b>11</b>
2.1 COBIT.....	11
2.2 SPBE.....	12
2.2.1 Visi SPBE.....	12
2.2.2 Misi SPBE.....	12
2.2.3 Kerangka Kerja SPBE.....	12
2.2.4 Layanan SPBE .....	13
2.2.5 Arsitektur SPBE.....	15
2.2.6 Arsitektur Aplikasi .....	16
2.2.7 Arsitektur Infrastruktur .....	16
2.2.8 Arsitektur Keamanan.....	17
2.3 SMART CITY .....	17
2.4 SATU DATA INDONESIA.....	18
2.5 PEMINDAHAN LOKASI KANTOR PEMERINTAH KOTA MAGELANG.....	20
<b>BAB III KONDISI AKTUAL</b> .....	<b>21</b>
3.1 ASPEK APLIKASI .....	21
3.1.1 Aplikasi Umum .....	22
3.1.2 Aplikasi Khusus.....	22
3.2 ASPEK INFRASTRUKTUR.....	24
3.2.1 Pusat Data .....	25
3.2.2 Jaringan.....	27
3.2.3 Sistem Penghubung Layanan.....	31
3.3 ASPEK KEAMANAN INFORMASI.....	31
3.4 ASPEK TATA KELOLA TIK.....	32

3.5	ASPEK SDM TIK .....	33
3.6	ASPEK DATA DAN INFORMASI .....	34
<b>BAB IV ANALISA KEBUTUHAN .....</b>		<b>36</b>
4.1	ANALISA RISIKO .....	36
4.2	ANALISA PEST .....	45
4.3	BALANCED SCORECARD .....	46
4.4	ANALISA GRID MCFARLAN .....	48
<b>BAB V KONDISI IDEAL .....</b>		<b>51</b>
5.1	ARSITEKTUR ENTERPISE .....	51
5.2	ARSITEKTUR APLIKASI .....	52
5.2.1	Diagram Sistem Penghubung Layanan .....	54
5.2.2	Diagram Single Sign On .....	55
5.2.3	Diagram Big data .....	55
5.2.4	Sumber Data .....	57
5.2.5	Data Ingestion .....	59
5.2.6	Big Data Storage .....	60
5.2.7	Data Analytic .....	63
5.2.8	Visual Presenting Data .....	66
5.3	ARSITEKTUR INFRASTRUKTUR .....	68
5.3.1	Diagram Jaringan .....	68
5.3.2	Diagram Pusat Data .....	81
5.3.3	Diagram Server dan Storage .....	97
5.4	ARSITEKTUR KEAMANAN .....	102
5.4.1	Arsitektur Keamanan Defensif .....	104
5.4.2	Arsitektur Keamanan Ofensif .....	116
5.5	ARSITEKTUR SDM .....	119
5.5.1	Job Role SDM Digital Transformation .....	119
<b>BAB VI KEBUTUHAN TIK .....</b>		<b>138</b>
6.1	DAFTAR KEBUTUHAN TIK ( 2022-2026 ) .....	138
<b>BAB VII PENUTUP .....</b>		<b>142</b>

## DAFTAR GAMBAR

Gambar 1 : Prinsip Pengembangan di Framework COBIT.....	11
Gambar 2 : Keterpaduan Unsur SPBE.....	13
Gambar 3 : Diagram Relasi dan Integrasi Komponen Arsitektur SPBE.....	15
Gambar 4 : Diagram Arsitektur Aplikasi .....	16
Gambar 5 : Diagram Arsitektur Infrastruktur .....	16
Gambar 6 : Diagram Arsitektur Keamanan.....	17
Gambar 7 : Smart City .....	18
Gambar 8 : Smart City Component .....	18
Gambar 9 : Kerangka Satu Data Indonesia .....	19
Gambar 10 : Kondisi Ruang Server Kota Magelang .....	26
Gambar 11 : Infrastruktur Server Kota Magelang .....	27
Gambar 12 : Analisa Pest Kota Magelang.....	46
Gambar 13 : Perspektif Balance Scorecard terhadap TI .....	46
Gambar 14 : Analisa Grid Mcfarlan Kota Magelang .....	49
Gambar 15 : Arsitektur Enterprise Pemerintahan Kota Magelang .....	51
Gambar 16 : Arsitektur Aplikasi.....	52
Gambar 17 : Diagram Sistem Penghubung Layanan.....	54
Gambar 18 : Contoh Penerapan Sistem Penghubung Layanan .....	54
Gambar 19 : Diagram Single Sign On.....	55
Gambar 20 : Diagram Infrastruktur Big Data .....	56
Gambar 21 : Source Data Big Data .....	58
Gambar 22 : Data Ingestion Big Data Apache Kafka .....	60
Gambar 23 : Data Storage Hadoop Menyimpan Data dari Kota Magelang .....	61
Gambar 24 : Integrasi Apache Kafka dan Apache.....	64
Gambar 25 : Kebutuhan Analisa Data Kota Magelang.....	64
Gambar 26 : Multi Platform Dashboard Analisa Data Kota Magelang.....	66
Gambar 27 : Arsitektur Visual Presenting Data .....	67
Gambar 28 : Keterkaitan Kebutuhan Arsitektur Aplikasi dengan Arsitektur Infrastruktur .....	69
Gambar 29 : Network Enterprise Architecture.....	69
Gambar 30 : Network Enterprise Architecture.....	70
Gambar 31 : Jaringan Utama Diskominfo Kota Magelang.....	71
Gambar 32 : Access Layer .....	72
Gambar 33 : Double ISP Kota Magelang.....	74
Gambar 34 : Redundancy MPLS/FO/VPN dan Internet .....	75
Gambar 35 : Replikasi layanan di DRC.....	76
Gambar 36 : Arsitektur Intranet Jaringan Kota Magelang .....	77
Gambar 37 : Perbandingan Penggunaan Bandwidth Sebelum dan Sesudah Dilakukan QOS.....	78

Gambar 38 : Klasifikasi Trafik yang melalui jaringan .....	79
Gambar 39 : Klasifikasi Paket berdasarkan kode Marking L2 dan L3 .....	79
Gambar 40 : Bandwidth Policy Berdasarkan Klasifikasi Tipe Trafik Data .....	80
Gambar 41 : Lantai Ruang Server Menggunakan Raised Floor .....	81
Gambar 42 : Deretan Server Dengan Menggunakan Raised Floor .....	82
Gambar 43 : Ruang Untuk Administrator Data Center .....	82
Gambar 44 : Perencanaan Sistem Listrik Data Center .....	84
Gambar 45 : Distribusi Kebutuhan Listrik dari PDU melalui circuit panel .....	85
Gambar 46 : Aliran Distribusi Udara.....	86
Gambar 47 : Koridor Panas .....	87
Gambar 48 : Instalasi Fire Suppression Untuk Data Center.....	89
Gambar 49 : Solusi Fire Fighting System .....	89
Gambar 50 : Fungsi Command and Center.....	91
Gambar 51 : Display Command Center .....	92
Gambar 52 : Control Room Data Center .....	93
Gambar 53 : Contoh Hasil Monitoring Jaringan .....	94
Gambar 54 : Contoh Monitoring Server dan Aplikasi .....	94
Gambar 55 : Hyper Converged Infrastructure (HCI) Server Concept.....	97
Gambar 56 : Arsitektur Cluster HA pada Hyperconverged .....	98
Gambar 57 : Arsitektur Storage dan Server.....	99
Gambar 58 : Layanan Cloud Pusat Data Nasional dan Diskominfo .....	100
Gambar 59 : Replikasi layanan di DRC.....	101
Gambar 60 : Arsitektur Keamanan .....	102
Gambar 61 : Arsitektur Keamanan .....	105
Gambar 62 : Tingkat sensitivitas dan tingkat kritikalitas data .....	106
Gambar 63 : <i>Data Classification</i> .....	107
Gambar 64 : <i>Application control</i> .....	107
Gambar 65 : <i>Security Control</i> .....	109
Gambar 66 : Kendali Perimeter .....	111
Gambar 67 : <i>Physical Security</i> .....	112
Gambar 68 : <i>Policies, Procedures and Awareness</i> .....	113
Gambar 69 : ISO 27001 .....	116
Gambar 70 : <i>Vulnerability Assessment &amp; Penetration Test (VAPT)</i> .....	117
Gambar 71 : <i>Incident Response &amp; Handling</i> .....	118
Gambar 72 : <i>Computer Hacking Forensic Readiness</i> .....	118
Gambar 73 : Job Role SDM Digital Transformation .....	119

## DAFTAR TABEL

Tabel 1 : Dampak Fungsi Teknologi Informasi Terhadap Organisasi.....	7
Tabel 2 : Kode Layanan SPBE.....	13
Tabel 3 : Kebutuhan Pemindahan Fasilitas dan Teknologi.....	20
Tabel 4 : Aplikasi Umum Daerah Pemerintahan Kota Magelang .....	22
Tabel 5 : Aplikasi Khusus Daerah Pemerintahan Kota Magelang.....	23
Tabel 6 : Kondisi dan Spesifikasi Fasilitas Data Center.....	25
Tabel 7 : Spesifikasi Jaringan Kota Magelang .....	28
Tabel 8 : Daftar Fasilitas yang sudah terhubung Jaringan .....	28
Tabel 9. Tata Kelola TIK di Kota Magelang.....	32
Tabel 10 : Daftar Risiko TIK Kota Magelang .....	36
Tabel 11 : Daftar Risiko dan Kontrol .....	40
Tabel 12 : Analisa Balanced Scorecard .....	47
Tabel 13 : Tabel Job Role Transformasi Digital .....	119
Tabel 14 : Daftar Kebutuhan TIK dan Timeline .....	138

# BAB I

## PENDAHULUAN

### 1.1 Latar Belakang

Perkembangan teknologi informasi telah mengubah konsep dan paradigma tentang organisasi, dan organisasi tersebut salah satunya adalah pemerintah daerah. Sejatinya organisasi adalah kumpulan individu atau sekelompok orang yang ingin mencapai suatu tujuan tertentu (misalnya visi dan misi yang telah dicanangkan dalam RPJMD). Secara komponen, organisasi dapat dibentuk oleh dua buah entitas, yaitu manusia dan struktur. Unsur manusia akan sangat dipengaruhi oleh nilai, budaya/kultur, kepercayaan, perilaku sosial, struktur masyarakat, lingkungan sekitar, dan lain sebagainya, sementara unsur struktur akan sangat terkait dengan sistem, teknologi, prosedur, ukuran dan bentuk, dan lain sebagainya.

Dalam beberapa kebijakan yang dikeluarkan oleh pemerintah pusat (E-Government, SPBE, Smart City, Satu Data Indonesia, Satu Peta Indonesia), telah nampak adanya keinginan untuk mengubah pemerintahan menjadi organisasi yang modern. Dimana organisasi modern berusaha menggabungkan kemampuan teknis untuk menghasilkan suatu layanan atau produk dan sumber daya manusia sebagai pelaku atau subjek dalam berorganisasi.

Perubahan paradigma tersebut telah mengakibatkan terjadinya revolusi pemikiran dalam perancangan sistem organisasi yang tepat dan efektif di era modern seperti saat ini dimana sejumlah prinsip lama yang telah sedemikian kuat dipegang, harus dilepas dan digantikan dengan beragam paradigma baru serta mindset baru.

Dalam konteks makro maka pemerintah membentuk sebuah struktur organisasi berdasarkan sejumlah aspek terkait dengan hal-hal sebagai berikut, pembagian OPD berdasarkan spesialisasi, pemberlakuan standarisasi, bentuk formaliasi komunikasi dan prosedur, struktur sentralisasi atau desentralisasi, dan lain sebagainya. Dibentuknya struktur tersebut adalah untuk memudahkan tercapainya visi, misi, dan obyektif yang telah dicanangkan, dimana keseluruhannya akan diukur melalui sejumlah indikator

kinerja (IKU), seperti produktivitas, kemampuan beradaptasi dan tata Kelola pemerintahan. Perlu diperhatikan bahwa struktur organisasi memiliki keterkaitan timbal balik yang sangat erat dengan perilaku organisasi karena di dalamnya akan mengandung baik secara implisit maupun eksplisit hal-hal semacam struktur pengaruh dan kekuasaan, pola interaksi dan pelaporan, batasan pekerjaan dan tanggung jawab. Hal tersebut di atas adalah pendekatan penjelasan dari UU no 23 tahun 2014 tentang Pemerintah Daerah, yang tentu saja akan menjadi bagian dari latar belakang Analisis kebutuhan TIK ini.

Mengenai ke arah mana sebuah organisasi akan memiliki kecenderungan dalam proses perancangan sistem organisasinya. Pendekatan “Kemampuan Teknis” (Pepres 95 tahun 2018 tentang SPBE) dan “struktur organisasi” (UU No 23 tahun 2014 tentang Pemerintah Daerah), dapat menyebutkan peran/ fungsi teknologi informasi dalam organisasi Pemerintah Daerah, yaitu :

1. Fungsi Operasional
2. Fungsi Pengawasan dan Kontrol
3. Fungsi Perencanaan dan Pengambil Keputusan
4. Fungsi Komunikasi
5. Fungsi Interorganisasi

Dimana dari fungsi teknologi informasi tersebut akan memberikan dampak kepada organisasi pemerintah daerah, yang dapat digambarkan dalam tabel berikut ini :

Tabel 1 : Dampak Fungsi Teknologi Informasi Terhadap Organisasi

No	Fungsi Teknologi Informasi	Dampak Organisasi
1	Fungsi Operasional	Membuat struktur organisasi menjadi lebih ramping dan jauh dari sifat birokratis karena sejumlah aspek administratif yang ketat dan teratur telah diambil alih fungsinya oleh teknologi informasi.
2	Fungsi Pengawasan dan Kontrol	Keberadaan teknologi informasi akan menjadi bagian yang tidak terpisahkan dengan aktivitas di level

		manajerial yang melekat di dalam setiap pejabat struktural
3	Fungsi Perencanaan dan Pengambil Keputusan	Teknologi informasi ke tataran peran yang lebih strategis lagi karena keberadaannya sebagai enabler dari Rencana Pembangunan (RPJMD) dan merupakan sebuah “knowledge generator” bagi para pimpinan yang dihadapkan pada realitas untuk mengambil sejumlah keputusan penting sehari-harinya.
4	Fungsi Komunikasi	Teknologi informasi ditempatkan posisinya sebagai sarana atau media individu perusahaan dalam berkomunikasi, berkolaborasi dan berinteraksi
5	Fungsi Interorganisasi	Teknologi Informasi digunakan sebagai media untuk berkolaborasi dengan instansi lain dalam suatu ekosistem tertentu , baik kontek berbagi pakai atau rangkaian proses ( supply chain )

Dengan memahami karakteristik dari organisasi Pemerintah Daerah terutama ditinjau dari sejumlah variabel yang mempengaruhinya (budaya organisasi yang telah terbentuk, perilaku para pimpinan dan pengambil keputusan terutama dalam hal digital leadership (sikap kepemimpinan), visi dan misi , tuntutan masyarakat, perkembangan teknologi informasi yang pesat ) dapat dikembangkan sebuah perencanaan kebutuhan teknologi informasi yang tepat dan efektif

## 1.2 Maksud dan Tujuan

Maksud dari penyusunan Dokumen Analisa Kebutuhan TIK Kota Magelang ini adalah agar dokumen ini dijadikan sebagai landasan berpikir, standarisasi, pentahapan, dan implementasi kebutuhan TIK bagi pengembangan SPBE, Smart City, Satu Data Indonesia Pemerintah Kota Magelang yang komprehensif, efisien, efektif, dan terpadu, untuk mencapai visi dan misi pembangunan kota magelang yang termaktub dalam RPJMD 2021-2026.

Adapun tujuan dari Analisa Kebutuhan TIK 2022 -2026 ini adalah :

1. Analisa Kelayakan perencanaan kebutuhan aplikasi
2. Analisa Kelayakan perencanaan kebutuhan infrastruktur TIK
3. Analisa Kelayakan perencanaan kebutuhan Keamanan Informasi
4. Analisa Kelayakan perencanaan kebutuhan SDM
5. Analisa Kelayakan perencanaan kebutuhan Tata Kelola TIK
6. Analisa Kelayakan perencanaan kebutuhan Data dan Informasi

### 1.3 Dasar Hukum

Dasar hukum pembuatan Analisa Kebutuhan TIK Kota Magelang 2022 -2026 yaitu:

1. Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;
2. Undang-Undang Nomor 25 Tahun 2004 tentang Sistem Perencanaan Pembangunan Nasional;
3. Undang-Undang Nomor 17 Tahun 2007 tentang Rencana Pembangunan Jangka Panjang Nasional Tahun 2005 - 2025;
4. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik;
5. Undang-Undang Nomor 39 Tahun 2008 tentang Kementerian Negara;
6. Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik;
7. Undang- Undang Nomor 5 Tahun 2014 tentang Aparatur Sipil Negara;
8. Undang- Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah
9. Undang- Undang Nomor 9 Tahun 2015 tentang Perubahan Kedua atas Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah;
10. Undang- Undang Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan;
11. Undang - Undang Nomor 11 Tahun 2008 juncto Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik;
12. Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik;
13. Peraturan Pemerintah Nomor 18 Tahun 2016 tentang Perangkat Daerah;
14. Peraturan Presiden Nomor 81 Tahun 2010 tentang Grand Design Reformasi Birokrasi 2010 - 2025;
15. Peraturan Presiden Nomor 96 Tahun 2014 tentang Rencana Pita Lebar Indonesia;

16. Instruksi Presiden Nomor 3 Tahun 2003 tentang Kebijakan dan Strategi Nasional Pengembangan E-Government.
17. Peraturan Presiden no. 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE)
18. Peraturan Presiden no. 39 tahun 2019 tentang Satu Data Indonesia (SDI)

## 1.4 Ruang Lingkup

Dalam penyusunan Analisa Kebutuhan TIK Kota Magelang 2022 -2026 ini, memiliki ruang lingkup sebagai berikut :

1. Ruang Lingkup Komponen TIK
  - a. Aplikasi , melingkupi Aplikasi Umum dan Khusus sesuai tertera dalam Perpres SPBE
  - b. Infrastruktur TIK melingkupi Pusat Data, Jaringan dan Sistem Penghubung Layanan
  - c. Keamanan Informasi , melingkupi Standar ISO 27001
  - d. SDM (SDM Teknis SPBE )
  - e. Tata Kelola TIK ( Kebijakan , Pelaksana )
  - f. Data dan Informasi
2. Ruang Lingkup Analisa
  - a. Analisa *Ward & Peppard* (Kondisi Organisasi dan Kondisi Teknologi Informasi )
  - b. Analisa *Balanced Scorecard*
  - c. Analisa *SWOT*
  - d. Analisa Risiko
  - e. Analisa *Grid McFarlan*
  - f. Analisa *PEST*

## BAB II

### PENDEKATAN

#### 2.1 COBIT

Control Objective for Information and related Technology (COBIT), adalah suatu panduan standar praktik manajemen teknologi informasi. Standar COBIT dikeluarkan oleh IT Governance Institute yang merupakan bagian dari ISACA. COBIT juga merupakan rangkaian dari best practices ( kerangka kerja ) yang digunakan manajemen TIK. Berbagai indikator, proses-proses dan praktik terbaik dalam COBIT dapat membantu dalam memaksimalkan keuntungan yang berasal dari penggunaan TIK dan mengembangkan tata kelola TIK yang cocok dan kendali di dalam organisasi.

Pengembangan framework COBIT sebenarnya berdasarkan 3 prinsip dasar, yaitu: Sumber Daya TIK, Proses TIK dan *Business Requirement*. Ke-tiga prinsip dasar muncul dari adanya kebutuhan terhadap ukuran kinerja dari teknologi informasi terhadap organisasi.



Gambar 1 : Prinsip Pengembangan di Framework COBIT

Pemaknaan yang sederhana tentang kebutuhan TIK dalam sudut pandang COBIT adalah, adanya sumber daya dan proses.

## 2.2 SPBE

### 2.2.1 Visi SPBE

Visi SPBE menjadi acuan dalam mewujudkan pelaksanaan SPBE yang terpadu di Instansi Pemerintah Kota Magelang untuk menghasilkan birokrasi pemerintah yang integratif, dinamis, transparan, dan inovatif, serta peningkatan kualitas pelayanan publik yang terpadu, efektif, responsif, dan adaptif.

Visi SPBE Kota Magelang selaras dengan Visi SPBE Nasional yang tertuang dalam Peraturan Presiden Nomor 95 Tahun 2018, yaitu:

**“Terwujudnya sistem pemerintahan berbasis elektronik yang terpadu dan menyeluruh untuk mencapai birokrasi dan pelayanan publik yang berkinerja tinggi.”**

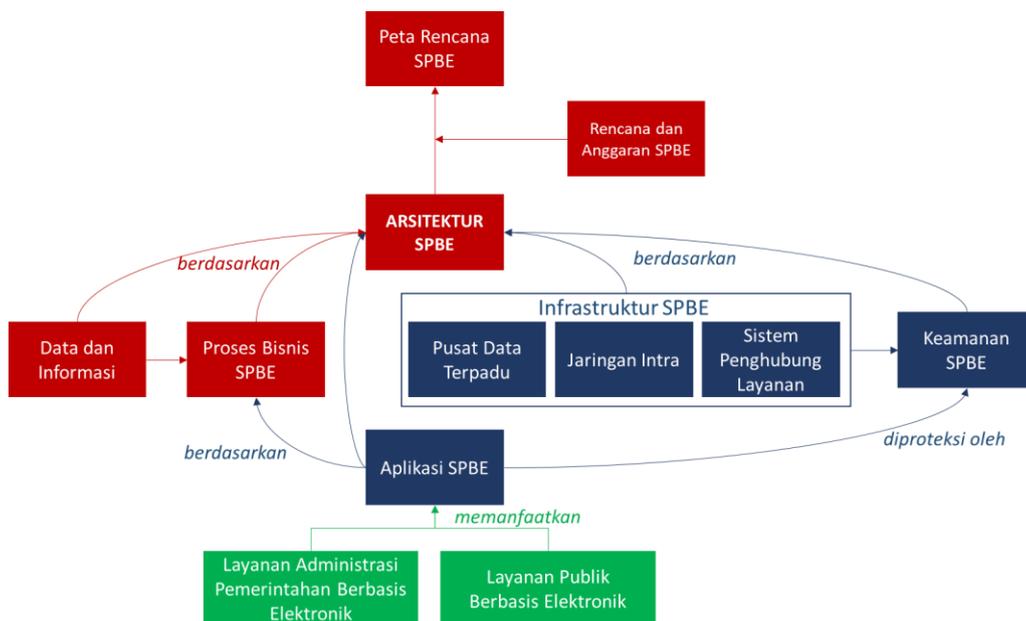
### 2.2.2 Misi SPBE

Misi SPBE merupakan upaya umum tentang bagaimana cara mewujudkan Visi SPBE. Misi SPBE Kota Magelang dirumuskan sebagai berikut:

1. Melakukan penataan dan penguatan organisasi dan tata kelola sistem pemerintahan berbasis elektronik yang terpadu
2. Mengembangkan pelayanan publik berbasis elektronik yang terpadu, menyeluruh, dan menjangkau masyarakat luas
3. Membangun fondasi teknologi informasi dan komunikasi yang terintegrasi, aman, dan andal
4. Membangun SDM yang kompeten dan inovatif berbasis teknologi informasi dan komunikasi.

### 2.2.3 Kerangka Kerja SPBE

Dimulai dengan melakukan digitalisasi layanan yang diselenggarakan oleh Pemerintah Kota Magelang dengan memanfaatkan aplikasi. Dimana aplikasi tersebut harus berbasis pada proses bisnis dan data yang terdefinisi sesuai RPJMD yang ada



Gambar 2 : Keterpaduan Unsur SPBE

Kemudian bagaimana aplikasi tersebut membutuhkan infrastruktur dan keamanan SPBE untuk menjamin keberlangsungan dan kualitas layanan berbasis elektronik.

#### 2.2.4 Layanan SPBE

Layanan SPBE merupakan awal terbentuknya kebutuhan aplikasi. Layanan SPBE terdiri dari layanan administrasi pemerintahan SPBE dan layanan publik. Dalam kebijakan terkini, yang menjadi fokus dari pemerintah daerah untuk melakukan digitalisasi adalah pada layanan publik. Layanan publik tentu harus diselaraskan dengan RPJMD Kota Magelang, yang berisi, misi, sasaran dan program kerja.

Adapun daftar layanan tersebut adalah :

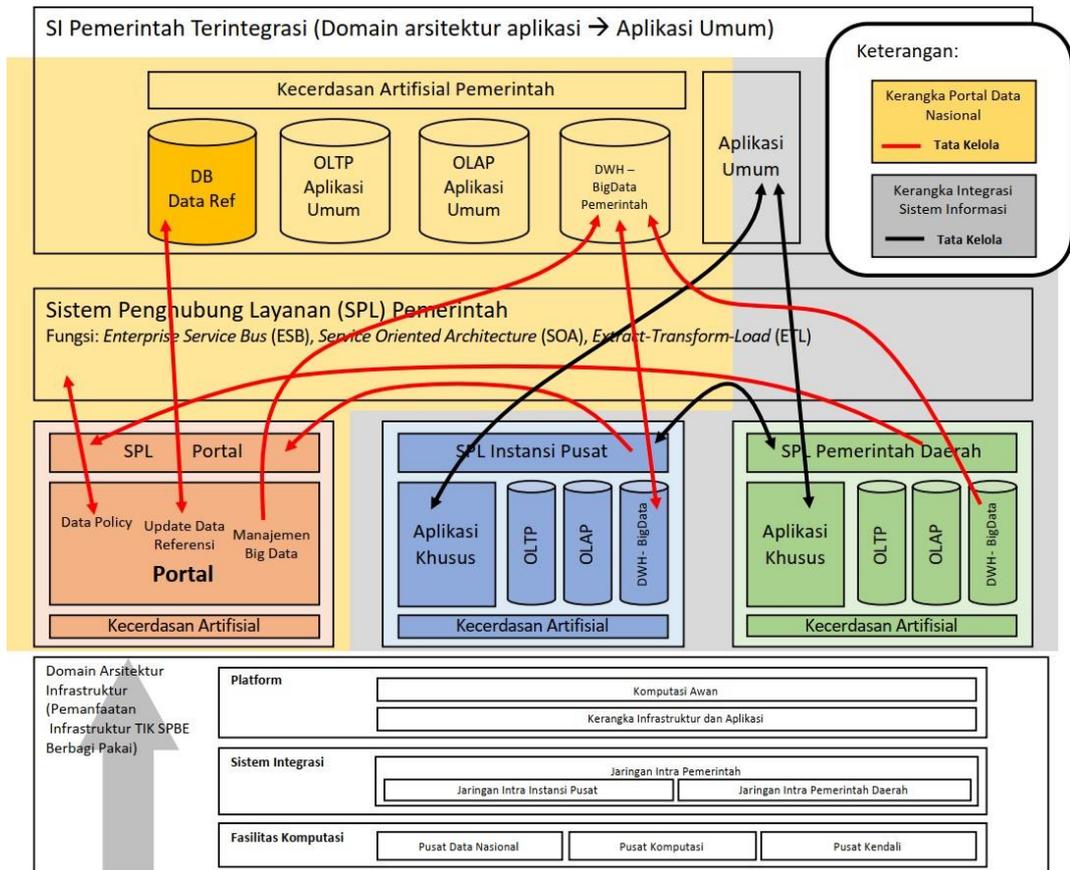
Tabel 2 : Kode Layanan SPBE

Kode Layanan	Nama Layanan
RAL.01.04	Layanan Ekonomi
RAL.01.05	Layanan Industri
RAL.01.06	Layanan Perdagangan
RAL.01.07	Layanan Pertanian
RAL.01.10	Layanan Perikanan
RAL.01.11	Layanan BUMN

<b>RAL.01.12</b>	Layanan Investasi
<b>RAL.01.13</b>	Layanan Koperasi
<b>RAL.01.14</b>	Layanan Usaha Kecil dan Menengah
<b>RAL.01.15</b>	Layanan Pariwisata
<b>RAL.01.16</b>	Layanan Perizinan dan Akreditasi
<b>RAL.01.17</b>	Layanan Pekerjaan Umum
<b>RAL.01.19</b>	Layanan Transportasi
<b>RAL.01.20</b>	Layanan Perumahan
<b>RAL.01.22</b>	Layanan Pertanahan
<b>RAL.01.23</b>	Layanan Kependudukan
<b>RAL.01.25</b>	Layanan Kesehatan
<b>RAL.01.26</b>	Layanan Sosial
<b>RAL.01.27</b>	Layanan Pemberdayaan Perempuan
<b>RAL.01.28</b>	Layanan Hukum
<b>RAL.01.29</b>	Layanan Keamanan
<b>RAL.01.30</b>	Layanan Hak Asasi Manusia
<b>RAL.01.31</b>	Layanan Pendidikan
<b>RAL.01.32</b>	Layanan Ketenagakerjaan
<b>RAL.01.33</b>	Layanan Ilmu Pengetahuan
<b>RAL.01.34</b>	Layanan Teknologi
<b>RAL.01.35</b>	Layanan Pemuda
<b>RAL.01.36</b>	Layanan Olahraga
<b>RAL.01.37</b>	Layanan Pertambangan
<b>RAL.01.41</b>	Layanan Lingkungan Hidup
<b>RAL.01.42</b>	Layanan Agama
<b>RAL.01.43</b>	Layanan Kebudayaan
<b>RAL.01.44</b>	Layanan Informasi
<b>RAL.01.45</b>	Layanan Komunikasi

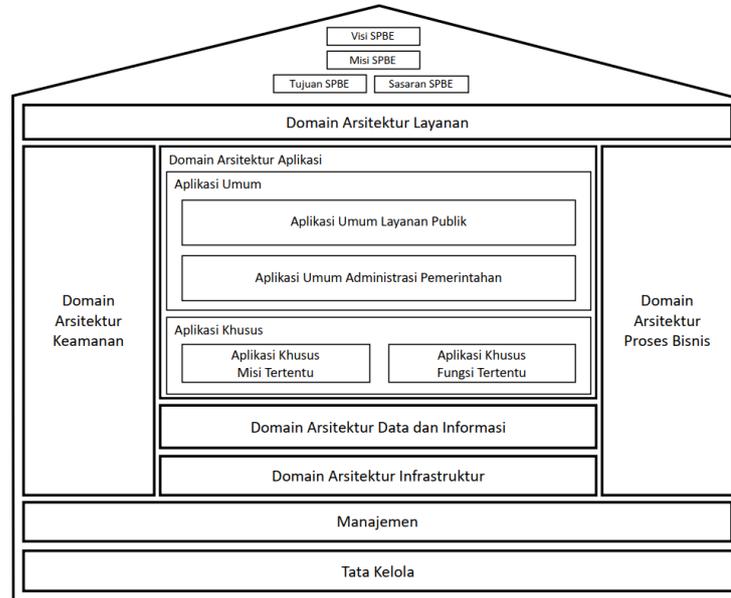
### 2.2.5 Arsitektur SPBE

Arsitektur SPBE adalah kerangka dasar yang mendeskripsikan integrasi proses bisnis, data dan informasi, infrastruktur SPBE, aplikasi SPBE, dan keamanan SPBE untuk menghasilkan layanan SPBE yang terintegrasi. Secara diagram dapat digambarkan sebagai berikut :



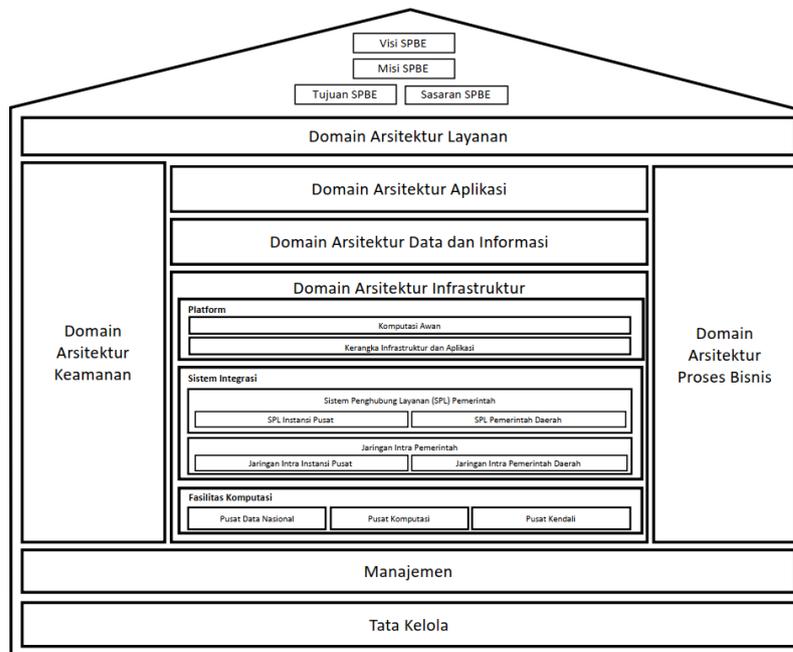
Gambar 3 : Diagram Relasi dan Integrasi Komponen Arsitektur SPBE

### 2.2.6 Arsitektur Aplikasi



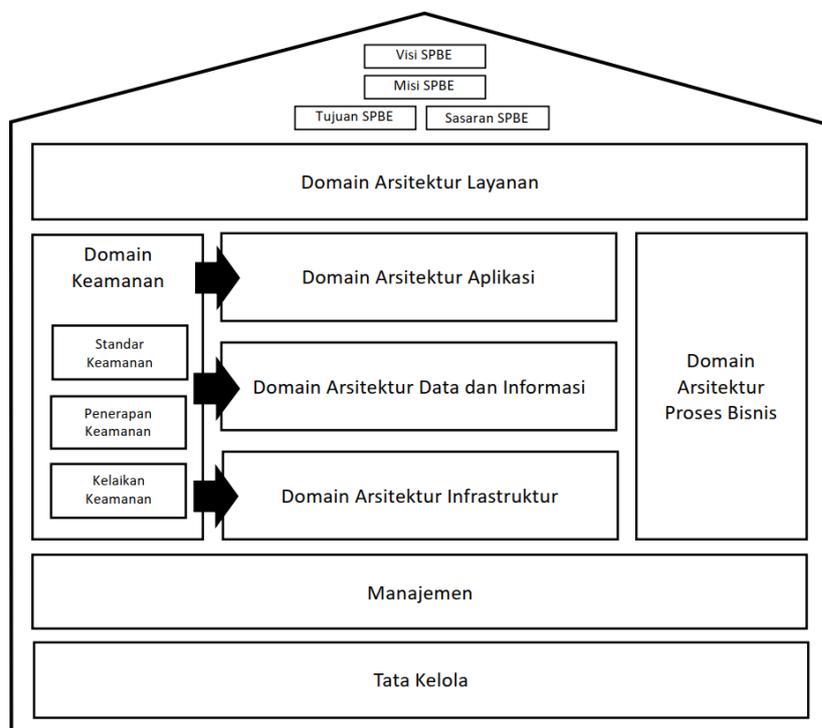
Gambar 4 : Diagram Arsitektur Aplikasi

### 2.2.7 Arsitektur Infrastruktur



Gambar 5 : Diagram Arsitektur Infrastruktur

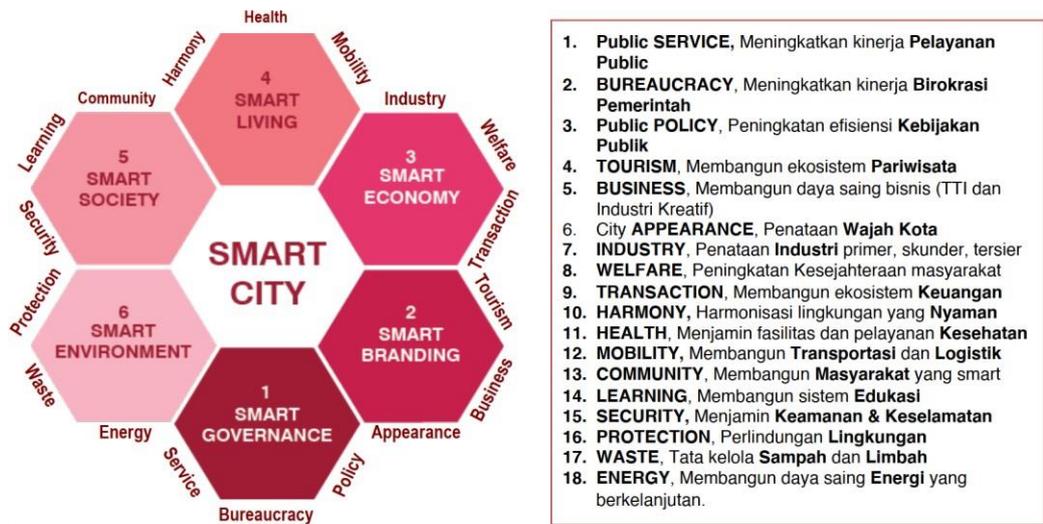
## 2.2.8 Arsitektur Keamanan



Gambar 6 : Diagram Arsitektur Keamanan

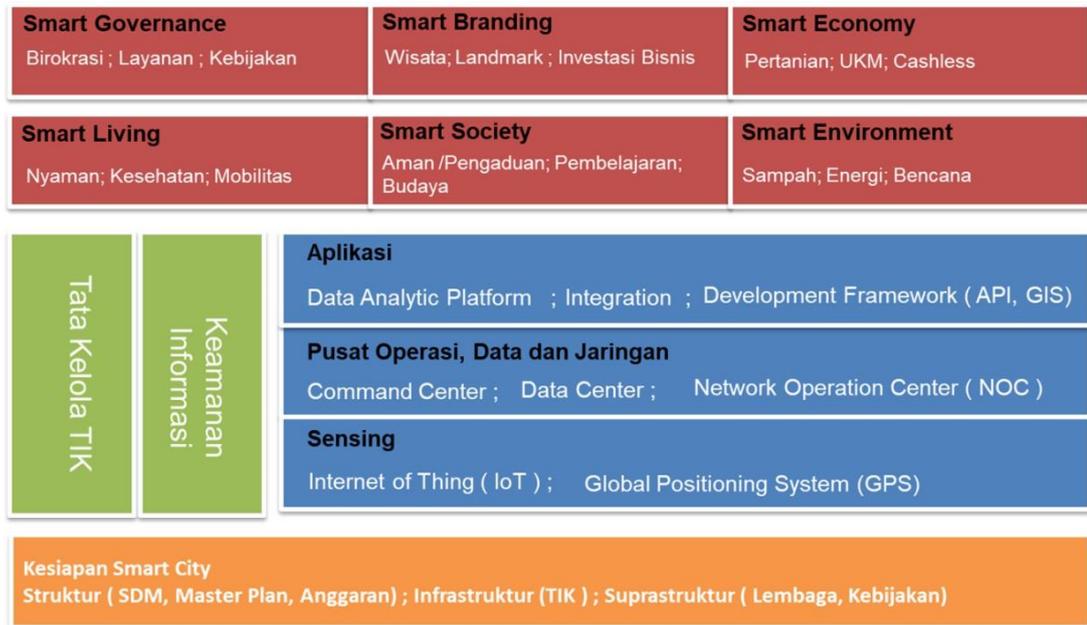
## 2.3 Smart City

Smart City memanfaatkan teknologi sebagai enabler untuk menjadikan kota/daerah yang layak huni, nyaman, mudah, sehat, aman, dan berkelanjutan. Dimana elemen pembangunan smart city yang ditetapkan di Indonesia saat ini adalah :



Gambar 7 : Smart City

Dimana dalam kerangka kebutuhan TIK untuk mendukung Smart City Kota Magelang, dapat digambarkan sebagai berikut:



Gambar 8 : Smart City Component

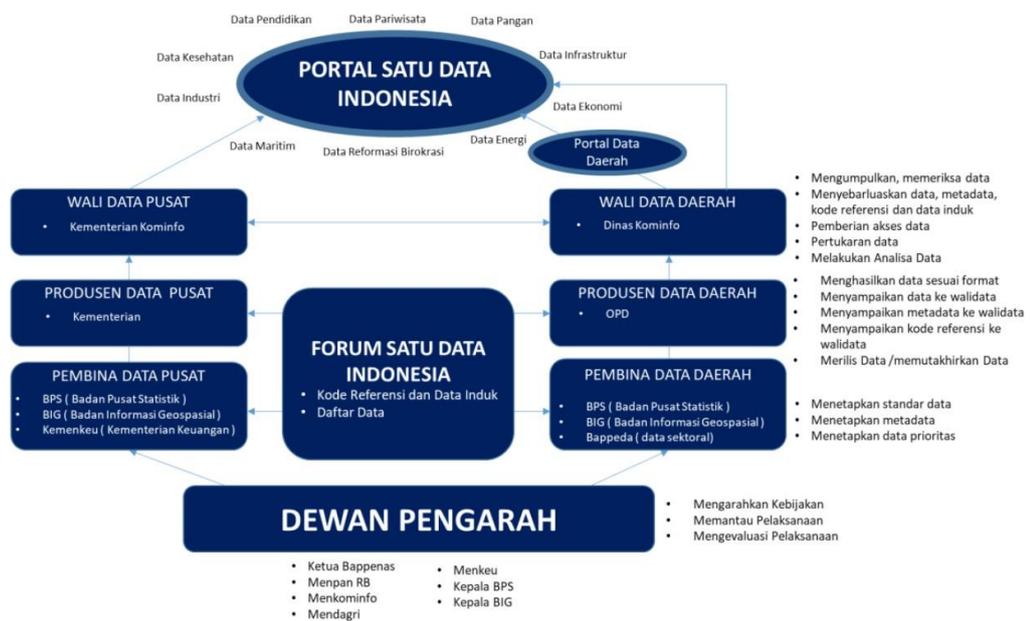
## 2.4 Satu Data Indonesia

Satu Data Indonesia adalah kebijakan tata kelola data pemerintah untuk menghasilkan data yang akurat, mutakhir, terpadu, dan dapat dipertanggungjawabkan, serta mudah diakses dan dibagipakai antara instansi pusat dan instansi daerah. Data yang dihasilkan oleh produsen data harus berdasarkan prinsip berikut:

- Memenuhi standar data;
- Memiliki metadata;
- Memenuhi kaidah interoperabilitas data; dan
- Menggunakan kode referensi dan/atau data induk.

Standar data selain data statistik dan data geospasial ditetapkan oleh Pembina Data lainnya di tingkat pusat. Perpres ini juga membentuk Dewan Pengarah dan Forum Satu Data Indonesia. Forum tersebut menjadi wadah komunikasi dan koordinasi instansi pusat dan/atau instansi daerah dalam penyelenggaraan Satu Data Indonesia.

Kerangka Satu Data Indonesia di Kota Magelang dapat digambarkan sebagai berikut :



Gambar 9 : Kerangka Satu Data Indonesia

Kebutuhan akan data dan tempat publish data dalam portal data, merupakan tugas dari dinas kominfo di pemerintah daerah

## 2.5 Pemindahan Lokasi Kantor Pemerintah Kota Magelang

Terdapatnya rencana pemindahan kantor pemerintah kota magelang, tentu menjadi sebuah sudut pandang yang akan mempengaruhi dalam Analisa kebutuhan TIK kedepannya.

Sebuah bangunan yang baru, apapun bentuknya, namun dengan melihat organisasi pemda dengan Struktur Organisasi dan Kemampuan Teknis dalam memberikan layanan kepada masyarakat dengan segala latar belakang kebijakan, maka dapat diperkirakan kelompok kebutuhan sebagai berikut :

Tabel 3 : Kebutuhan Pemindahan Fasilitas dan Teknologi

No	Kategori	Jenis
1	Fasilitas	Bangunan : Data Center / Pusat Data -SOC/NOC ( Tier 3 )
		Bangunan : Command Center
2	Teknologi	Infrastruktur Jaringan FO yang menghubungkan seluruh OPD

## BAB III

### KONDISI AKTUAL

#### 3.1 Aspek Aplikasi

Pemerintahan Kota Magelang mempunyai beberapa aplikasi yang mendukung layanan yang dirancang untuk melaksanakan tugas atau fungsi Layanan TIK Daerah. Baik Layanan tersebut diperuntukan untuk Pemerintahan Pusat/Daerah, maupun diberikan sebagai bentuk layanan kepada masyarakat.

Sebagai gambaran Aplikasi Umum merupakan Aplikasi yang mempunyai persamaan, standar, dan digunakan secara bagi pakai oleh instansi pusat dan/atau pemerintah daerah. Sedangkan Aplikasi Khusus adalah Aplikasi yang dibangun, dikembangkan, digunakan, dan dikelola oleh instansi pusat atau pemerintah daerah tertentu untuk memenuhi kebutuhan khusus yang bukan kebutuhan instansi pusat dan pemerintah daerah lain.

Berikut adalah beberapa gambaran kondisi:

1. Pengembangan Aplikasi tidak terkelompokkan terpadu berbasis layanan sesuai dengan Rekomendasi Sistem Pemerintahan Berbasis Elektronik (SPBE)/ Rencana Pembangunan Jangka Menengah Daerah (RPJMD).
2. Penggunaan dan pengembangan aplikasi Umum dan khusus di daerah yang tidak sejalan dengan program pemerintah pusat beresiko membuat inefisiensi sumber Daya IT (Cost) yang membebani Pemerintahan Kota Magelang. Masih ditemukan beberapa Aplikasi Umum daerah
3. Tidak adanya SSO (Single Sign On) sehingga terlalu banyak aplikasi yang dimiliki Pemerintahan Kota Magelang dan pengguna dipaksa untuk menghafalkan akses ke semua aplikasi. Ada Risiko pada monitoring dan kontrol akses penggunaan aplikasi di lingkungan Pemerintahan Kota Magelang

### 3.1.1 Aplikasi Umum

Pemerintahan Kota Magelang menggunakan Aplikasi Umum yang digunakan Semua OPD untuk mendukung layanan Administrasi Pemerintahan Kota Magelang. Masih banyak penggunaan Aplikasi Umum daerah yang belum terintegrasi dengan Pusat, dan berikut adalah daftar aplikasi tersebut berdasarkan tipe layanan.

Tabel 4 : Aplikasi Umum Daerah Pemerintahan Kota Magelang

Kode Layanan	Nama Layanan	Nama Aplikasi	Web / Dekstop
RAL.02.02	Layanan Keuangan	e-Budgeting, SIPD, SIMDA	Web , Dekstop
RAL.02.03	Layanan Perencanaan Pembangunan	SIPD, SIMBANGDA, Smart Magelang	Web
RAL.02.04	Layanan Aparatur Negara	LAKONE, SIMPEG, eKinerja, SKP	Mobile App, Web
RAL.02.05	Layanan Kesekretariatan	TNDE, SIARDINA, Agenda Walikota dan Wakil Walikota	Web
RAL.02.06	Layanan Dukungan Operasional Organisasi	Belum Ada	
RAL.02.07	Layanan Akuntabilitas Kinerja	rtcs SAKIP, SIPD, Smart SAKIP	Web
RAL.02.08	Layanan Organisasi dan Tata Kelola	SRIKANDI	
RAL.02.09	Layanan Data dan Informasi pemerintah	SIKN, PPID, SIABAH, JDIH	Web

### 3.1.2 Aplikasi Khusus

Pemerintahan Kota Magelang menggunakan Aplikasi Khusus yang digunakan Semua OPD/Publik untuk mendukung layanan Administrasi Pemerintahan Kota Magelang. Banyak aplikasi yang belum tersedia dengan kebutuhan layanan yang ada di pemerintahan Kota Magelang.

Tabel 5 : Aplikasi Khusus Daerah Pemerintahan Kota Magelang

Kode Layanan	Nama Layanan	Nama Aplikasi	Web / Dekstop
RAL.01.04	Layanan Ekonomi	IndieGo, SeHati, MAGESTY	Web
RAL.01.05	Layanan Industri	Belum Ada	
RAL.01.06	Layanan Perdagangan	Marketplace Magelang Cerdas, Marketplace Magesty	
RAL.01.07	Layanan Pertanian	Belum Ada	
RAL.01.08	Layanan Perkebunan	Belum Ada	
RAL.01.09	Layanan Peternakan	Belum Ada	
RAL.01.10	Layanan Perikanan	Belum Ada	
RAL.01.12	Layanan Investasi	OSS	
RAL.01.13	Layanan Koperasi	Belum Ada	
RAL.01.14	Layanan Usaha Kecil dan Menengah	Pendaftaran UMKM Magesty, Markeplace Kerjasama dengan Tokopedia	Web/ Mobile
RAL.01.15	Layanan Pariwisata	Registrasi Objek Wisata, Virtual Tour TKL	Web
RAL.01.16	Layanan Perizinan dan Akreditasi	OSS, SiCantik	Web
RAL.01.17	Layanan Pekerjaan Umum	SIG Tata Ruang	Web
RAL.01.18	Layanan Transmigrasi	Belum Ada	
RAL.01.19	Layanan Transportasi	Cek Kir Online	Web
RAL.01.20	Layanan Perumahan	Senja Magelang (Sedot Tinja)	Mobile App
RAL.01.22	Layanan Pertanahan	Belum Ada	Bukan Kewenangan Pemerintah Daerah
RAL.01.23	Layanan Kependudukan	Layanan Disdukcapil (SIAK)	Web
RAL.01.24	Layanan Pemerintah Daerah	SIMBANGDA, LAKONE, SIMRESSO, E-Kinerja	Web
RAL.01.25	Layanan Kesehatan	Portal Covid Kota Magelang	Web
RAL.01.26	Layanan Sosial	Cek Bansos, Santunan Kematian, Magesty	Web
RAL.01.27	Layanan Pemberdayaan Perempuan	Belum Ada	
RAL.01.28	Layanan Hukum	JDIH	Web

RAL.01.29	Layanan Keamanan	SIG Satpol PP	Web
RAL.01.31	Layanan Pendidikan	PPDB, Inobel	Web
RAL.01.32	Layanan Ketenagakerjaan	Jobfair Online, Penta (Layanan Pencari Kerja	Web
RAL.01.33	Layanan Ilmu Pengetahuan	SIKN, iMagelang (e-Library), Magelang Cerdas	Web, Mobile App
RAL.01.34	Layanan Teknologi	Tower In Your Hand	Web
RAL.01.35	Layanan Pemuda	Belum Ada	
RAL.01.36	Layanan Olahraga	Belum Ada	
RAL.01.37	Layanan Pertambangan	Belum Ada	
RAL.01.38	Layanan Energi	Belum Ada	
RAL.01.39	Layanan Kehutanan	Belum Ada	
RAL.01.41	Layanan Lingkungan Hidup	Sistem Informasi Pemakaman Online	Web
RAL.01.42	Layanan Agama	Aplikasi Santan (Santunan Kematian), Magesty	Web
RAL.01.43	Layanan Kebudayaan		Web
RAL.01.44	Layanan Informasi	DataGo, Open Data, Portal Kota Magelang, Magelang Cerdas	Web
RAL.01.45	Layanan Komunikasi	PPID, Monggo Lapor, Magelang Cerdas	Web

### 3.2 Aspek Infrastruktur

Pemerintahan Kota Magelang mempunyai infrastruktur yang cukup memadai dengan kebutuhan yang ada sekarang, akan tetapi tidak ideal karena ada peningkatan kebutuhan dan ekspektasi TIK di Kota Magelang. Baik Komponen Pusat Data, Jaringan, Serta Sistem Penghubung Layanan untuk mendukung layanan TIK yang ada Pemerintahan Kota Magelang.

Berikut adalah beberapa gambaran kondisi:

1. Pusat Data Masih berupa Ruang Server dan tidak memiliki standar dan sertifikasi internasional, sehingga sangat berisiko mengganggu proses bisnis yang ada di pemerintahan kota magelang.

2. Masih ada OPD yang menyimpan server di fasilitas OPD sendiri, dan belum terpusat di Pusat Data Diskominsta Kota Magelang. Kurangnya Fasilitas Ruang Server OPD beresiko mengganggu pelayanan di Pemerintahan Kota Magelang.
3. Peremajaan dan Desain Jaringan yang tidak diperbaharui tidak sesuai dengan ekspektasi dari Pemerintahan Kota Magelang yang semakin meningkat.
4. Tidak tersedianya Redundancy Jaringan di Internal Kota Magelang, Baik dari sisi juga backup link untuk koneksi Non-Diskominsta (Koneksi Backup Untuk OPD Selain Jaringan Internal Diskominsta)
5. Tidak tersedianya Redundancy Power listrik untuk Switch Backbone di OPD.
6. Tidak Mempunyai Disaster Recovery Site.

### 3.2.1 Pusat Data

Diskominsta kota Magelang belum memiliki pusat data yang layak untuk digunakan untuk melayani akses server aplikasi dan data, serta layanan *colocation server* dari OPD di wilayah Kota Magelang.

Berikut adalah beberapa gambaran kondisi:

1. Fasilitas Ruang Server dan Fasilitas Kantor Diskominsta yang masih menggunakan Lahan Bukan Kepemilikan Pemerintahan Kota Magelang beresiko mengganggu Proses Pelayanan di Lingkungan Pemerintahan Kota Magelang
2. Penggunaan Genset yang tidak dedicated untuk data center, beresiko membuat beberapa server harus mati karena ketidakterediaan sumber listrik kedua (backup)

Tabel 6 : Kondisi dan Spesifikasi Fasilitas Data Center

No	Data Center	Spesifikasi	Alamat Lokasi
1	Ruang Server Diskominsta	<ul style="list-style-type: none"> <li>• Data Center Yang belum tersertifikasi dan terstandar</li> <li>• Satu jalur distribusi</li> <li>• UPS &amp; Genset Masih Belum Sesuai</li> </ul>	Jl. Jend. Sarwo Edhie Wibowo No.2, Tenjosari, Banyurojo, Kec. Mertoyudan, Kabupaten

		<ul style="list-style-type: none"> <li>• <i>Layout Data Center</i> Belum tertata</li> </ul>	Magelang, Jawa Tengah 56172
2	Collocation	<ul style="list-style-type: none"> <li>• Colocation Telkomsigma BSD Tangerang sejumlah 1 Rak 42U</li> </ul>	Graha Telkomsigma II Jl. CBD lot VIII Nomor 8, kelurahan lengkong gudang, Tangerang 15321
3	Disaster Recovery Site	Belum Mempunyai <i>dedicated Facility</i> untuk DRP	-



Gambar 10 : Kondisi Ruang Server Kota Magelang

Berikut daftar kemampuan dan kondisi *data center* di Pemerintah Kota Magelang saat ini. Diskominsta mengelola server-server aplikasi Pemerintah Kota Magelang. Server-server tersebut ditempatkan dalam suatu ruang server yang dikelola terpusat oleh Diskominsta dan Beberapa aplikasi layanan publik dan administrasi pemerintah ditempatkan di server tersebut, diantaranya aplikasi portal data DataGo, Magelang Cerdas dan aplikasi *command center dashboard*.



Gambar 11 : Infrastruktur Server Kota Magelang

Selain Secara fisik Diskominsta Kota Magelang juga menyediakan layanan cloud service internal berupa IaaS di <https://cloud.magelangkota.go.id> untuk OPD di lingkup kota magelang.

### 3.2.2 Jaringan

Infrastruktur TIK yang dikelola oleh Diskominsta, sudah menggunakan jaringan fiber optic mandiri dan bekerja sama dengan provider jaringan untuk internet. Jaringan tersebut sudah menghubungkan beberapa OPD yang ada di wilayah Kota Magelang. Selain jaringan fiber optic, jaringan wireless juga digunakan sebagai layanan tambahan publik untuk.

Berikut adalah beberapa gambaran kondisi:

1. Jaringan Intranet Pemerintahan Kota Magelang sudah memadai akan tetapi diperlukan Peremajaan dan Desain Jaringan sesuai dengan ekspektasi dari Pemerintahan Kota Magelang yang semakin meningkat.
2. Tidak tersedianya Redundancy Jaringan di Internal Kota Magelang, Baik dari sisi juga backup link untuk koneksi Non-Diskominsta (Koneksi Backup Untuk OPD Selain Jaringan Internal Diskominsta)
3. Tidak tersedianya Redundancy Power listrik untuk Switch Backbone di OPD.

Den berikut adalah gambaran detail spesifikasi jaringan yang ada di lingkungan pemerintahan kota magelang.

Tabel 7 : Spesifikasi Jaringan Kota Magelang

Topik	Spesifikasi	Keterangan
<b>Bandwidth</b>	<b>Internet</b>	Annual Fee IP-ADD/22
	- Link 1 : 800mbps (JMN)	103.86.138.0-
	- Link 2 : 500mbps (TELKOM)	103.86.139.255
	<b>Server</b>	2001:df0:6700 ::/48
	- NOC 50mbps	
	<b>Colocation:</b>	Periode Februari 2022- Januari 2023
	- 100mbps IIX	
	- 10mbps IX	
<b>Jaringan Intra</b>	<b>86 Titik</b>	
<b>Wireless Publik</b>	184	Wifi RW 184 titik di Wilayah RW @20mbps  RTH beberapa

Dari sisi infrastruktur jaringan, sudah terdapat jaringan antar Organisasi Perangkat Daerah (OPD) dan jaringan internet yang terpusat di Diskominsta. Internet sudah terpusat di Diskominsta

Tabel 8 : Daftar Fasilitas yang sudah terhubung Jaringan

No	Lokasi
<b>OPD</b>	
1	<b>Badan Kepegawaian, pendidikan dan Pelatihan (BKPP)</b>
2	<b>Badan Kesatuan Bangsa, Politik dan Perlindungan Masyarakat (Kesbangpolinmas)</b>
3	<b>Badan Penanggulangan Bencana Daerah</b>
4	<b>Badan Pengelola Keuangan dan Aset Daerah (BPKAD)</b>
5	<b>Badan Perencanaan Pembangunan Daerah (Bappeda)</b>
6	<b>Dinas Kepemudaan, Olahraga Dan Pariwisata (Disporapar)</b>

7	Dinas Kependudukan Dan Pencatatan Sipil (Disdukcapil)
8	Dinas Kesehatan (Dinkes)
9	Dinas Komunikasi, Informatika dan Statistik (Diskominsta)
10	Dinas Lingkungan Hidup (DLH)
11	Dinas Pekerjaan Umum dan Penataan Ruang (DPUPR)
12	Dinas Pemberdayaan Masyarakat, Perempuan, perlindungan Anak, Pengendalian Penduduk dan Keluarga berencana (DP4KB)
13	Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu (DPMPTSP)
14	Dinas Pendidikan dan Kebudayaan (P&K)
15	Dinas Perhubungan (Dishub)
16	Dinas Perindustrian dan Perdagangan (Disperindag)
17	Dinas Perpustakaan dan Kearsipan (Disperpusip)
18	Dinas Pertanian dan Pangan (Disperpa)
19	Dinas Perumahan dan Kawasan Permukiman (Perkim)
20	Dinas Tenaga Kerja (Disnaker)
21	Dinas Sosial (Dinsos)
22	Inspektorat Kota Magelang
23	Kecamatan Magelang Selatan
24	Kecamatan Magelang Tengah
25	Kecamatan Magelang Utara
26	RSU Tidar
27	Satuan Polisi Pamong Praja
28	Sekretariat Daerah
29	Sekretariat Dewan
<b>KELURAHAN</b>	
1	Kelurahan Wates
2	Kelurahan Cacaban
3	Kelurahan Gelangan
4	Kelurahan Jurangombo Selatan
5	Kelurahan Jurangombo Utara
6	Kelurahan Kedungsari
7	Kelurahan Kemirirejo
8	Kelurahan Kramat Selatan
9	Kelurahan Kramat Utara
10	Kelurahan Magelang
11	Kelurahan Magersari
12	Kelurahan Panjang
13	Kelurahan Potrobangsari
14	Kelurahan Rejowinangun Selatan
15	Kelurahan Rejowinangun Utara
16	Kelurahan Tidar Selatan

17	Kelurahan Tidar Utara
<b>KESEHATAN</b>	
1	Puskesmas Pembantu Botton
2	Puskesmas Gelangan
3	Puskesmas Jurangombo
4	Puskesmas Kerkopan
5	Puskesmas Magelang Selatan
6	Puskesmas Magelang Tengah
7	Puskesmas Magelang Utara
8	Puskesmas Magersari
9	Puskesmas Potrobangsari
10	Puskesmas Wates
11	Pustu Kyai langgeng
12	Pustu Jurangombo
13	Pustu Potrobangsari (Dumpoh)
14	Instalasi Farmasi
15	Laboratorium Kesehatan
16	RSB Paten / Pustu Rejowinangun
17	Puskesmas
18	PSC
19	RS Budi Rahayu
20	Pustu Panjang
21	Pustu Rejo Utara
<b>SEKOLAH</b>	
1	SMP N 1
2	SMP N 10
3	SMP N 11
4	SMP N 12
5	SMP N 13
6	SMP N 2
7	SMP N 3
8	SMP N 4
9	SMP N 5
10	SMP N 6
11	SMP N 7
12	SMP N 8
13	SMP N 9
<b>LAIN LAIN</b>	
1	Damkar
2	Magelang FM

3	Terminal Tipe C Magersari
4	Gedung Wanita
5	Kantor Bukit Tidar
6	GOR Samapta

### 3.2.3 Sistem Penghubung Layanan

Dengan kebutuhan data dan infrastruktur yang sangat pesat serta penggunaan Web Service yang tidak menyeluruh, belum mempunyai Web Service Gateway (Government Service Bus) untuk komunikasi dan monitoring API antar Aplikasi

## 3.3 Aspek Keamanan Informasi

Keamanan menjadi salah satu komponen vital dalam Layanan teknologi di wilayah kota magelang. Kurangnya manajemen keamanan akan membuat risiko keamanan CIA (Confidentiality, Integrity & Availability) semakin tinggi.

Berikut adalah beberapa gambaran kondisi:

1. Diskominsta Kota Magelang tidak mempunyai Kebijakan Sistem Manajemen Pengamanan Informasi (ISO 27001)
2. Belum ada struktur CSIRT, namun fungsi penanganan insiden keamanan informasi sudah dilakukan. Direncanakan akan dilakukan sosialisasi CSIRT dan Bimtek penanganan insiden dari BSSN.
3. Belum Melakukan Proses Manajemen risiko keamanan resiko yang terarah dan konsisten, sehingga berisiko kontrol keamanan informasi yang digunakan tidak relevan.
4. Belum mempunyai Standar dan SOP keamanan di Aplikasi dan Infrastruktur. Walaupun BSSN sudah memberikan panduan dan standar, kontrol keamanan belum dijalankan secara terukur
5. Proses Audit dan Assesment (VAPT (Vulnerability Assessment/ Penetration Testing)) sudah dilakukan akan tetapi belum konsisten
6. Diskominsta Kota Magelang tidak menggunakan *firewall dedicated* dan *Firewall, IDS, IPS, SIEM* untuk melindungi aset-aset informasi yang dimilikinya.
7. Kesadaran keamanan informasi masih belum dilakukan kepada seluruh ASN

### 3.4 Aspek Tata Kelola TIK

Tata Kelola TIK di Kota Magelang dapat digambarkan dalam 3 perspektif , yaitu:

1. Ter definisinya dan terlaksananya proses TIK (Perencanaan, Pengembangan, Operasional dan Audit TIK);
2. Adanya pelaksana TIK dengan Tupoksi nya (Diskominsta); dan
3. Adanya pengawas TIK dengan Tupoksi nya (Tim Perumus Kebijakan TIK).

Tabel 9. Tata Kelola TIK di Kota Magelang

No	Komponen	Kondisi Aktual	Keterangan
<b>1</b>	Perencanaan (Adanya Masterplan TIK )	Sudah ada	Grand Design Pengembangan Telematika Pemerintah Kota Magelang
<b>2</b>	Pengembangan		
	a) Pengembangan Infrastruktur Data Center	Sudah memiliki ruang server	Meletakkan server OPD dan server teknologi virtualisasi.
	b) Pengembangan Jaringan OPD	Seluruh OPD sudah terhubung	-
	c) Pengembangan Aplikasi khusus	Ada	Beberapa aplikasi dikembangkan untuk pelayanan
	d) Proses Penganggaran tahunan	Ada	Dana dan Realisasi Per Tahun
	e) Pengembangan SDM TIK	Dilakukan	Sudah melakukan pelatihan SDM bidang TIK
<b>3</b>	Operasional		
	a) Berfungsinya Operator OPD / PIC	Ada Tim Pengelola Jaringan Intra Pemerintah di beberapa OPD strategis	Terkoordinasi dengan Diskominsta

	b) Adanya Pusat Service Desk ( <i>Single point of contact</i> )	Belum memiliki call center layanan IT	
	c) Adanya Daftar Layanan TIK	<ol style="list-style-type: none"> <li>1. Layanan penyediaan internet</li> <li>2. Layanan colocation</li> <li>3. Layanan Pembuatan aplikasi</li> <li>4. Layanan video conference</li> <li>5. Layanan <i>help desk</i></li> </ol>	Sudah Ada
	d) Adanya SLA Layanan TIK	Belum punya SLA	-
4	Melaksanakan Audit TIK secara reguler	Sudah dilakukan	Sudah dilaksanakan asesmen Indeks KAMI dan VAPT
5	Tupoksi Diskominsta yang telah dan yang belum dilakukan secara optimal sebagai Diskominsta	Sudah di lakukan	Tata kelola Keamanan Informasi belum optimal
6	Tupoksi Dewan Pengarah TIK ( apakah sudah ada atau belum )	Sudah ada	Harus lebih dioptimalkan

### 3.5 Aspek SDM TIK

Salah satu aspek yang menjadi komponen layanan yang baik adalah SDM yang kompeten. Kurangnya manajemen SDM yang baik membuat kualitas layanan tidak terjaga bahkan gagal. Berikut adalah beberapa gambaran kondisi SDM TIK Diskominsta kota magelang.

1. SDM TIK yang ada di OPD tidak fokus di bidang TIK saja, tapi juga memiliki tupoksi di bidang lain
2. Jumlah dan Kompetensi SDM TIK yang ada di Diskominsta dipertanyakan karena tidak semua mempunyai sertifikasi yang relevan dengan fungsi jabatannya

### 3.6 Aspek Data dan Informasi

Informasi yang dihasilkan dari berbagai sistem informasi yang ada di Kota Magelang, secara umum dikonsumsi oleh masyarakat umum, masyarakat bisnis dan internal pemerintahan seperti Bupati dan OPD-OPD terkait.

Hal ini selaras dengan konsep arsitektur sistem informasi Pemerintah yang harus bisa menyajikan informasi untuk *Government-to-Citizen* atau *Government-to-Customer* (G2C), *Government-to-Business* (G2B), *Government-to-Government* (G2G) dan *Government-to-Employees* (G2E).

Berikut adalah beberapa gambaran kondisi:

1. Belum ada standar data yang dibuat, penggunaan standar merefensi ke Peraturan BPS No 4 Tahun 2020
2. Penggunaan Web Service sudah dilakukan untuk beberapa sumber data seperti DataGo, SIMBANGDA, SIMDA
3. Penggunaan data dari datago sudah digunakan sebagai bahan perencanaan pembangunan seperti RPJMD, RKPD, LKPJ & LPPD

#### A. Jenis Informasi

Jenis informasi yang sudah ada dan disajikan kepada pengguna informasi meliputi aplikasi Internal Pemerintah, dan portal *web* Kota Magelang. Terdapat 717 data yang telah dibagi.

#### B. Open Data (DataGo)

Kota Magelang sudah memberikan akses data yang mudah bagi masyarakat untuk mengetahui berbagai data melalui portal *web* data Kota Magelang. Data-data tersebut antara lain:

1. Data Ekonomi, Berisi laporan keuangan dari setiap OPD di Pemerintah Kota Magelang.
2. Data Energi
3. Data Industri
4. Data Infrastruktur, yang berisi status dan rencana pembangunan infrastruktur di kawasan Kota Magelang.
5. Kesehatan, berisi informasi yang meliputi seluruh data-data di RSUD dan Klinik di lingkungan Kota Magelang.
6. Maritim
7. Lingkungan Hidup, berisi informasi seputar keadaan lingkungan Kota Magelang

8. Pangan, berisi informasi yang meliputi data-data Ketersediaan Energi, Konsumsi Energi dan Ketersediaan Pangan di lingkungan Kota Magelang
2. Pendidikan dan Kebudayaan, berisi informasi segala aspek di bidang Pendidikan dan Kebudayaan di lingkungan Kota Magelang
3. Pariwisata, berisi informasi segala aspek di bidang Pariwisata di lingkungan Kota Magelang
4. Sosial, berisi informasi mengenai jumlah Penduduk di lingkungan Pemerintah Kota Magelang di bidang Sosial
5. Tata Kelola Pemerintahan

## BAB IV

### ANALISA KEBUTUHAN

#### 4.1 Analisa Risiko

Berikut adalah daftar risiko TI yang terdapat di lingkungan Pemerintah Kota Magelang beserta tingkat risiko untuk tiap Skenario Risiko TI:

Tabel 10 : Daftar Risiko TIK Kota Magelang

Kode Risiko	Skenario Risiko	Deskripsi Risiko	Kemungkinan	Dampak	Hasil	Level
R1	Terjadi gangguan terhadap server di data center kominfo atau server internal OPD	Berhentinya layanan Pemerintah Kota Magelang yang bersifat elektronik sehingga terjadi penurunan kinerja Pemerintah Kota Magelang	3	5	15	Sedang
R2	Terjadi gangguan terhadap Sistem Informasi atau Aplikasi	Berhentinya layanan Pemerintah Kota Magelang yang bersifat elektronik sehingga terjadi penurunan kinerja Pemerintah Kota Magelang	2	5	10	Rendah
R3	Terjadi kehilangan dan kebocoran data ke pihak yang tidak berwenang / berkepentingan	<ul style="list-style-type: none"> <li>· Hilangnya data dan bocornya informasi penting Pemda, sehingga menurunkan tingkat kepercayaan warga dan instansi</li> <li>· Belum terdapat SOP tentang penyimpanan data di server (bagian dari Tata Kelola Data )</li> </ul>	2	4	8	Rendah
R4	Terjadi gangguan terhadap ketersediaan (low availability)	Staf tidak bisa bekerja secara efektif sehingga terjadi penurunan produktivitas kerja	3	5	15	Sedang

Kode Risiko	Skenario Risiko	Deskripsi Risiko	Kemungkinan	Dampak	Hasil	Level
	layanan dasar TI (Internet / wifi)	dan pelayanan terhadap masyarakat				
R5	Belum terpenuhinya Kinerja TI (Target SLA dan Pencapaiannya) dalam pelaksanaan proses bisnis Pemerintah Kota Magelang	Staf tidak bisa bekerja secara optimal dan proses bisnis menjadi terganggu sehingga terjadi penurunan produktivitas kerja dan pelayanan terhadap masyarakat	3	5	15	Sedang
R6	Terjadi gangguan terhadap ketersediaan (low availability) Data dan Informasi yang dibutuhkan oleh proses bisnis Pemerintah Kota Magelang	Belum terdapat jaminan recovery data (RPO & RTO) sesuai kebutuhan proses bisnis sehingga menjadi terganggu atau bahkan bisa berhenti dalam waktu yang terlalu lama dan menyebabkan kerugian	2	3	6	Rendah
R7	Terjadinya akses dan modifikasi data yang dilakukan oleh user yang tidak berhak	<ul style="list-style-type: none"> <li>Belum optimalnya tata kelola data yang mengacu kepada suatu best practice framework Data Governance</li> <li>Data Security Awareness untuk pegawai belum terbentuk</li> </ul>	2	5	10	Rendah
R8	Terjadi gangguan kelistrikan pada Data Center Kominfo dan server internal OPD	Berhentinya seluruh layanan TI dan potensi terjadi kerusakan perangkat / sistem TI yang masih berada di Data Center (on premise) sehingga proses bisnis Pemda yang terkait dengan sistem tersebut terganggu atau bahkan berhenti	2	5	10	Rendah

Kode Risiko	Skenario Risiko	Deskripsi Risiko	Kemungkinan	Dampak	Hasil	Level
R9	Terjadi ketergantungan layanan dengan pihak ketiga yang belum termaktub dalam kontrak dengan baik.	Lemahnya pengelolaan pihak ketiga dalam hal kontrak, monitor, serta proses pemutusan & pergantian pihak ketiga terkait keamanan informasi sehingga tidak sesuai dengan kebutuhan proses bisnis Pemda	5	5	25	Sangat Tinggi
R10	Terjadi penyalahgunaan user ID	Perubahan rotasi atau mutasi pegawai belum selaras secara sepenuhnya dan real-time dengan perubahan hak akses aplikasi sehingga bisa terjadi pelanggaran keamanan akses data oleh pengguna yang tidak berwenang	5	4	20	Tinggi
R11	Belum terkelolanya keamanan informasi berbasis proses secara terpusat	Belum adanya Tugas, Wewenang dan Tanggung Jawab secara terstruktur dan formal terhadap pengelolaan keamanan informasi untuk seluruh OPD	3	5	15	Sedang
R12	Terdapat lubang keamanan di Sistem Informasi / Aplikasi yang dikembangkan oleh OPD sehingga dapat dieksploitasi oleh peretas	Belum adanya standar secure programming untuk memastikan bahwa keamanan Sistem Informasi yang dikembangkan sudah berkualitas (sesuai security requirement)	4	5	20	Tinggi
R13	Terjadi insiden keamanan secara tiba-tiba karena tidak ada informasi (peringatan dini) tentang potensi ancaman dan	Belum ada mekanisme penanganan saat ditemukan potensi ancaman atau lubang keamanan baik dari pihak ketiga maupun dari internal Pemda	4	5	20	Tinggi

Kode Risiko	Skenario Risiko	Deskripsi Risiko	Kemungkinan	Dampak	Hasil	Level
	lubang keamanan yang ada					
R14	Terjadinya penggunaan software ilegal di lingkungan Pemerintah Kota Magelang	Terjadi penggunaan software ilegal atau penggunaan hak cipta tanpa adanya perizinan	5	4	20	Tinggi
R15	Terjadinya pengembangan aplikasi tanpa rekomendasi dari Diskominsta dan pusat	Terjadi pelanggaran kepatuhan terhadap regulasi yang ada terkait pengembangan aplikasi umum dan aplikasi khusus	4	4	16	Tinggi
R16	Penggunaan teknologi aplikasi yang sudah lama dan tidak adanya dokumentasi aplikasi yang baik	Terdapat penggunaan teknologi/framework aplikasi yang sudah lama dan tidak adanya dokumentasi aplikasi yang baik sehingga akan menyulitkan pada saat melakukan pengembangan aplikasi	2	5	10	Rendah

Berbagai risiko TI yang masih memiliki tingkat Rendah, Sedang, Tinggi dan Sangat Tinggi perlu dimitigasi dengan penerapan berbagai kontrol atau kendali risiko agar tidak mengganggu kelangsungan proses pelayanan di Pemerintah Kota Magelang secara signifikan. Hanya risiko TI yang telah memiliki tingkat sangat rendah saja yang dapat diterima oleh Pemerintah Kota Magelang.

Oleh karena itu, untuk menurunkan tingkat risiko TI menjadi tingkat sangat rendah maka diperlukan penerapan berbagai kontrol atau kendali yang efektif berbasis Annex A pada standar SNI ISO/IEC 27001.

Berikut adalah rekomendasi 50 (lima puluh) kontrol atau kendali risiko berbasis Annex A pada standar SNI ISO/IEC 27001 yang perlu diterapkan oleh Pemerintah Kota Magelang agar semua risiko TI dapat dimitigasi secara efektif :

Tabel 11 : Daftar Risiko dan Kontrol

No	Domain	Control Objective	Control	Risiko
1	Kendali Akses	A9.1 Persyaratan bisnis untuk kendali akses	A9.1.1 Kebijakan kendali akses	R3, R7
2	Kendali Akses	A9.4 Kendali akses sistem dan aplikasi	A9.4.1 Pembatasan akses informasi	R3
3	Kendali Akses	A9.2 Manajemen akses pengguna	A9.2.1 Registrasi dan pembatalan registrasi pengguna	R10
4	Kendali Akses	A9.2 Manajemen akses pengguna	A9.2.2 Penyediaan akses pengguna	R10
5	Kendali Akses	A9.2 Manajemen akses pengguna	A9.2.3 Manajemen hak akses istimewa	R10, R7
6	Kendali Akses	A9.2 Manajemen akses pengguna	A9.2.4 Manajemen informasi otentikasi rahasia dari pengguna	R10
7	Kendali Akses	A9.2 Manajemen akses pengguna	A9.2.5 Reviu hak akses pengguna	R10
8	Kendali Akses	A9.2 Manajemen akses pengguna	A9.2.6 Penghapusan atau penyesuaian hak akses	R10
9	Manajemen aset	A8.1 Tanggungjawab terhadap aset	A8.1.1 Inventarisasi aset	R7, R14, R15
10	Manajemen aset	A8.1 Tanggungjawab terhadap aset	A8.1.2 Kepemilikan aset	R7, R14, R15
11	Manajemen aset	A8.1 Tanggungjawab terhadap aset	A8.1.3 Penggunaan yang dapat diterima atas aset	R7, R14, R15

No	Domain	Control Objective	Control	Risiko		
12	Manajemen aset	A8.1	Tanggungjawab terhadap aset	A8.1.4	Pengembalian aset	R14
13	Manajemen aset	A8.2	Klasifikasi Informasi	A8.2.1	Klasifikasi informasi	R7
14	Manajemen aset	A8.2	Klasifikasi informasi	A8.2.2	Pelabelan informasi	R7
15	Manajemen aset	A8.2	Klasifikasi informasi	A8.2.3	Penanganan aset	R7
16	Keamanan fisik dan lingkungan	A11.2	Peralatan	A11.2.5	Pemindahan aset	R14
17	Kesesuaian	A18.2	Reviu keamanan informasi	A18.2.1	Reviu independen terhadap keamanan informasi	R6, R9, R15
18	Kesesuaian	A18.2	Reviu keamanan informasi	A18.2.2	Kesesuaian dengan kebijakan dan standar keamanan	R6, R9, R15
19	Kesesuaian	A18.2	Reviu keamanan informasi	A18.2.3	Reviu kesesuaian teknis	R6, R15
20	Kriptografi	A10.1	Kendali kriptografi	A10.1.1	Kebijakan terhadap penggunaan kendali kriptografi	R3
21	Keamanan sumber daya manusia	A7.2	Selama bekerja	A7.2.2	Kepedulian pendidikan, dan pelatihan keamanan informasi	R3
22	Aspek keamanan informasi dari manajemen keberlangsungan bisnis	A17.1	Keberlangsungan keamanan informasi	A17.1.1	Perencanaan keberlangsungan keamanan informasi	R1, R2, R6
23	Aspek keamanan informasi dari manajemen keberlangsungan bisnis	A17.1	Keberlangsungan keamanan informasi	A17.1.2	Mengimplementasikan keberlangsungan keamanan informasi	R1, R2, R6

No	Domain		Control Objective		Control	Risiko
24	Aspek keamanan informasi dari manajemen keberlangsungan bisnis	A17.1	Keberlangsungan keamanan informasi	A17.1.3	Memeriksa, mreview dan mengevaluasi keberlangsungan keamanan informasi	R1, R2, R6
25	Aspek keamanan informasi dari manajemen keberlangsungan bisnis	A17.2	Redundansi	A17.2.1	Ketersediaan fasilitas pengolahan informasi	R6
26	Manajemen insiden keamanan informasi	A16.1	Manajemen insiden keamanan informasi dan perbaikan	A16.1.5	Tanggapan terhadap insiden keamanan informasi	R6
27	Information security incident management	A16.1	Manajemen insiden keamanan informasi dan perbaikan	A16.1.3	Pelaporan kelemahan keamanan informasi	R13
28	Kebijakan keamanan informasi	A5.1	Arahan manajemen untuk keamanan informasi	A5.1.1	Kebijakan untuk keamanan informasi	R15
29	Keamanan operasi	A12.1	Prosedur dan tanggungjawab operasional	A12.1.4	Pemisahan lingkungan pengembangan, pengujian dan operasional	R3
30	Organisasi keamanan informasi	A6.1	Organisasi internal	A6.1.1	Peran dan tanggungjawab keamanan informasi	R11
31	Organisasi keamanan informasi	A6.1	Organisasi internal	A6.1.2	Pemisahan tugas	R11

No	Domain		Control Objective		Control	Risiko
32	Organisasi keamanan informasi	A6.1	Organisasi internal	A6.1.4	Hubungan dengan kelompok minat khusus	R11
33	Organisasi keamanan informasi	A6.1	Organisasi internal	A6.1.5	Keamanan informasi dalam manajemen proyek	R11
34	Keamanan fisik dan lingkungan	A11.2	Peralatan	A11.2.8	Peralatan pengguna yang tidak diawasi	R3
35	Keamanan fisik dan lingkungan	A11.2	Peralatan	A11.2.9	Kebijakan mengosongkan meja dan mengosongkan layar	R3
36	Keamanan fisik dan lingkungan	A11.2	Peralatan	A11.2.1	Penempatan dan perlindungan peralatan	R1, R2, R8
37	Keamanan fisik dan lingkungan	A11.2	Peralatan	A11.2.2	Utilitas pendukung	R1, R8, R4
38	Keamanan fisik dan lingkungan	A11.2	Peralatan	A11.2.3	Keamanan kabel	R1, R8
39	Keamanan fisik dan lingkungan	A11.2	Peralatan	A11.2.4	Pemeliharaan peralatan	R1, R2, R8
40	Hubungan pemasok	A15.1	Keamanan informasi dalam hubungan pemasok	A15.1.1	Kebijakan keamanan informasi untuk hubungan pemasok	R4, R6, R9
41	Hubungan pemasok	A15.1	Keamanan informasi dalam hubungan pemasok	A15.1.2	Memasukkan klausul keamanan dalam perjanjian pemasok	R4, R5, R6, R9
42	Hubungan pemasok	A15.1	Keamanan informasi dalam hubungan pemasok	A15.1.3	Rantai pasok teknologi informasi dan komunikasi	R4, R6, R9

No	Domain		Control Objective		Control	Risiko
43	Hubungan pemasok	A15.2	Manajemen penyampaian layanan pemasok	A15.2.1	Pemantauan dan reviu layanan pemasok	R4, R6, R9, R11
44	Hubungan pemasok	A15.2	Manajemen penyampaian layanan pemasok	A15.2.2	Mengelola perubahan layanan pemasok	R4, R6, R9
45	Akuisisi, pengembangan dan perawatan sistem	A14.1	Persyaratan keamanan sistem informasi	A14.1.1	Analisis dan spesifikasi persyaratan dan keamanan informasi	R12,R16
46	Akuisisi, pengembangan dan perawatan sistem	A14.1	Persyaratan keamanan sistem informasi	A14.1.2	Pengamanan layanan aplikasi pada jaringan publik	R12
47	Akuisisi, pengembangan dan perawatan sistem	A14.1	Persyaratan keamanan sistem informasi	A14.1.3	Perlindungan transaksi layanan aplikasi	R12
48	Akuisisi, pengembangan dan perawatan sistem	A14.2	Keamanan dalam proses pengembangan dan dukungan	A14.2.5	Prinsip rekayasa sistem yang aman	R12
49	Akuisisi, pengembangan dan perawatan sistem	A14.2	Keamanan dalam proses pengembangan dan dukungan	A14.2.6	Lingkungan pengembangan yang aman	R12, R16
50	Akuisisi, pengembangan dan perawatan sistem	A14.3	Data Uji	A14.3.1	Proteksi data uji	R12

Berbagai risiko TI di lingkungan Pemerintah Kota Magelang bukanlah risiko yang statis, namun bersifat dinamis sehingga dapat berubah-ubah sesuai dengan kondisi dan faktor baik internal maupun eksternal. Risiko-risiko TI yang baru dapat muncul seiring berjalannya waktu, dan berbagai risiko TI yang tercantum dalam dokumen Risk Register ini dapat berubah dari sisi kemungkinan (*likelihood*) maupun dampak (*consequence*).

Oleh karena itu, asesmen risiko TI harus dilakukan secara berkala dan konsisten agar berbagai risiko-risiko TI di lingkungan Pemerintah Kota Magelang dapat selalu di-*review* ulang agar dokumen IT Risk Register Pemerintah Kota Magelang ini selalu dalam kondisi yang *up-to-date* serta penerapan kontrol atau kendali tetap berjalan secara efektif untuk melakukan mitigasi terhadap risiko-risiko yang baru atau berubah.

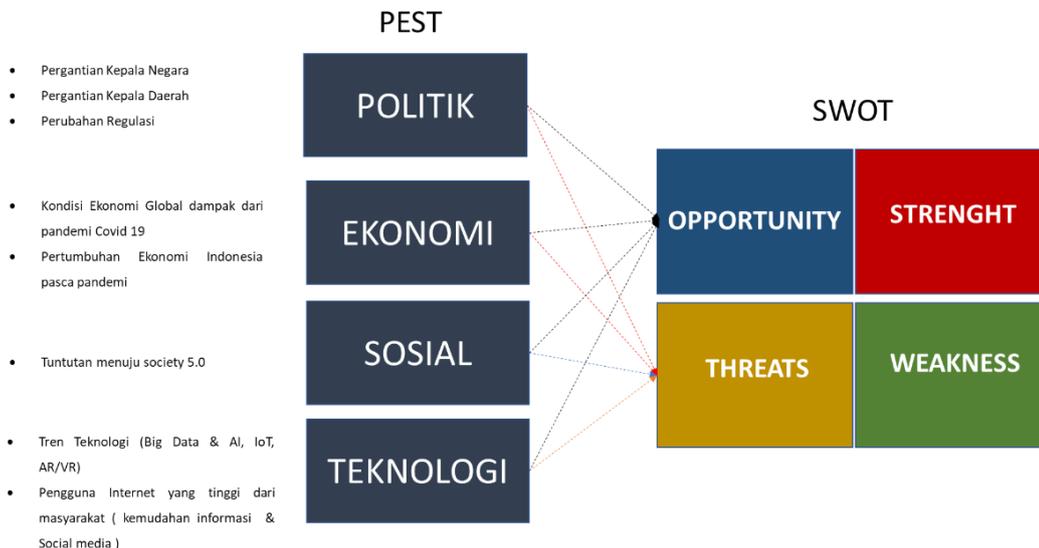
## 4.2 Analisa PEST

PEST *analysis* terkait dengan pengaruh lingkungan pada suatu bisnis. PEST merupakan suatu cara atau alat yang bermanfaat untuk meringkas lingkungan eksternal dalam operasi bisnis.

PEST harus ditindaklanjuti dengan pertimbangan bagaimana bisnis harus menghadapi pengaruh dari 4 aspek, yaitu:

1. *Politic*, meliputi kebijakan pemerintah, masalah-masalah hukum, serta mencakup aturan-aturan formal dan informal dari lingkungan dimana perusahaan melakukan kegiatan.
2. *Economic*, meliputi keadaan perekonomian pada waktu sekarang dan di masa yang akan datang dapat mempengaruhi kemajuan dan strategi organisasi.
3. *Social*, meliputi terpusat pada penilaian dari sikap masyarakat dan ASN yang mempengaruhi strategi.
4. *Technology*, meliputi perencanaan strategi yang efektif meneliti lingkungan untuk mencari perubahan teknologi yang dapat mempengaruhi operasional dan layanan, karena perubahan teknologi dapat memberikan peluang besar untuk meningkatkan hasil, tujuan atau mengancam kepercayaan masyarakat kepada pemerintah

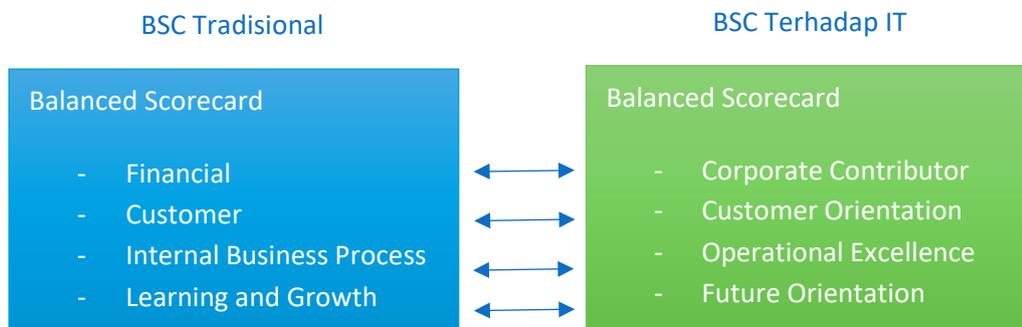
Dalam kaitannya Analisa Kebutuhan TIK Kota Magelang , berikut ini faktor-faktor eksternal yang mempengaruhi berdasarkan PEST *Analysis*:



Gambar 12 : Analisa Pest Kota Magelang

### 4.3 Balanced Scorecard

Balance Scorecard IT memandang Dinas Kominsta Kota Magelang merupakan penyedia layanan internal sehingga perspektif Balanced ScoreCard terhadap IT diubah seperti gambar berikut.



Gambar 13 : Perspektif Balance Scorecard terhadap TI

Terdapat beberapa perspektif dalam mengevaluasi kinerja SI/TI, yaitu:

1. Perspektif Kontribusi Organisasi (*Corporate Contribution*)
2. Perspektif Orientasi Pengguna (*Customer Orientation*)
3. Perspektif Keunggulan Operasional (*Operational Excellence*)
4. Perspektif Orientasi di Masa Depan (*Future Orientation*)

Analisa *Balanced Scorecard IT* di Pemerintah Kota Magelang, dapat dilihat pada tabel berikut.

Tabel 12 : Analisa *Balanced Scorecard*

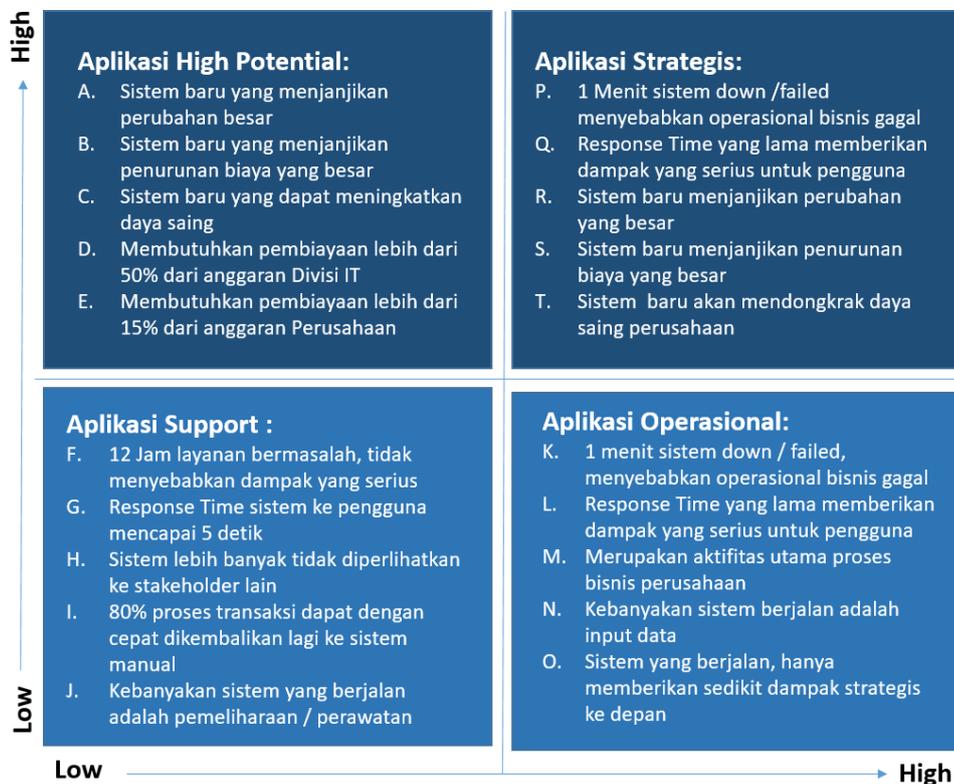
NO	Perspektif	Penjelasan	Sasaran Strategis TIK
1	<i>Corporate Contributor</i>	Hasil seperti apa yang diharapkan oleh Pimpinan	Memastikan IT yang sesuai dengan strategi organisasi ( Visi Misi dan Program Kerja )
			Mengelola IT Risk yang berkorelasi terhadap risiko organisasi
			Membuat transparansi dalam penganggaran IT yang memberikan value/manfaat untuk organisasi
2	<i>Customer Orientation</i>	Bagaimana memenuhi kebutuhan customer	Menyelenggarakan layanan IT yang sesuai dengan kebutuhan bisnis
			Menyediakan aplikasi dan teknologi yang memadai
3	<i>Operation Excellence</i>	Proses kerja yang dilakukan untuk meningkatkan kontribusi organisasi	Memastikan keamanan informasi dalam aplikasi dan infrastruktur
			Mengoptimalkan aset IT yang dimiliki
			Pengembangan IT yang berbasis pada project management ( scope, time, resource, quality )
			Menjamin ketersediaan dan kehandalan informasi
			Membangun IT yang sesuai dengan kepatuhan internal organisasi

4	Future Orientation	Bagaimana mutu SDM, organisasi dan IT dikelola dan dikembangkan	Membangun SDM IT yang kompeten
			Mengembangkan knowledge management untuk mendapatkan inovasi organisasi

#### 4.4 Analisa Grid McFarlan

*Strategic Grid McFarlan* bertujuan untuk menganalisis suatu aplikasi atau sistem informasi di suatu operasional organisasi/perusahaan berdasarkan kondisi saat ini, kondisi yang direncanakan serta aplikasi-aplikasi yang dianggap berpotensi dalam menunjang bisnis operasional. Sehingga mempermudah operasional pihak manajemen untuk mengambil keputusan dalam menentukan posisi SI/TI operasional organisasi/perusahaan serta keinginan operasional organisasi/perusahaan dalam menentukan ke arah mana SI/TI akan dipenuhi yang tentunya disesuaikan dengan kapabilitas dan visi serta misi operasional organisasi/perusahaan di masa yang akan datang.

Analisis Aplikasi Portofolio digunakan untuk memetakan aplikasi yang ada saat ini dan juga kebutuhan aplikasi dimasa akan datang dalam mendukung bisnis organisasi atau perusahaan. Pemetaan aplikasi ini dengan empat kuadran (*strategic, high potential, key operation, and support*) sesuai kategori penilaian suatu aplikasi terhadap dampaknya terhadap bisnis. Dari hasil pemetaan tersebut didapatkan gambaran kontribusi SI terhadap bisnis. Hasil tersebut dapat menjadi masukan bagi kegiatan pembuatan strategi SI dan kemungkinan pengembangannya ke depan.



Gambar 14 : Analisa Grid Mcfarlan Kota Magelang

Dari daftar modul aplikasi yang ada di Kota Magelang, masing-masing modul aplikasi dapat dikelompokkan ke dalam 4 kuadran (*High Potensial*, *Support*, *Operasional*, *Strategis*) berdasarkan kriteria atau indikator yang ditunjukkan dalam gambar berikut:

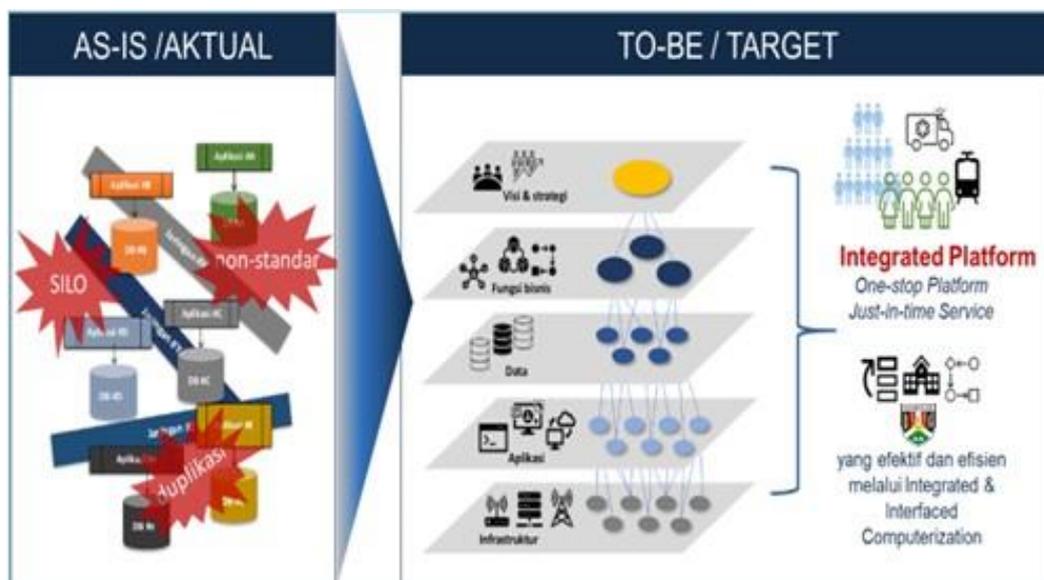
1. **Aplikasi yang masuk di kuadran *strategic*** adalah aplikasi yang merupakan aplikasi utama proses bisnis di Kota Magelang, yang harus terus menerus dikembangkan dan ditingkatkan kinerja dan keamanannya.
2. **Aplikasi yang masuk di kuadran *high potential*** adalah aplikasi yang saat ini memiliki potensi untuk menjadi strategis untuk masa yang akan datang, dan perlu lebih dikembangkan lagi untuk menjadi bagian utama dari bisnis proses di Kota Magelang.
3. **Aplikasi yang berada di kuadran *key operation*** adalah aplikasi yang saat ini sangat penting untuk dijaga efektivitas dan keberlangsungannya. Walaupun tidak begitu strategis, namun menjadi kunci keberlangsungan operasional di Kota Magelang.

4. **Aplikasi yang masuk di kuadran *support*** adalah aplikasi yang saat ini membantu dalam proses bisnis di Kota Magelang, namun tidak terlalu *critical* bagi proses bisnis di Kota Magelang. Aplikasi-aplikasi yang masih di kuadran *support* ini nantinya dapat bergeser di posisi *high potensial* maupun di kuadran *strategic* apabila ada perubahan tata kelola Pemerintahan Kota Magelang berdasarkan *benefit* (manfaat), *risk* (risiko) dan *resource* (anggaran dan SDM), serta melakukan suatu inovasi yang difokuskan kepada 3 aspek di *Digital Customer Experience*, *Internal Process* dan *Business Model*.

## BAB V

### KONDISI IDEAL

#### 5.1 Arsitektur Enterprise

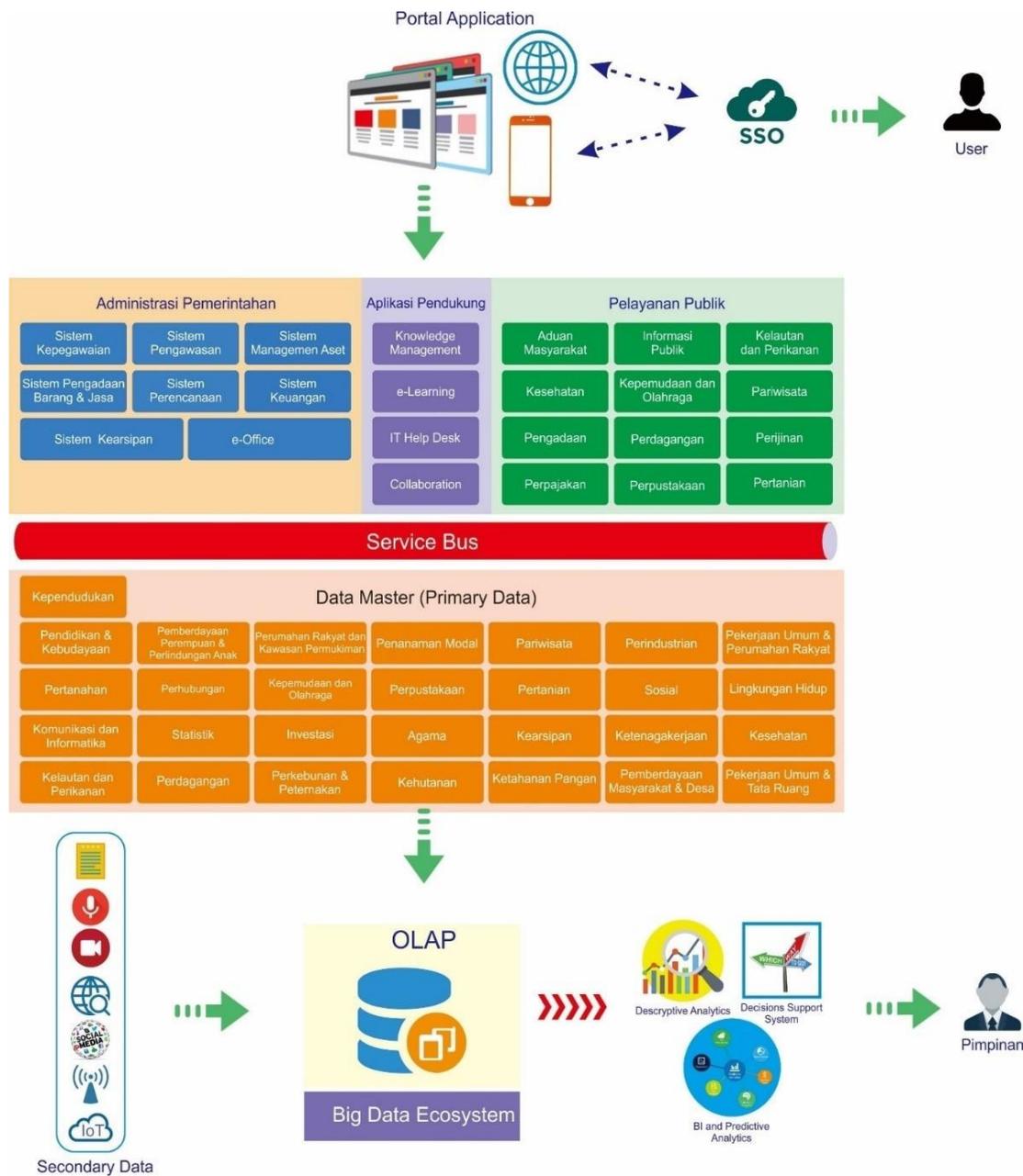


Gambar 15 : Arsitektur Enterprise Pemerintahan Kota Magelang

Arsitektur Enterprise merupakan kerangka dasar yang mendeskripsikan integrasi antara Fungsi Bisnis, Data, Aplikasi, Infrastruktur dan Keamanan Informasi di Pemerintahan Kota Magelang agar menghasilkan layanan untuk dapat mencapai visi misi Pemerintahan Kota Magelang. Diharapkan dengan adanya arsitektur enterprise membuat integrasi dapat dilakukan dengan efektif dan efisien dan tercipta *platform* yang terintegrasi untuk pengguna. Secara menyeluruh arsitektur enterprise merupakan bagian terpadu dan tidak terpisahkan dari domain penerapan implementasi TIK di suatu organisasi, salah satu bentuk dari arsitektur enterprise adalah arsitektur SPBE.

## 5.2 Arsitektur Aplikasi

Diagram aplikasi dapat digambarkan sebagai berikut :



Gambar 16 : Arsitektur Aplikasi

Secara fungsi dan proses dapat dijelaskan sebagai berikut :

### 1. Fungsi Login

Menggambarkan fungsi untuk mendapatkan hak akses ke dalam fungsi portal

**2. Fungsi Portal Front End**

Menggambarkan fungsi berupa rumpun layanan yang dapat dinikmati oleh pengguna, baik layanan administrasi pemerintahan dan layanan publik

**3. Fungsi Portal Back End**

Menggambarkan fungsi aplikasi aplikasi yang mendukung layanan , yang merupakan aplikasi umum dari pemerintah pusat, aplikasi khusus dari OPD dan aplikasi pendukung dapat dari Pusat atau Diskominsta

**4. Fungsi Sistem Penghubung**

Menggambarkan fungsi penghubung antar aplikasi dalam berbagi data, sehingga dapat mewujudkan *single entry system*

**5. Fungsi Data**

Menggambarkan fungsi penyimpanan data dalam format RDBMS yang menyimpan data transaksi dari aplikasi

**6. Fungsi Analitik**

Menggambarkan fungsi analisa data, yang berasal dari kumpulan data , baik dalam teknologi Data warehouse ataupun Big Data

**7. Fungsi Tampilan Data**

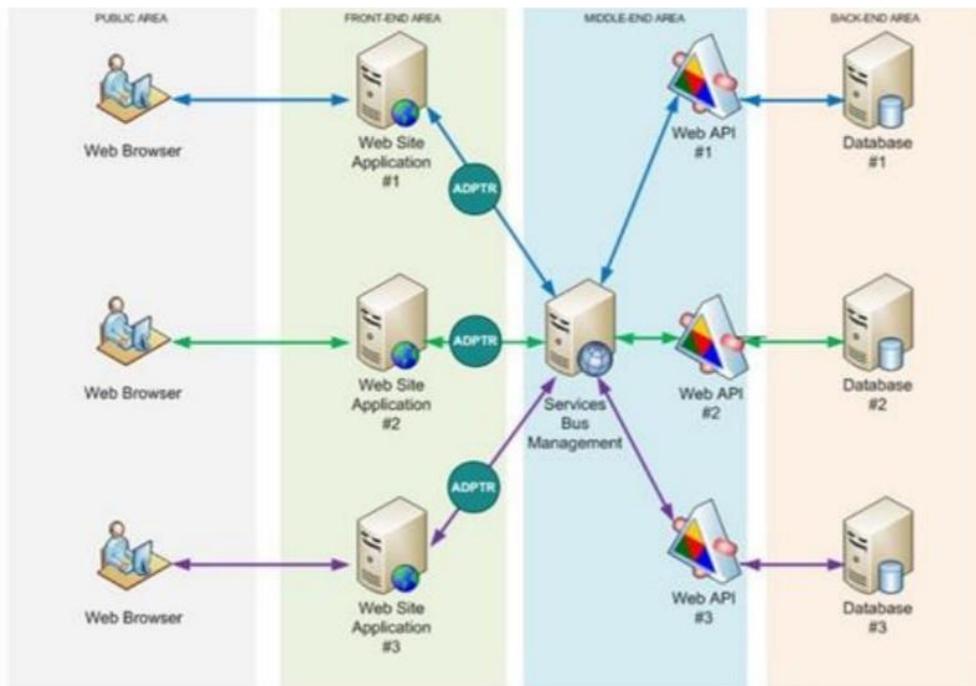
Menggambarkan fungsi perubahan data menjadi informasi dan knowledge sehingga mampu memberikan insight kepada *stakeholder* khususnya pimpinan

Dari fungsi-fungsi yang ada, maka dapat ditentukan infrastruktur yang mendukung hal tersebut.

- Infrastruktur Login / Single Single On
- Infrastruktur Portal
- Infrastruktur Aplikasi Umum
- Infrastruktur Aplikasi Pendukung
- Infrastruktur Aplikasi Khusus
- Infrastruktur Service Bus / Sistem Penghubung
- Infrastruktur Data Sektoral / Portal Data
- Infrastruktur Data Warehouse / Big Data
- Infrastruktur Jaringan Interkoneksi Tertutup
- Infrastruktur Jaringan Internet Terpusat

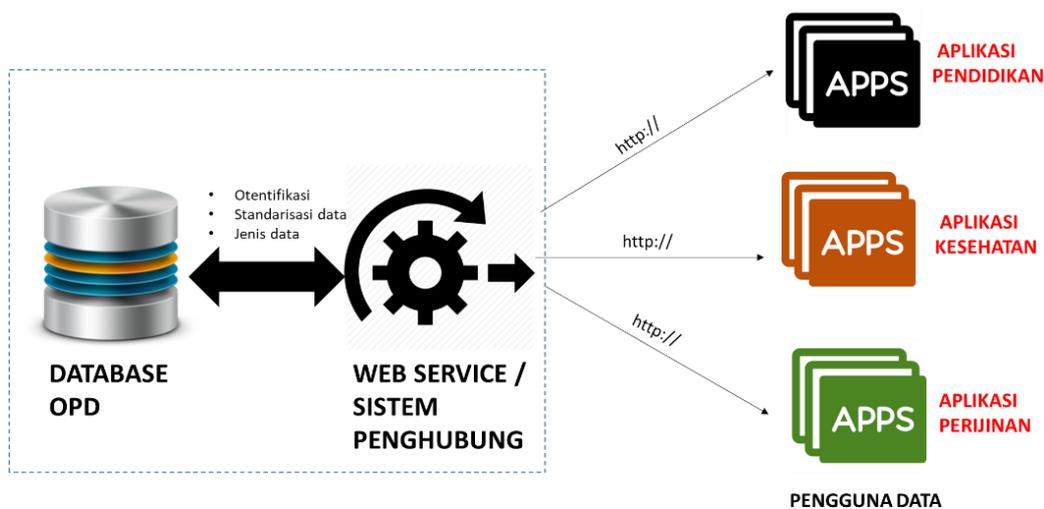
### 5.2.1 Diagram Sistem Penghubung Layanan

Digunakan oleh aplikasi untuk dapat memperoleh data (berbagi data) dari database dengan sistem yang berbeda. Penggambaran infrastrukturnya adalah sebagai berikut :



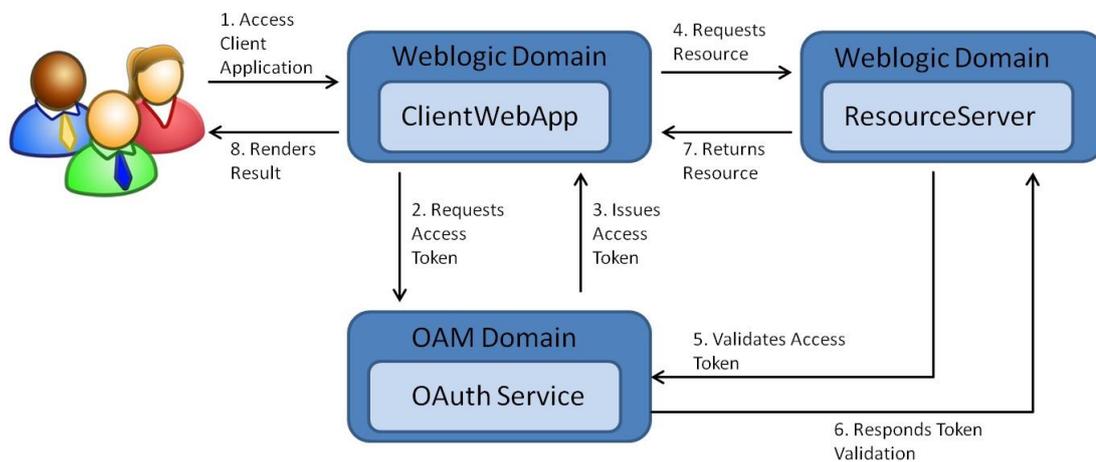
Gambar 17 : Diagram Sistem Penghubung Layanan

Di dalam *middle-end area* merupakan fungsi sistem penghubung layanan, sebagai contoh database server adalah database Disdukcapil, sedangkan *web application 1* adalah aplikasi Dinas Pendidikan, *web application 2* adalah aplikasi Dinas Kesehatan dan lain sebagainya.



Gambar 18 : Contoh Penerapan Sistem Penghubung Layanan

### 5.2.2 Diagram Single Sign On



Gambar 19 : Diagram Single Sign On

Dengan penjelasan fungsi , sebagai berikut :

- 1. Fungsi Interface Client Web App**  
 Tampilan untuk menginput user dan password
- 2. Fungsi SSO Oauth Service**  
 Menyadap permintaan dari pengguna yang mencoba mengakses sumber daya aplikasi web yang dilindungi dan menolak akses hingga pengguna memiliki otorisasi dari SSO Policy untuk mengakses sumber daya.
- 3. Fungsi Resource Server**  
 Server pemilik sumber daya yang akan diakses oleh pengguna. Pada saat pengguna melakukan akses sumber daya, maka Resource Server akan mengontak Oauth Service untuk meminta validasi akses sumber daya. Jika pengguna memiliki hak akses, maka Resource Server akan mengijinkan untuk mengakses sumber daya, namun sebaliknya jika pengguna tidak memiliki hak akses, maka Resource Server akan menolak hak akses tersebut.

### 5.2.3 Diagram Big data

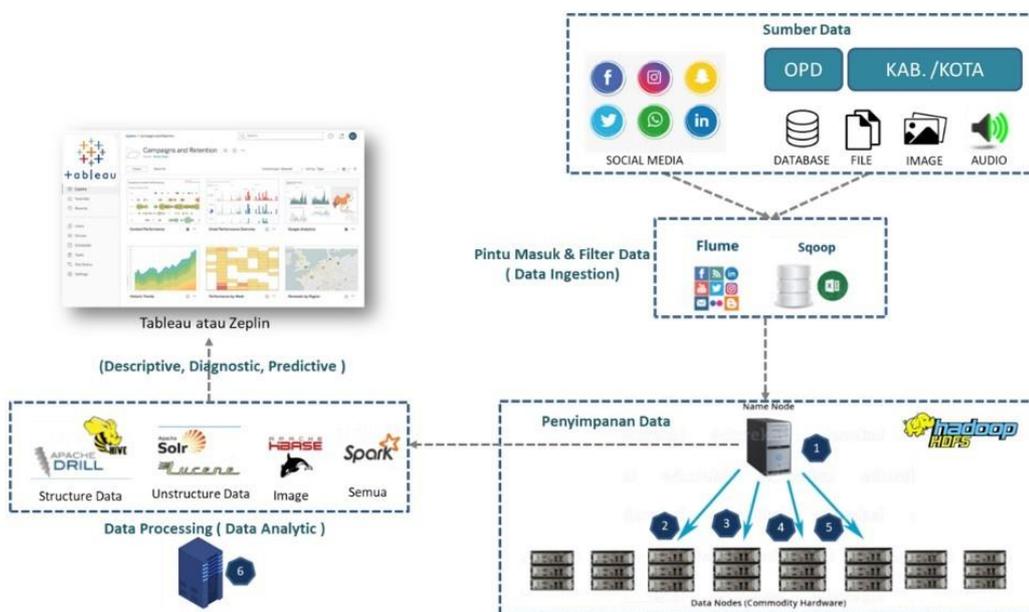
Penyusunan Arsitektur Data dan Informasi SPBE di Kota Magelang harus selaras dan sesuai dengan satu Data Jawa Tengah dan Satu Data Indonesia sebagai referensi gambaran pemanfaatan data yang ada di pemerintahan. Arsitektur Data dan informasi

yang baik membantu Kota Magelang dapat terwujud keselarasan antara pihak pusat sebagai induk hingga pihak daerah untuk pemanfaatan penerapan SPBE.

Arsitektur Big data dapat dimanfaatkan untuk mempercepat pelaksanaan dan pengawasan terhadap semua data dan informasi yang ada di pemerintah dan dapat juga mempercepat proses pengambilan keputusan sehingga dapat menciptakan berbagai kebijakan yang lebih cepat, akurat dan murah dengan berbagai institusi di pemerintahan.

Big Data yang menggunakan informasi dengan menggunakan pendekatan analitik, sehingga hasilnya menjadi lebih terstruktur, sehingga hasil Analisa data menjadi informasi dapat dilakukan secara cepat dan transparan.

Kota Magelang menggunakan big data sebagai kebutuhan kedepan untuk monitoring terhadap semua komponen yang ada di pemerintahan daerah, Dampak penggunaan Big Data dalam sektor pemerintahan adalah adanya transparansi pada data-data yang disajikan. Hal ini akan sangat berguna bagi masyarakat untuk mengetahui secara lebih transparan data-data yang mengenai pemerintahan sehingga dapat mewujudkan Open Government yang dapat meningkatkan kepercayaan masyarakat terhadap pemerintah. Dibawah ini adalah arsitektur big data yang akan dibuat oleh Kota Magelang



Gambar 20 : Diagram Infrastruktur Big Data

Dengan penjelasan fungsi sebagai berikut :

**1. Fungsi Sumber Data**

Adanya ketersediaan data yang berasal dari OPD, Portal Data Kota , CCTV , Dokumen, Social Media dan IoT ( Internet of Things)

**2. Fungsi Data Ingestion**

Peran untuk “menelan” seluruh sumber data ke dalam Big Data Infrastruktur

**3. Fungsi Storage Big Data**

Peran untuk menyimpan data dengan pola multi node dan Root Node

**4. Fungsi Processing Big Data**

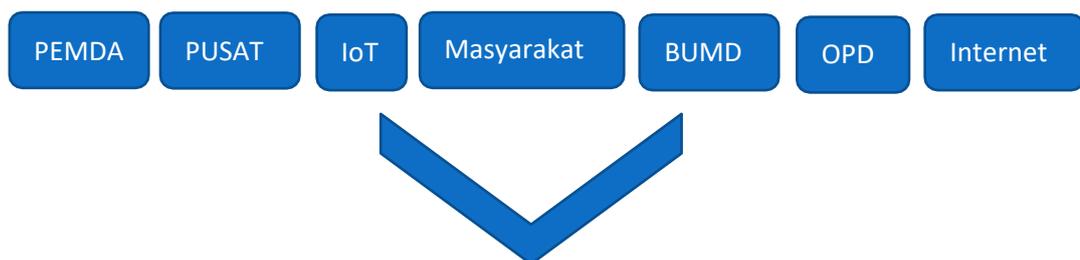
Fungsi untuk memproses data melalui tahapan analisa, menggunakan Machine Learning

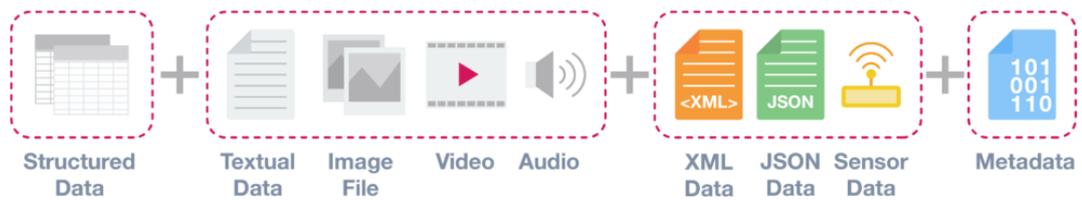
**5. Fungsi Presenting Data**

Fungsi untuk menampilkan informasi dan knowledge dalam bentuk *dashboard* yang mampu memberikan insight kepada stakeholder , khususnya pimpinan Daerah

#### 5.2.4 Sumber Data

Pada tahapan pertama dalam pembuatan arsitektur big data adalah Data Sources atau sumber data, Pemerintahan Daerah Kota Magelang berfokus pada aktivitas bagaimana/cara mendapatkan data yang dibutuhkan dalam proses pemerintahan Pemerintahan Daerah. Sumber data yang dapat digunakan oleh Kota Magelang sangat beragam jenisnya dan berasal dari berbagai sumber. Berdasarkan sumber data, data yang dapat digunakan oleh Kota Magelang dapat dikelompokkan menjadi beberapa tipe yaitu:





Gambar 21 : Source Data Big Data

- **Structured Data**  
 Jenis data yang dapat diproses, disimpan, dan diambil dalam format tetap/sudah terstruktur. Jenis data ini disimpan dalam bentuk tabel, baris dan kolom yang normalnya disimpan dalam excel atau spreadsheet/ Database, dimana informasi pada data sangat terorganisir dan dapat dengan mudah diakses.
  1. Sistem Informasi Pemerintah Daerah
  2. Sistem Informasi di masing masing OPD
  3. Portal Data Kota
  4. Dokumen (Excel, Text, CSV)
  5. Iot (Internet of Things)
  6. Website Pemerintah Daerah
- **Unstructured Data**  
 Data dengan bentuk yang tidak dikenal, harus disimpan dengan format khusus karena tidak memiliki struktur yang spesifik. Raw data dari jenis data ini hanya dapat menghasilkan nilai setelah diproses dan dianalisis. Menyimpan data jenis ini pun memiliki kerumitan seperti memerlukan penggunaan sistem penyimpanan yang memadai, seperti database NoSQL (MongoDB dan CouchDB).
  1. Email Internal Pemda
  2. Account Social Media Pemda
  3. Portal Berita (News)
  4. CCTV / Video (ATC)
  5. Data Teks dengan format khusus
  6. Foto / Gambar (Dokumentasi Acara/ Data Dari Masyarakat)
  7. Suara

- *Semi Structure*

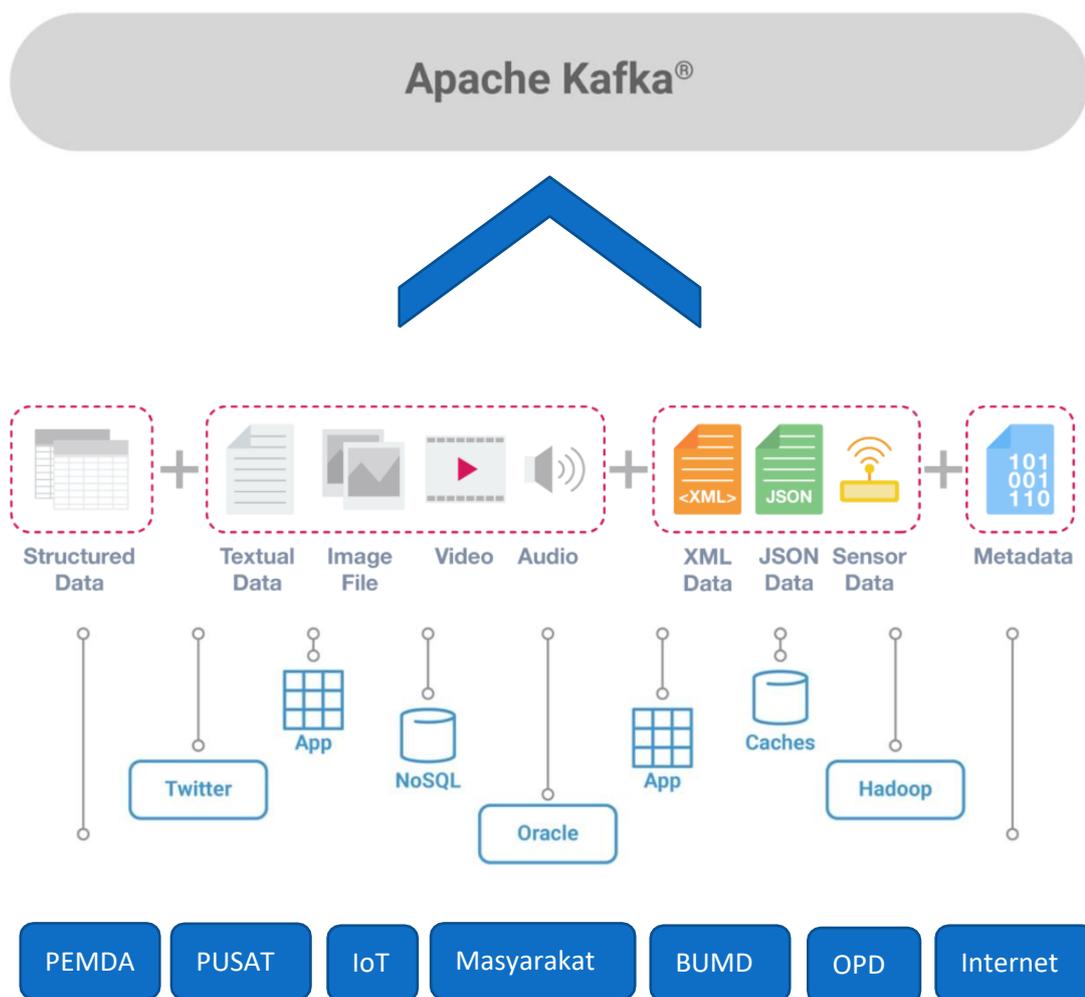
Jenis data yang dimasukkan ke dalam sebuah database, tetapi skemanya tidak sama dengan database biasa yang hanya terdiri dari baris dan kolom. Data semi-terstruktur mengandung format data terstruktur dan tidak terstruktur. Walaupun belum diklasifikasi oleh repository tertentu (database), namun mengandung informasi yang penting.

1. API (Application program interface)
2. CSV (Comma Separated Values) / Export Data dari system lain
3. File Xml (Extensible Markup Language) / Web Service Sistem Informasi Lain
4. File Json (Javascript Object Notation) / Web Service Sistem Informasi Lain

### 5.2.5 Data Ingestion

*Data Ingestion* adalah pengumpulan data dan membawanya ke dalam sistem pemrosesan, sehingga data yang dapat disimpan, dianalisis, dan diakses. Sistem pemrosesan data dapat. Dalam konteks pemerintahan daerah, semua data yang ada di pemerintahan, baik Structured, Unstructured dan semi unstructured dialirkan dan dikirim ke *Data Ingestion System* (Apache Kafka).

Apache Kafka merupakan platform terdistribusi untuk data streaming. Pada dasarnya, Apache Kafka merupakan sistem publish/subscribe messaging, dimana terdapat satu atau lebih sistem yang men-generate data untuk suatu topik tertentu secara real-time akan berkomunikasi dengan Apache Kafka (disebut sebagai Producers). Kemudian, topik tersebut dapat dibaca oleh satu atau lebih sistem yang membutuhkan data-data dari topik tersebut secara real-time (disebut sebagai Consumers). Apache Kafka “menelan” seluruh sumber data ke dalam Big Data Infrastruktur.



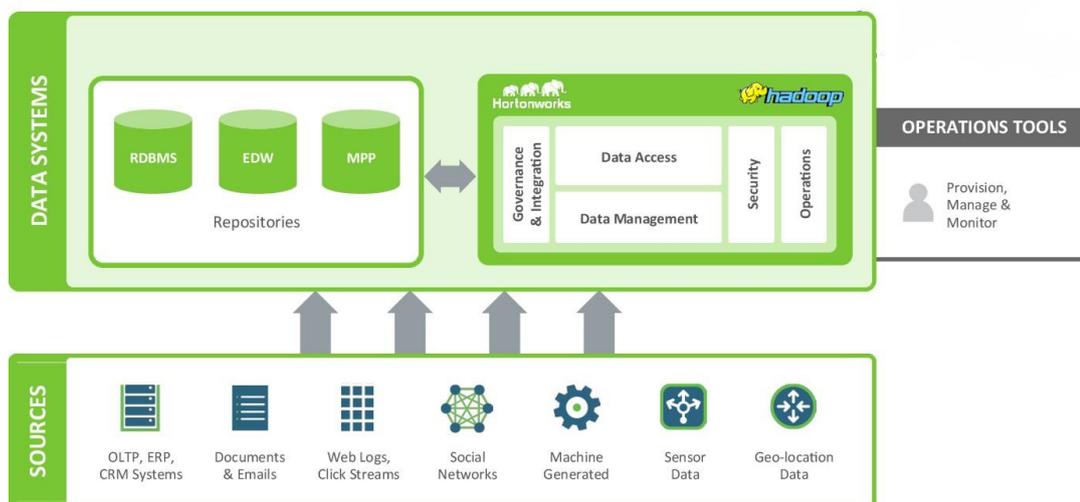
Gambar 22 : Data Ingestion Big Data Apache Kafka

### 5.2.6 Big Data Storage

Big data storage merupakan sistem untuk menyimpan, mengolah, dan mengambil data dalam jumlah besar, atau Big data. Penyimpanan Big data memungkinkan penyimpanan dan pemilahan Big data sedemikian rupa sehingga dapat dengan mudah diakses, digunakan, dan diproses oleh aplikasi dan layanan yang bekerja pada Big data.

Data yang telah diambil dari berbagai macam sumber di Kota Magelang akan disimpan dalam *server* yang sudah disiapkan untuk sistem *Big Data*. Sesuai dengan namanya, *Big Data* membutuhkan kapasitas penyimpanan data yang sangat besar, karena masuknya data yang sangat besar dan beragam ke dalam *server* setiap harinya. Salah satu alasan inilah disebut *Data Warehouse* karena proses penyimpanan, pengolahan, dan pengambilan data dari *server* akan sangat berbeda dengan *Database* biasa.

Hadoop ini tidak hanya merupakan software, melainkan kumpulan dari beberapa software yang saling bekerja sama dalam proses pengolahan data. Kita bisa menyebut Hadoop sebagai sebuah ekosistem dari software-software yang saling bekerja sama. Nah, untuk mengetahui bagaimana Hadoop bekerja, maka kita harus mengetahui software apa saja yang ada di balik Hadoop. Penasaran? Yuk simak ulasan berikut ini!



Gambar 23 : Data Storage Hadoop Menyimpan Data dari Kota Magelang

Hadoop Sendiri Mempunyai Beberapa Komponen:

### 1. Core Hadoop

Teknologi Core Hadoop menjadi software utama yang menjadi dasar dari penggunaan Hadoop. Core Hadoop ini terbagi menjadi HDFS (Hadoop Distributed File System) dan *Map Reduce*. Keduanya bisa di-download melalui website Apache

Hadoop. HDFS digunakan sebagai pendukung dalam proses pengolahan data dalam jumlah besar. Data-data yang memiliki volume besar tersebut akan diolah secara paralel, namun sebelumnya harus dibagi ke dalam bagian-bagian yang lebih kecil.

Selanjutnya proses dari HDFS akan dilanjutkan oleh tahapan Map dengan mengubahnya menjadi tuple. Dari data tersebut akan didapatkan key yang kemudian akan dipasangkan dengan value nya. Kemudian data dari tahapan Map ini akan dilakukan shuffle dan reduce dan dikembalikan ke HDFS lagi. Tahapan ini dinamakan Reduce.

## 2. Data Mining dan Database NoSQL

Data mining merupakan proses API (Application Programming Interface) yang berfungsi untuk menjalankan proses Map Reduce. Contoh dari Data Mining yang biasa digunakan dalam Hadoop adalah Apache Hive dan Apache Pig. Dengan adanya proses API maka akan lebih mudah dalam menjalankan Map Reduce dan juga mempermudah proses query.

Database NoSQL (Not Only SQL) biasanya digunakan untuk mempermudah proses Map Reduce yang terkadang memakan waktu yang sangat lama serta dilakukan secara periodik, karena data yang diproses dalam jumlah yang sangat besar. Database NoSQL ini dapat memberikan akses data yang lebih cepat dan sewaktu-waktu. Contoh dari Database NoSQL di dalam Hadoop adalah Apache Hbase dan Apache Cassandra.

## 3. Software Pendukung Lainnya

Software pendukung lain ini merupakan software yang digunakan untuk membantu proses operasional dari Hadoop. Misalnya untuk mengatur proses distribusi data dan pemrosesan data, ataupun mengatur input ke dalam Hadoop dari sumber data yang bersifat streaming. Misalnya, Apache Flume yang berfungsi untuk mengatur input ke dalam Hadoop dari sumber data yang bersifat streaming, seperti Twitter.

Selain yang telah disebutkan sebelumnya, ternyata masih banyak software pendukung Hadoop yang memiliki fungsinya masing-masing, seperti Apache Zookeeper, Apache Ambari, Apache Oozie, dll. Namun dalam proses penggunaannya,

tentunya kita tidak perlu menggunakan semuanya. Kita cukup memilih untuk menggunakan software mana yang lebih menunjang pekerjaan kita.

### 5.2.7 Data Analytic

Salah satu sifat dari *Big Data* selain ukuran data yang sangat besar, juga jenis data yang sangat beragam. Agar data-data tersebut dapat dianalisis dengan baik, maka terkadang data-data tersebut perlu diubah ke dalam format lain sehingga memungkinkan untuk dianalisis.

*Big data analytic* mempunyai komponen sebagai berikut:

#### 1. Data Mining

*Data mining* ini merupakan proses pengumpulan informasi untuk melihat pola dari kumpulan data yang sangat besar dan *data discovery*. Data mining memiliki fokus untuk mengekstrak pola dari data dengan menggunakan metode statistika agar dapat dianalisa. Hasil dari analisa ini akan digunakan untuk mencari prediksi yang tepat agar dapat digunakan untuk mengambil keputusan.

#### 2. Machine Learning Analytic

*Machine Learning* digunakan agar sistem komputer dapat melakukan proses pembelajaran dengan sendirinya secara otomatis tanpa diberi instruksi pemrograman terlebih dahulu serta dapat meningkatkan keakuratan hasil prediksi. Umumnya penggunaan machine learning bersifat real time. Machine Learning juga merupakan bagian dari *Artificial Intelligence* atau kecerdasan buatan.

#### 3. Apache Spark

Merupakan engine (perangkat lunak) analisis terpadu super cepat untuk memproses data dalam skala besar; meliputi Big Data dan machine learning dan memproses semua data yang ada di pemerintahan Kota Magelang .

Secara lebih detailnya, Apache Spark dapat didefinisikan sebagai engine (perangkat lunak) untuk memproses data dalam skala besar secara *in-memory*, dilengkapi dengan API pengembangan yang elegan dan ekspresif guna memudahkan analisa data yang membutuhkan perulangan akses yang cepat terhadap data yang diproses, seperti halnya *streaming*, *machine learning*, maupun SQL, secara efisien.



Gambar 24 : Integrasi Apache Kafka dan Apache

Data Analytics merupakan proses yang berkaitan dengan informasi yang Pemerintahan Daerah ingin dapatkan, atau hasil pengeolahan data melalui berbagai proses. Dan berikut merupakan kebutuhan yang ada di dalam pemerintahan berkaitan dengan analisa data di pemerintahan:



Gambar 25 : Kebutuhan Analisa Data Kota Magelang

Tahap analitik yang dibutuhkan oleh Kota Magelang adalah:

### 1. *Extraction & Integration*

Proses menghubungkan dan mengintegrasikan semua data yang dimiliki oleh Kota Magelang menjadi satu agar dapat di Analisa, proses ini ada di dalam data ingestion.

### 2. *Descriptive Analytics*

Analisa untuk mendapatkan gambaran umum / info dari data yang sudah dikumpulkan. Berupa model statistic yang membantu untuk memahami apa yang terjadi dan mengapa.

Contoh dari *descriptive analytics* adalah berapa jumlah Kamar tidur yang tersedia di RSUD, Berapa Jumlah Masyarakat yang komplain mengenai pelayanan pemerintahan, Berapa Jumlah Pasien yang positif covid, dll.

### 3. *Diagnostic Analytics*

Analisis lanjutan yang memeriksa data untuk menjawab pertanyaan, "Mengapa itu terjadi?, Mengapa Pasien Covid meningkat ?, mengapa ketersediaan kamar di rumah sakit kurang ? dll" . proses diagnosa Ini ditandai dengan teknik seperti penelusuran, penemuan data, penggalian data, dan korelasi.

### 4. *Predictive Analytics*

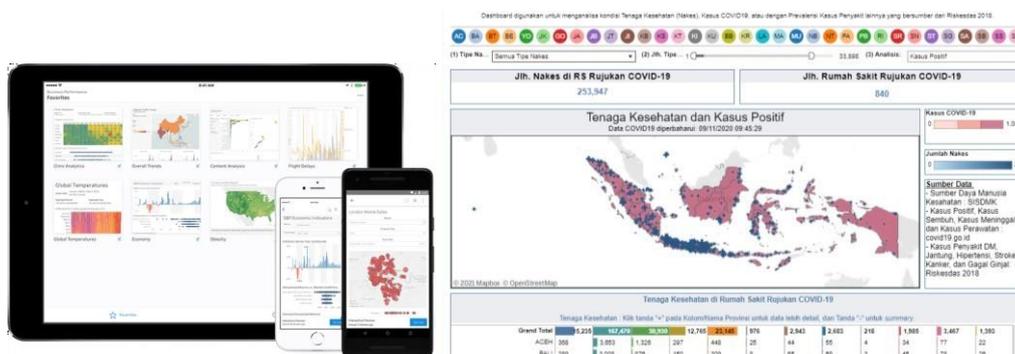
Analisa yang memberikan hasil prediksi tentang sesuatu yang akan datang, perkiraan jumlah pasien covid, perkiraan kenaikan pengangguran dan hasil Analisa yang bersifat prediksi. Analisa ini menjalankan ratusan atau ribuan model dengan cepat dan adopsi teknik prediktif seperti *support vector machines*, *neural networks* dan *random forests*, untuk dapat melakukan prediksi di masa depan

### 5. *Prescriptive Analytics*

Analisa data yang memberi informasi sesuatu akan terjadi serta memberikan saran respon terhadap kondisi yang kemungkinan akan terjadi dimasa yang akan datang. Dalam konteks pengambilan keputusan ini membantu top-level manajemen dalam mengambil keputusan. Contoh Analisa ini memberikan informasi bahwa tahun depan akan kekurangan kamar di rumah sakit umum daerah, dan memberikan saran berupa penambahan fasilitas.

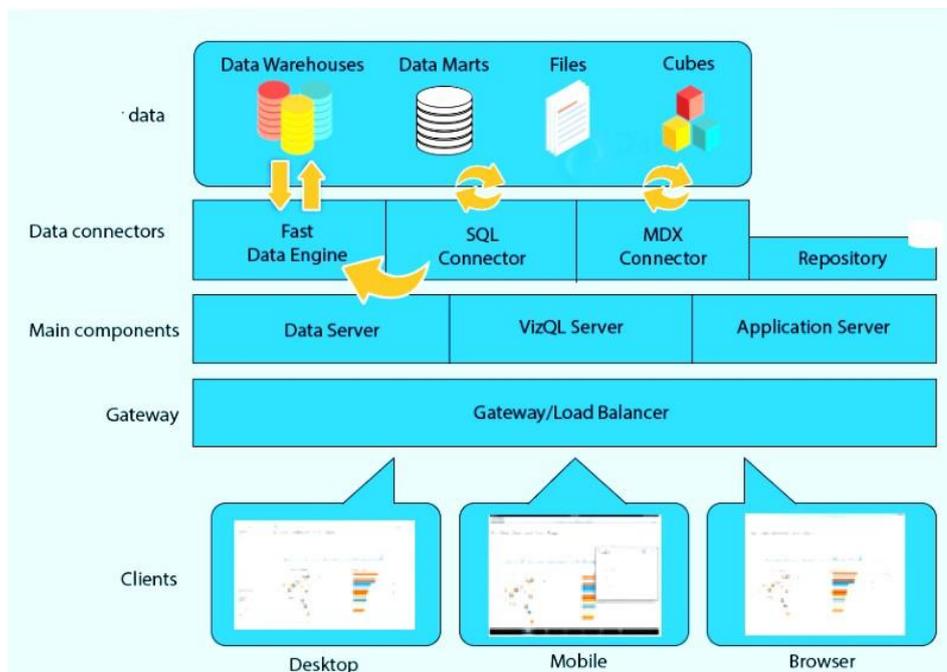
### 5.2.8 Visual Presenting Data

Kebutuhan untuk menampilkan hasil Analisa data dari berbagai macam sumber membantu Pemerintah Daerah Kota Magelang, untuk memantau pergerakan data secara real time. Aplikasi yang menampilkan informasi *executive summary* untuk melakukan pemantauan dan evaluasi seluruh layanan pemerintahan dan layanan public dapat digunakan untuk merespon semua kondisi dilapangan secara cepat. Beberapa fungsionalitas dan kriteria yang perlu diperhatikan dalam aplikasi Dashboard tersebut adalah platform untuk melakukan presentasi data dan bentuk dari presentasi data tersebut.



Gambar 26 : Multi Platform Dashboard Analisa Data Kota Magelang

Dengan menggunakan software visualisasi seperti Tableau atau PowerBI, maka data tersebut dapat digunakan dengan tepat. Berikut adalah arsitektur *software visual presenting data* dan kaitannya dengan data yang di visualkan :



Gambar 27 : Arsitektur Visual Presenting Data

Penggunaan software *visual presenting data* seperti Tableau atau PowerBI berfungsi untuk memvisualisasikan data dan menyederhanakan pola analisis *business intelligence* (BI). Fungsi lainnya adalah untuk menampilkan informasi dan *knowledge* dalam bentuk dashboard yang dimanfaatkan oleh sistem pemerintahan untuk mempercepat pelaksanaan program pemerintah. Beberapa manfaat yang dapat diambil dari Big Data di pemerintah dapat berupa pemanfaatan untuk program pemerintah, memberdayakan warga untuk meningkatkan transparansi dan partisipasi semua pemangku kepentingan.

## 5.3 Arsitektur Infrastruktur

Sehingga pijakan terdekat dari arsitektur infrastruktur ini adalah Arsitektur Aplikasi dan Arsitektur Data. Keberadaan infrastruktur merupakan bentuk kebutuhan sebagai dukungan untuk berjalannya aplikasi dan data dalam membentuk layanan SPBE.

Ruang lingkup Infrastruktur yang tertera dalam Perpres no. 95 tahun 2018 tentang SPBE adalah sebagai berikut :

### 1. Jaringan Intra Pemerintah

Jaringan interkoneksi tertutup yang menghubungkan antar Jaringan Intra Instansi Pusat dan Pemerintah Daerah.

### 2. Sistem Penghubung Layanan

Perangkat integrasi yang terhubung dengan Sistem Penghubung Layanan Instansi Pusat dan Pemerintah Daerah untuk melakukan pertukaran Layanan SPBE antar Instansi Pusat dan/atau Pemerintah Daerah.

### 3. Pusat Data Nasional

Pusat Data Instansi Pusat dan Pemerintah Daerah yang memenuhi persyaratan tertentu berupa standar internasional terkait desain Pusat Data dan manajemen Pusat Data.

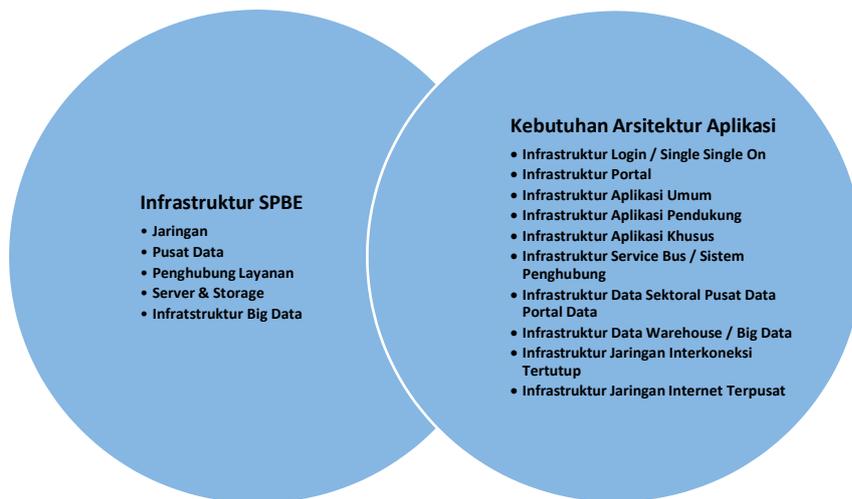
Salah satu referensi arsitektur SPBE sebagai komponen dasar adalah Prinsip. Prinsip digunakan sebagai ukuran keberhasilan dari pengembangan arsitektur. Dan prinsip untuk Arsitektur Infrastruktur adalah :

1. Seluruh sistem dan jaringan harus terkonsolidasi dan terintegrasi untuk penggunaan secara efektif dan efisien. Serta memastikan keberlanjutan layanan SPBE
2. Infrastruktur harus mudah dan konsisten untuk digunakan seluruh aplikasi
3. Memiliki sasaran keamanan untuk mendapatkan *confidentiality*, *integrity* dan *availability*
4. Memiliki sistem monitoring untuk server dan jaringan secara berkelanjutan.

### 5.3.1 Diagram Jaringan

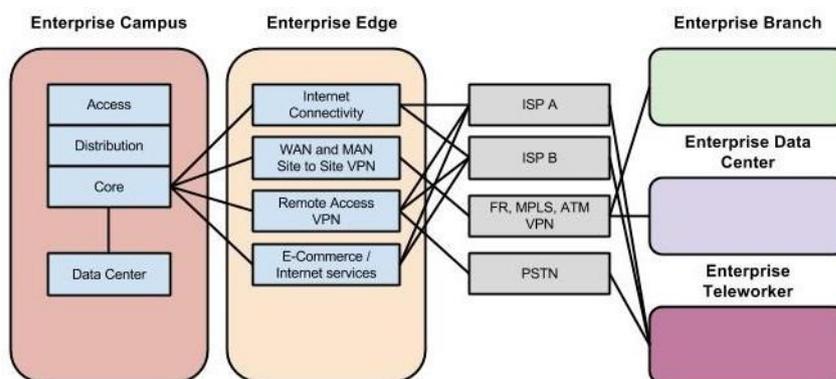
Kondisi ideal yang diinginkan dari Diskominsta adalah terhubungnya seluruh OPD melalui jaringan yang dikelola sendiri maupun jaringan *virtual private network* (VPN) melalui koneksi internet sebagai backup, dengan harapan semua OPD akan dapat saling berkomunikasi secara cepat dan dapat dilayani koneksi internetnya melalui koneksi

terpusat di Diskominsta. Disamping itu arsitektur jaringan yang memadai diharapkan dapat memenuhi kebutuhan dari Layer SPBE yang lain, dalam hal ini adalah kebutuhan di arsitektur aplikasi. Berikut adalah gambaran kebutuhan dari Arsitektur Aplikasi terhadap Arsitektur Infrastruktur SPBE.



Gambar 28 : Keterkaitan Kebutuhan Arsitektur Aplikasi dengan Arsitektur Infrastruktur

Dengan berbagai macam kebutuhan yang ada di dalam Arsitektur aplikasi dari Fungsi, login, Aplikasi, Sistem Pendukung dan Sistem utama yang ada, maka perlu dibuat arsitektur Jaringan yang sesuai dengan best practice dan dapat memenuhi kebutuhan Arsitektur Aplikasi SPBE, dalam proses pembuatan arsitektur tentu saja harus mengikuti kaidah dan *best practice* yang ada salah satu yang digunakan dalam proses penyusunan arsitektur jaringan adalah *network enterprise architecture*.

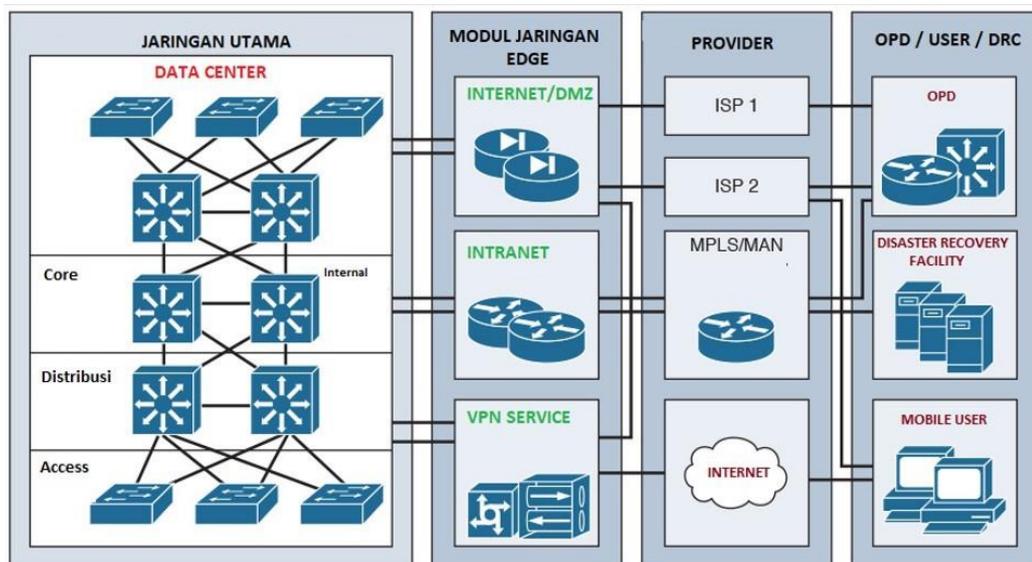


Gambar 29 : Network Enterprise Architecture

Dalam proses penyusunan arsitektur jaringan , lebih difokuskan untuk arsitektur core, intranet dan QOS untuk bisa menjamin layanan infrastruktur jaringan dapat memenuhi kebutuhan arsitektur aplikasi.

### A. Backbone / Core Network

*Backbone network* Kota Magelang merupakan inti/tulang punggung jaringan di Kota Magelang yang menjadi saluran pusat untuk melakukan transfer data. Berikut adalah gambaran arsitektur jaringan yang ada di Kota Magelang :

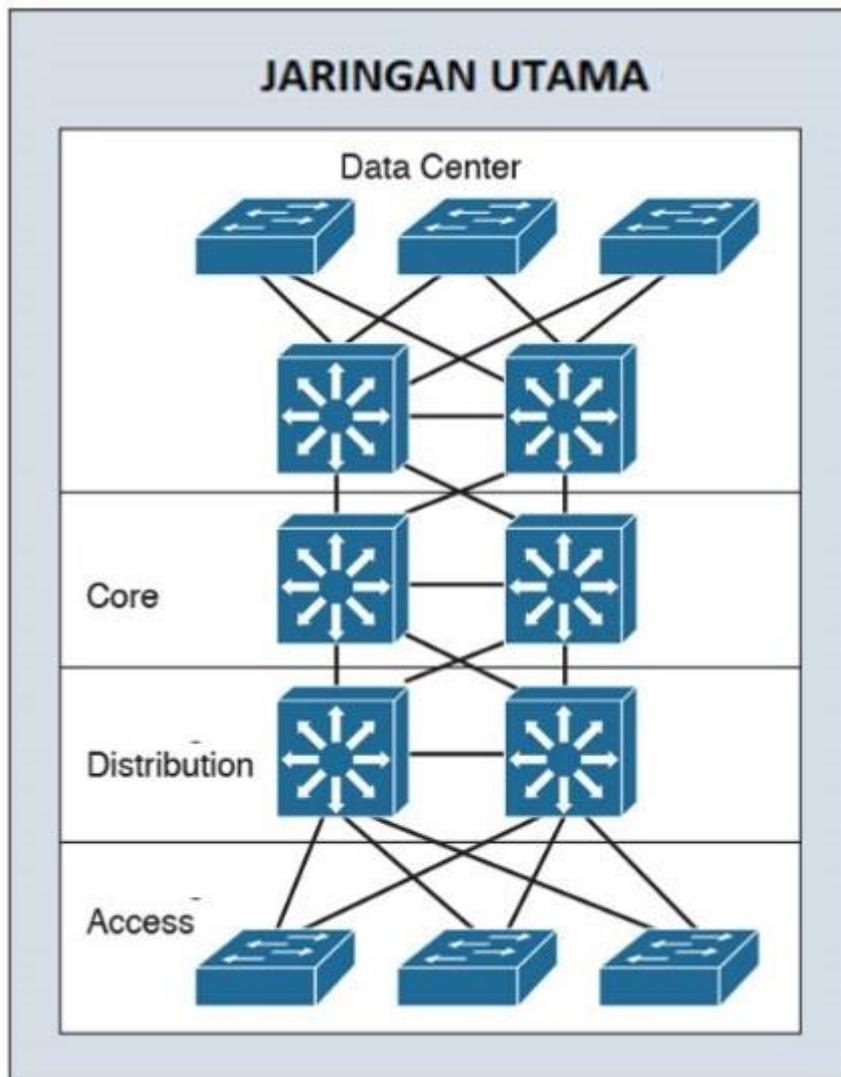


Gambar 30 : Network Enterprise Architecture

*Backbone* dalam jaringan biasanya dipakai untuk menghubungkan semua modul modul yang ada di jaringan Kota Magelang menjadi satu. Modul tersebut adalah:

#### 1. Network Diskominsta

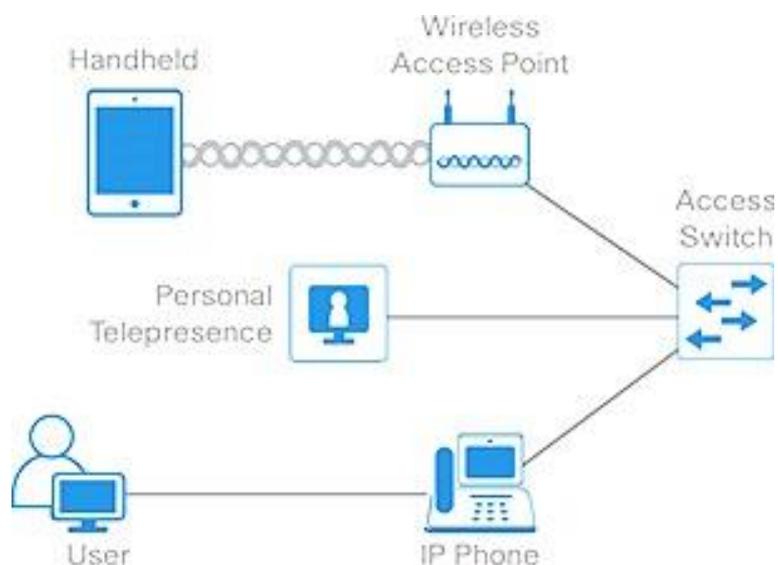
Merupakan Jaringan Utama dari Diskominsta Kota Magelang , dimana modul ini mempunyai beberapa sub modul antara lain:



Gambar 31 : Jaringan Utama Diskominsta Kota Magelang

- **Access Layer**

Access Layer mengendalikan akses pengguna/OPD ke sumber daya dan layanan yang ada di Kota Magelang . Desain access layer diperlukan untuk menyediakan fasilitas akses ke jaringan dan layanan Kota Magelang . Fungsi utamanya adalah menjadi sarana bagi suatu titik yang ingin berhubungan dengan jaringan luar (Internet/Intranet). Filtering data oleh firewall/router juga diperlukan untuk mencegah akses ke suatu IP tertentu.



Gambar 32 : Access Layer

Di dalam layer access lebih bagaimana jaringan menyediakan untuk koneksi ke sisi client (Mobile, Desktop, Notebook, Sensor, Iot, Voip Phone, CCTV dll) dan menyediakan beberapa feature seperti *port security, VLANs, Fast Ethernet/Gigabit Ethernet, PoE, and link aggregation* di dalam layanannya.

- **Distribution Layer**

Distribution layer adalah penghubung antara *access layer* dan *core layer*. Fungsi utama distribution layer adalah menyediakan routing, filtering dan untuk menentukan cara terbaik menangani permintaan layanan dalam jaringan. Setelah distribution layer menentukan lintasan terbaik maka kemudian permintaan diteruskan ke core layer. Core layer dengan cepat meneruskan permintaan itu ke layanan yang benar.

Distribution layer diterapkan kepada setiap modul yang ada di dalam jaringan baik itu Modul OPD, Modul Data Center, Modul Edge Network, Modul Internet dll. Dalam layer distribution dilakukan pembagian atau pembuatan segmen-segmen jaringan berdasarkan kebutuhan infrastrukturnya. Kebanyakan Fungsi Distribution Layer adalah:

1. Address atau Area Jaringan ke OPD
2. Akses dari OPD ke Jaringan Utama Diskominsta
3. Routing dari masing masing OPD Virtual LAN (VLAN)

4. Keamanan data dan jaringan (Security)
5. Titik dimana Akses secara Remote ke Jaringan dapat dilakukan

- **Core Layer**

Core layer adalah tulang punggung (backbone) dari jaringan. Layer ini biasanya digunakan untuk menghubungkan berbagai modul jaringan menjadi 1. Dalam jaringan di Kota Magelang . Core layer bertanggung jawab atas lalu lintas dalam jaringan. Dalam lapisan ini data – data diteruskan secepatnya dengan menggunakan metode dan protokol jaringan tercepat (high speed). Misalnya fast ethernet 100Mbps, Gigabit Ethernet, FDDI. Pada lalu lintas data digunakan switch karena penyampaiannya pasti dan cepat.

Dalam lapisan ini tidak diperbolehkan melakukan penyaringan atau filter paket data karena dapat memperlambat transmisi data dan tidak mendukung OPD. Untuk toleransi kesalahan digunakan peralatan yang redundancy.

## 2. **Data center**

Modul yang mempunyai spesifikasi tinggi untuk kebutuhan layanan di pemerintahan. Modul pusat data berkapasitas tinggi dan terpusat dapat menyediakan sumber daya server internal kepada OPD/User. Modul pusat data biasanya juga mendukung layanan manajemen jaringan untuk Pemerintahan, termasuk pemantauan, logging, pemecahan masalah, dan fitur manajemen umum lainnya dari ujung ke ujung. Modul pusat data juga biasanya berisi email internal dan server pemerintahan yang menyediakan aplikasi, file, cetak, email, dan layanan Domain Name System (DNS) untuk pengguna internal.

## B. Jaringan Edge

- **Internet dan zona demiliterisasi (DMZ)**

Modul yang menyediakan konektivitas menuju internet dan koneksi aman bagi pengguna ke layanan Internet Kota Magelang seperti server publik, email, dan DNS. Konektivitas ke satu atau beberapa penyedia layanan Internet (ISP) juga tersedia. Komponen ini termasuk router firewall dan firewall, router Internet, server FTP dan HTTP, server SMTP, dan server DNS.

- **VPN Service**

Modul yang menyediakan akses remote/vpn dari OPD/User untuk dapat mengakses layanan internal Kota Magelang , di dalam modul ini mempunyai

otentikasi untuk pengguna. Komponen submodul ini meliputi firewall, VPN konsentrator, Adaptive Security Appliances (ASA), dan peralatan sistem pencegahan intrusi jaringan (IPS).

- *WAN/Intranet*

Modul yang menghubungkan semua Remote Area baik OPD/User ke internal network Kota Magelang . WAN mencakup berbagai teknologi untuk menghubungkan antara OPD dengan Diskominsta Kota Magelang , Baik Menggunakan Fiber Optic Mandiri, maupun menggunakan Wan Service Provider sebagai pilihan kedua, atau keduanya. WAN mencakup teknologi seperti *Multiprotocol Label Switching (MPLS)*, *Metro Ethernet*, *leased lines*, *Synchronous Optical Network (SONET)* dan *Synchronous Digital Hierarchy (SDH)*, *PPP*, *Frame Relay*, *ATM*, *cable*, *digital subscriber line (DSL)*, dan *nirkabel*.

### C. Provider and Site

- **Internet Service Provider**

Internet Service Provider (ISP) merupakan Pemerintahan Daerah yang menyediakan jasa untuk mengakses atau menggunakan Internet, dalam kaitannya dengan pemerintahan Kota Magelang , internet sangat diperlukan untuk bisa mengakses data data yang menunjang administrasi pemerintahan dan layanan ke masyarakat yang diberikan oleh pemerintahan.

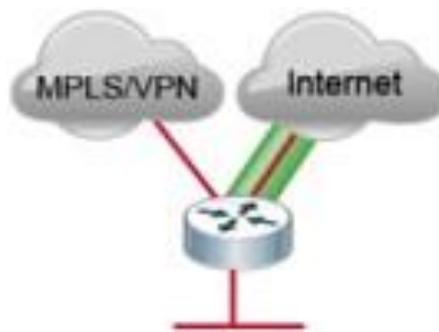
Karena pentingnya infrastruktur tersebut maka, setidaknya kota memiliki dua atau lebih ISP untuk menunjang kebutuhan tersebut.



Gambar 33 : Double ISP Kota Magelang

- **WAN/MPLS Service**

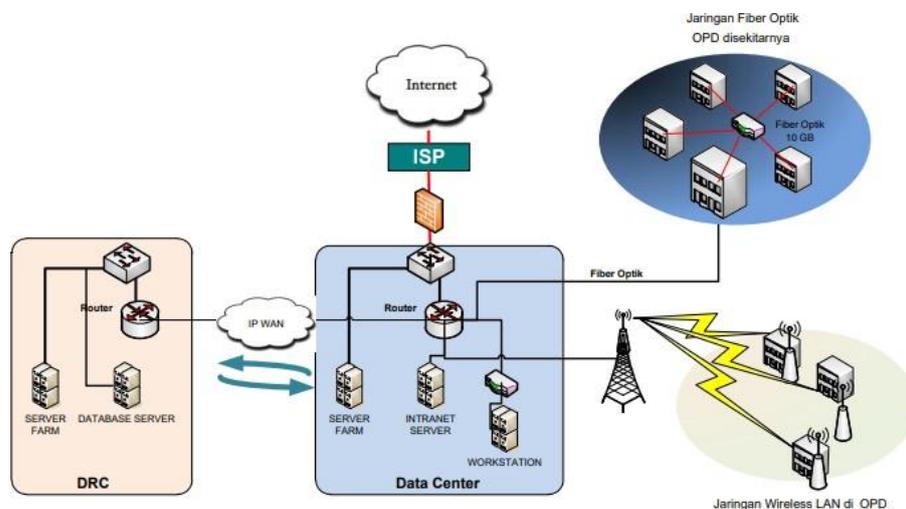
Multiprotocol Label Switching (atau disingkat MPLS) merupakan sebuah metode transmisi data yang menggunakan label untuk melakukan forwarding paket data. Dengan penggunaan label ini maka pengiriman paket data akan dilakukan dalam kelompok-kelompok. Setiap kelompok yang ditransmisikan tidak terkait dengan kelompok lainnya. Dengan penggunaan label dalam transmisi data MPLS merupakan metode transmisi dengan beban proses yang minimal.



Gambar 34 : Redundancy MPLS/FO/VPN dan Internet

- **Disaster Recovery Center (Pusat Data Nasional/ DRC Provinsi Jateng)**

DRC (Disaster Recovery Center) adalah sebuah tempat yang mana ditujukan untuk menempatkan perangkat IT, sistem, aplikasi dan data cadangan untuk bisa menghadapi bencana yang diperlukan oleh pemerintahan. Bencana yang serius ini tidak hanya bisa menimpa satu unit kerja saja namun bisa beberapa unit. Unit yang sering terserang adalah penyimpanan data dan juga pengolahan data maupun informasi.



Gambar 35 : Replikasi layanan di DRC

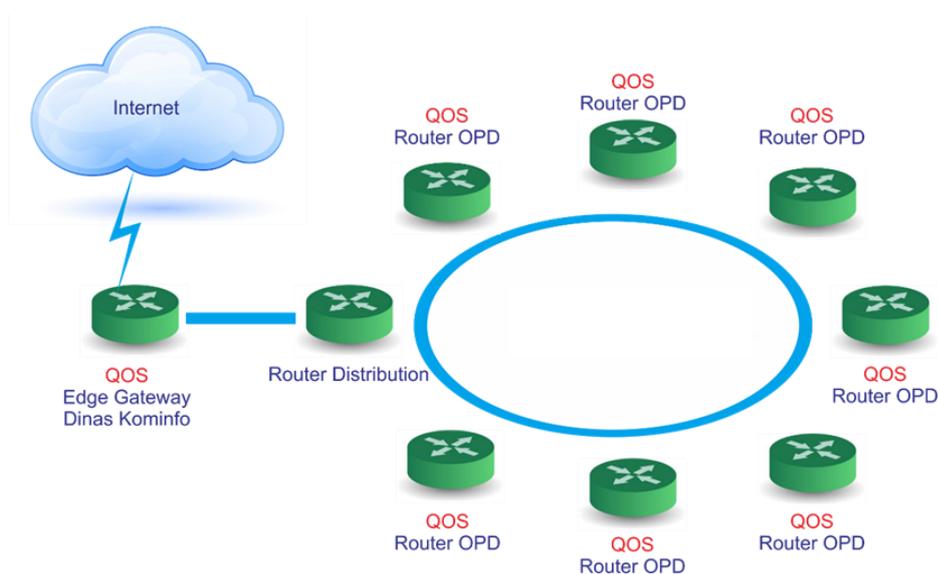
Berdasarkan cara kerjanya, DRC memiliki beberapa jenis, antara lain:

- **Cold DRC**  
Menyediakan sistem yang sama seperti di lokasi data center di Pemerintah dimana aplikasi dan data akan diupload sebelum fasilitas drc bisa digunakan, namun proses pemindahan dari data center ke lokasi DRC akan dilakukan secara manual.
- **Warm DRC**  
Menyediakan komputer dengan segala komponennya, aplikasi, link komunikasi, dan backup data yang paling update, dimana system tidak otomatis berpindah tetapi masih terdapat proses manual meskipun dilakukan seminimal mungkin.
- **Hot DRC**  
Mengatur secepat mungkin operasional pemerintahan, system dengan aplikasi, link komunikasi yang sama sudah dipasang dan sudah tersedia di lokasi DRC, data secara terus menerus di-backup menggunakan koneksi live antara data center dan lokasi DRC, dan operasional pemerintahan akan berjalan pada saat itu juga, tanpa harus mematikan sistem di data center lama.

#### D. Intranet

Kota Magelang sudah memiliki Jaringan FO yang menghubungkan setiap OPD, sehingga membangun interkoneksi tertutup. Secara keseluruhan dibutuhkan jaringan interkoneksi tertutup yang menghubungkan semua OPD di Kota Magelang . Kebutuhan titik-titik LAN yang terhubung ke dalam jaringan interkoneksi tertutup Kota Magelang ,.

Dengan menggunakan jaringan metronet maupun internet Diskominsta Kota Magelang masing-masing OPD dapat terhubung dan menggunakan layanan yang ada disediakan oleh Diskominsta Kota Magelang Kota Magelang .



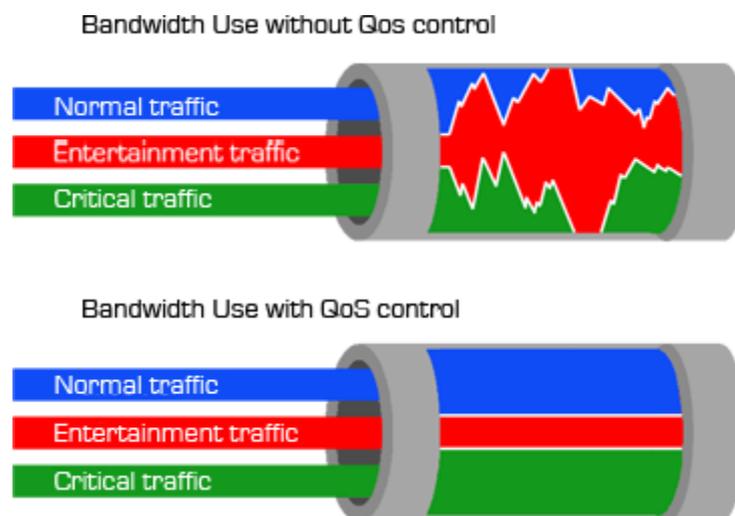
Gambar 36 : Arsitektur Intranet Jaringan Kota Magelang

#### E. QOS

OPD sudah mendapatkan layanan koneksi internet dari Diskominsta. Selain mendapat koneksi internet dari Kominfo akan tetapi hasil survey didapati keluhan terkait koneksi internet yang diberikan oleh Diskominsta masih terasa lambat. Dengan membandingkan alokasi *bandwidth* di setiap OPD dan apa yang dikeluhkan oleh pengguna, maka Diskominsta perlu melakukan jaminan kualitas jaringan internal OPD dan pengaturan penggunaan *bandwidth* jaringan internet yang biasa di buat *Quality of Service (QOS)* di *router (Edge Gateway)* Diskominsta maupun di setiap *router* OPD.

Dalam melakukan jaminan kualitas layanan jaringan, terdapat mekanisme yang disebut *Quality of Service* (QoS). QoS ini dibutuhkan karena ketersediaan *bandwidth* internet cenderung lebih kecil dibanding kebutuhan penggunaannya, sehingga harus butuh pengaturan agar semua layanan dapat diakses secara maksimal.

Jaringan Pemerintahan perlu menyediakan layanan yang dapat diprediksi dan terukur sebagai aplikasi (seperti suara, video, dan data yang sensitif terhadap keterlambatan) untuk melintasi jaringan. Pemerintah menggunakan QoS untuk memenuhi persyaratan lalu lintas dari aplikasi sensitif, seperti suara dan video real-time, dan untuk mencegah penurunan kualitas yang disebabkan oleh packet loss, penundaan dan jitter. Pemerintah dapat mencapai QoS dengan menggunakan alat dan teknik tertentu, seperti jitter buffer dan traffic shaping. Bagi banyak Pemerintah, QoS termasuk dalam service-level agreement (SLA) dengan penyedia layanan jaringan untuk menjamin tingkat kinerja tertentu.

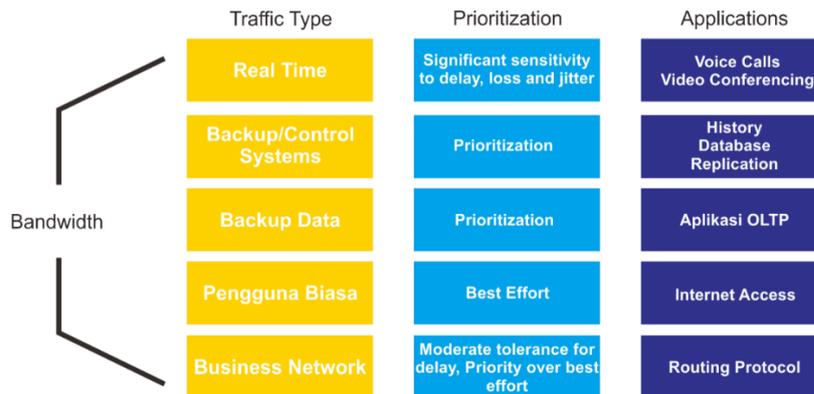


Gambar 37 : Perbandingan Penggunaan Bandwidth Sebelum dan Sesudah Dilakukan QoS

Berikut langkah-langkah yang harus dilakukan untuk menjamin kualitas penggunaan *bandwidth* jaringan internet:

1. **Klasifikasi Tipe Trafik**

Langkah ini untuk menentukan tipe trafik yang melalui jaringan internet agar dapat mengetahui layanan mana yang akan diberikan prioritas *bandwidth* tinggi dan layanan mana yang diberikan prioritas *bandwidth* rendah (*Best effort*).



Gambar 38 : Klasifikasi Trafik yang melalui jaringan

Klasifikasi tipe trafik dapat ditentukan berdasarkan network pengguna, jenis aplikasi (protokol dan nomor port) dan berdasarkan marking di layer 2 (frame) maupun layer 3 (packet).

QoS Class Names	Layer 3 QoS Markings		IPP / CoS Markings
	PHB	DSCP	
Network Control	CS6	48	6
Voice Real-Time Transport	EF	46	5
Clinical Life Critical	CS5	40	5
Multimedia Conferencing	AF41	34	4
Real-Time Interactive	CS4	32	4
Multimedia Streaming	AF31	26	3
Call Signaling	CS3	24	3
Low-Latency Data	AF21	18	2
OAM (Net Mgmt)	CS2	16	2
High-Throughput Data	AF11	10	1
Low-Priority Data	CS1	8	1
Best Effort	0	0	0

Gambar 39 : Klasifikasi Paket berdasarkan kode Marking L2 dan L3

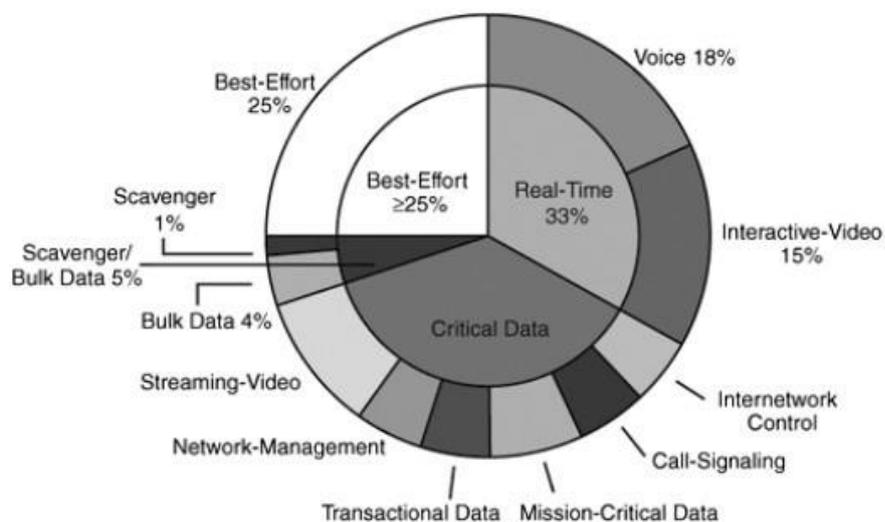
## 2. Menentukan tipe antrian (*Queue Type*)

Setelah melakukan klasifikasi tipe trafik, langkah selanjutnya adalah menentukan tipe antrian. Tipe antrian ini menentukan bagaimana paket masuk dan ditransmisikan. Ada beberapa tipe antrian yang dikenal di dalam jaringan:

- FIFO (*First In First Out*) – tipe antrian default dimana paket yang pertama masuk akan ditransmisikan pertama juga
- RED (*Random Early Detect*) – sistem *dropper* menurut rata-rata panjang antrian. RED mengendalikan trafik jaringan sehingga terhindar dari kemacetan pada saat trafik tinggi berdasarkan pemantauan perubahan nilai antrian minimum dan maksimum. Jika isi antrian dibawah nilai minimum maka mode 'drop' tidak berlaku, saat antrian mulai terisi hingga melebihi nilai maksimum maka RED akan membuang (*drop*) paket data secara acak sehingga kemacetan pada jaringan dapat dihindari. RED umumnya dipakai di *router gateway* dengan tingkat trafik yang sangat tinggi.
- PCQ (*Per Connection Queue*) – sistem antrian paket yang akan menyamakan *bandwidth* untuk masing-masing pengguna berdasarkan *IP Address*. Sistem antrian ini sangat cocok untuk penggunaan *bandwidth* dengan jumlah client yang banyak dan disamakan kecepatannya.

## 3. Membuat *Bandwidth Policy*

Langkah ini digunakan untuk menentukan kecepatan download maupun upload sesuai dengan klasifikasi trafik yang diinginkan. Penentuan kecepatan download dan upload ditentukan berdasarkan keinginan dan kepentingan pemerintahan. Gambar berikut adalah contoh menentukan persentase *bandwidth* berdasarkan klasifikasi trafik yang diinginkan.



Gambar 40 : Bandwidth Policy Berdasarkan Klasifikasi Tipe Trafik Data

### 5.3.2 Diagram Pusat Data

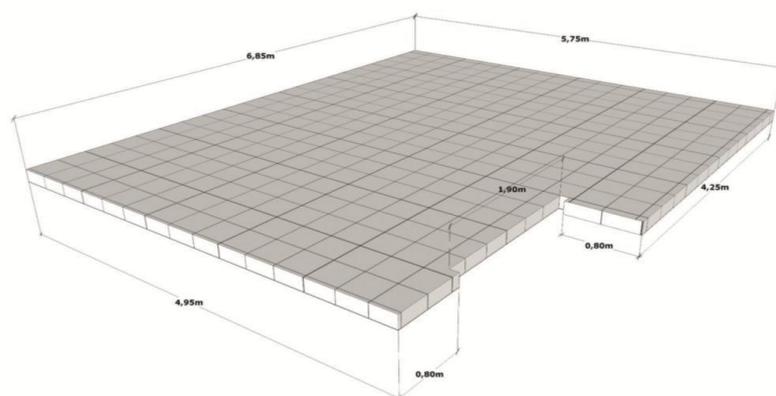
Melakukan Pembinaan terhadap pusat data (*data center*) merupakan Langkah untuk memenuhi kebutuhan di Pemerintahan Kota Magelang . Pengembangan awal pada perancangan proses data center mencakup tata letak, Manajemen kabel dan infrastruktur, tingkat keandalan, pertimbangan lingkungan serta harus memenuhi standar *availability, scalability/flexibility*, dan *security*. Sudah dilakukan oleh Kota Magelang .

Saat ini di Pemerintah Kota Magelang tingkat kebutuhan data/informasi dirasakan cukup tinggi dan tingginya nilai data/informasi menyiratkan agar data/informasi tersebut harus dapat terdokumentasi dan tersimpan dalam suatu sistem yang handal, terjamin keamanannya, dan dikondisikan untuk selalu online selama 24 jam 7 hari.

Untuk itu, mulai dari hal-hal teknis menyangkut pengaturan catu daya, pengatur udara, pencegah bahaya kebakaran, sistem pengamanan fisik dan struktur ruangan pun harus dibangun untuk memenuhi kebutuhan tersebut.

### F. Desain Lantai Ruang Data Center

Khusus untuk ruangan server atau ruang penyimpanan data dengan luas ruangan sekitar 40 meter persegi dibuat menggunakan raised floor, sebagai media akses bagi jaringan kabel data atau “Networking Cable Data” dan difungsikan sebagai media akses precision cooling, untuk desainnya bisa dilihat seperti pada gambar dibawah ini.



Gambar 41 : Lantai Ruang Server Menggunakan Raised Floor



Gambar 42 : Deretan Server Dengan Menggunakan Raised Floor



Gambar 43 : Ruang Untuk Administrator Data Center

Implementasi dari Data center yang sudah dibuat ini merupakan salah satu upaya yang ditempuh oleh Dinas Komunikasi dan Informatika Kota Magelang , yang dalam hal ini bertanggung jawab dalam Pengembangan TIK dan Integrasi Infrastruktur pada Pemerintah Kota Magelang dapat digunakan untuk menjamin kontinuitas pelayanan terhadap OPD di Kota Magelang .

### G. Kelistrikan

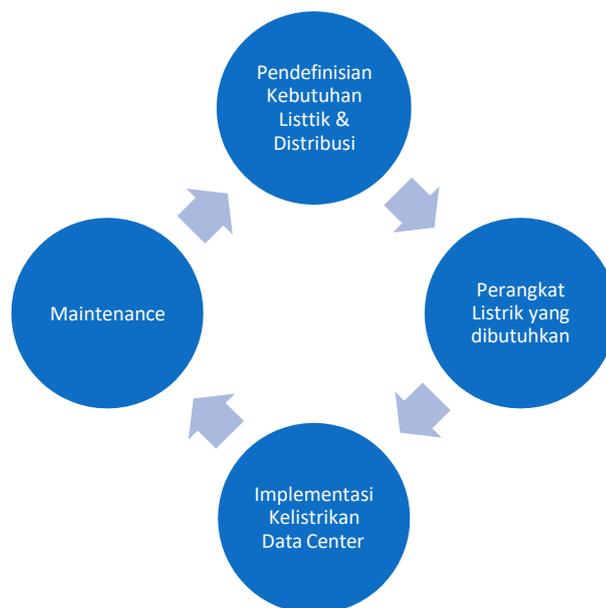
Kebutuhan energi sebuah pusat data didapat dari sistem listrik yang dalam hal ini disediakan oleh PLN. Kebutuhan akan listrik pun akan terus bertambah seiring bertambahnya energi yang dibutuhkan oleh pusat data. Ada 4 pertimbangan umum yang

dapat diterapkan untuk mengatasi masalah kebutuhan energi yang terus bertambah pada pusat data, yaitu:

- a. Membuat sistem energi (sistem energi dapat berupa sistem listrik, sistem pembangkit energi lainnya) yang modular sehingga dapat dengan mudah beradaptasi dengan pertumbuhan atau perubahan kebutuhan energi.
- b. Pre-engineered, terapkan solusi identifikasi energi yang standar sehingga meminimalkan perencanaan dan perekayasaan yang akan dilakukan sendiri guna mempercepat pembangunan dan pengimplementasian pada pusat data.
- c. Memilih sistem energi dengan fitur mistake-proofing dan sedikit titik kegagalan yang dapat meningkatkan availabilitas.
- d. Menerapkan sistem manajemen energi yang menyediakan visibilitas dan pengontrolan energi pada berbagai level.

Sistem listrik untuk sebuah pusat data merupakan sumber energi utama sampai saat ini (baik untuk operasional utama dan back-up). Oleh karenanya perancangan sistem listrik harus *se-robust* mungkin untuk dapat memenuhi kebutuhan listrik pusat data dan ketika sewaktu-waktu dapat terjadi gangguan listrik yang telah atau tidak diprediksi sebelumnya, hal tersebut perlu diantisipasi. Pada bagian selanjutnya akan diberikan tabel guideline penyusunan sistem listrik yang ideal untuk pusat data.

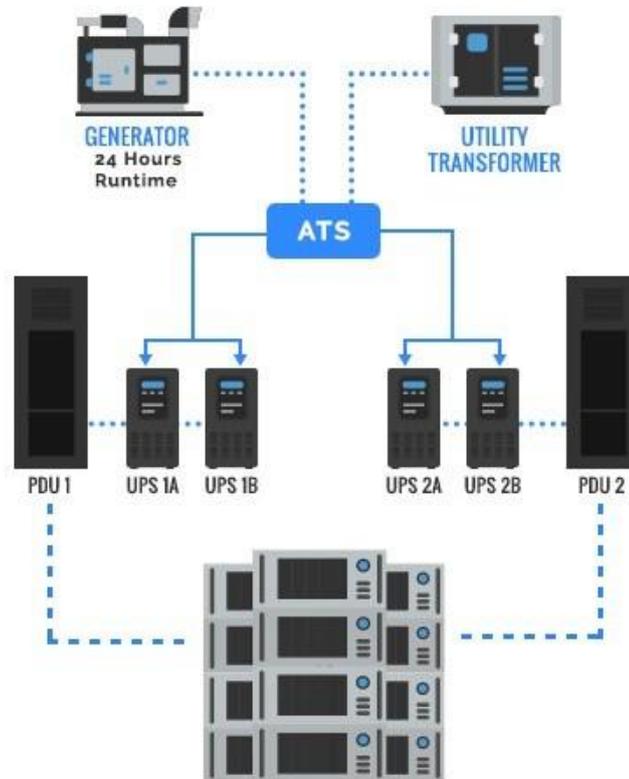
Tujuan dari pembuatan sistem energi yang menggunakan modular, sesuai dengan standar, *hot swappable*, dan terbukti handal dapat mengurangi MTTR (*Mean Time to Recover*). Bagian awal perencanaan komponen listrik adalah pendefinisian kebutuhan energi listrik dan pendistribusiannya. Kebutuhan energi listrik dihitung untuk setiap ruangan yang berbeda-beda (biasanya dikategorikan berdasarkan fungsionalitas ruangan). Misalkan pada ruangan server, dihitung jumlah lokasi kabinet server di ruangan tersebut kemudian menghitung sumber energi maksimum yang dibutuhkan agar keseluruhan server tersebut dapat beroperasi (apabila server tersebut hidup semua dalam keadaan normal).



Gambar 44 : Perencanaan Sistem Listrik Data Center

Untuk lebih akurat maka dapat dilakukan perhitungan untuk penambahan kebutuhan listrik untuk mengatasi keadaan kritikal atau saat terjadi penambahan server. Selain server, maka kebutuhan energi lain yang akan dilihat adalah perangkat jaringan, air handler, overhead light, badge access reader, dan perangkat yang membutuhkan energi listrik untuk beroperasi. Setelah jelas berapa energi listrik keseluruhan yang diperlukan, maka langkah selanjutnya adalah merancang pendistribusian energi listrik ke seluruh perangkat. Ada dua cara untuk mendistribusikan energi listrik dalam ruang pusat data, yaitu:

1. Distribusi secara langsung dari PDU ke setiap lokasi kabinet, dipandang lebih fleksibel melalui saluran kabel yang tersedia karena tidak melalui perantara apapun. Namun untuk pusat data yang berkapasitas besar hal ini tidak mungkin dilakukan karena akan tidak efisien dari segi pengkabelan.
2. Distribusi melalui panel circuit, dari PDU akan menuju ke panel circuit kemudian dari tempat tersebut akan didistribusikan ke masing-masing lokasi kabinet. Jauh lebih efisien dari segi pengkabelan karena untuk jarak yang jauh antara lokasi kabinet server dengan PDU, hanya membutuhkan satu kabel yang panjang, baru kemudian dari panel sirkuit disalurkan ke masing-masing kabinet server dengan kabel yang berjarak pendek.



Gambar 45 : Distribusi Kebutuhan Listrik dari PDU melalui circuit panel

Untuk mencapai tingkat reliabilitas yang tinggi maka saluran listrik ke lokasi kabinet server dijalankan dari sumber yang berbeda sehingga perubahan terhadap komponen-komponen listrik, pengkabelan, dan alternatif terminasi didasarkan pada kebutuhan energi secara lokal, tegangan yang biasa dipakai berapa, namun tetap perhatikan desain yang baik untuk sistem listrik keseluruhan (kolaborasi dari modul modul listrik yang ada). Kemudian perhatikan juga mengenai redundancy kebutuhan energi didalam ruangan, misalnya setiap kabinet server akan memiliki dua power strip dan akan ada power input yang berbeda juga di setiap server. Pendefinisian kebutuhan listrik juga memasukkan perkiraan tambahan kebutuhan di masa mendatang.

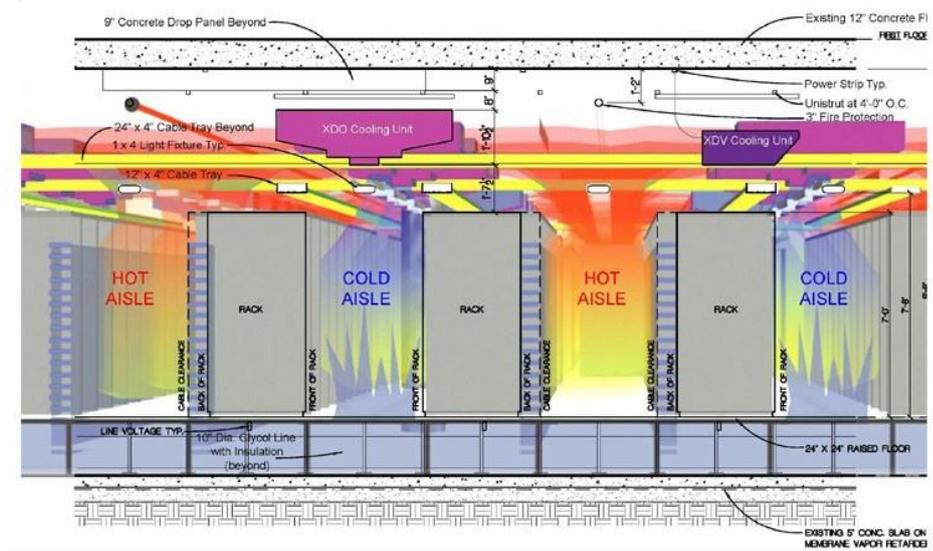
#### H. Pendinginan

Sistem pendingin pada pusat data dibuat untuk menjaga kestabilan temperatur yang cocok untuk pusat data. Keadaan temperatur dan kelembaban yang harus dijaga di dalam pusat data:

- a. Temperatur kering: 20°C -25°C (68°F-77°F), dengan rata-rata keadaan temperatur normal di set menjadi 22°C±1°C.

- b. Kelembaban relatif: 40%-50%, dengan titik normal berada pada 45%±5%.
- c. Titik embun maksimum: 21°C (69.8°F)
- d. Perubahan maksimum yang boleh terjadi dari batas suhu sekarang adalah sebesar 5°C(9°F) per jam.

Desain sistem pendingin harus terencana dengan baik agar aliran udara dari perangkat pendingin mengalir dengan arah paralel ke barisan kabinet/rak.



Gambar 46 : Aliran Distribusi Udara

Kriteria umum desain sistem pendingin pada pusat data yang harus dipenuhi, adalah:

- a. Memiliki skalabilitas dan adaptabilitas yang sangat baik
- b. Sudah terstandarisasi
- c. Sederhana namun cerdas
- d. Manajemen yang baik

Kegiatan pengaturan temperatur dan sirkulasi udara yang dikenal sebagai HVAC (heating, ventilation, air conditioning), bertujuan untuk menjaga agar temperatur tetap dalam keadaan rendah dan konstan serta menyebarkan titik-titik panas yang dibuat oleh suatu kelompok perangkat yang dalam hal ini terletak di pusat data. Temperatur yang rendah sangat diperlukan untuk efisiensi operasi server dan perangkat jaringan untuk menghindarkan dari fluktuasi. Sistem pendingin pada pusat data pada prinsipnya adalah sistem aliran udara dingin, yang terbagi menjadi tiga perangkat utama yaitu air handler, chiller, dan menara pendingin. Selain itu, juga ada perangkat pendingin tambahan.



Gambar 47 : Koridor Panas

Kebutuhan utama dari desain sistem pendingin dari pusat data, antara lain:

### 1. Kebutuhan sistem pendingin

Terkait dengan redundansi untuk perangkat pendingin, redundansi yang dapat dilakukan terkait dengan sistem pendingin adalah memasang lebih dari satu air handler, kemudian juga sediakan menara pendingin tambahan untuk setiap chiller. Selain itu, persediaan air yang dibutuhkan untuk menciptakan udara dingin harus diamankan secara ekstra antara lain dengan membangun kontainer penyimpan air dan lakukan konfigurasi infrastruktur pendingin dan fire suppression.

### 2. Tekanan Udara

Tekanan udara pada pusat data harus dijaga pada level tertentu yang disebut sebagai tekanan statis. DC didesain untuk memiliki tekanan antara 0.2-0.5 in. wc. Untuk menjaga agar tekanan udara tetap stabil maka periksa seluruh ruangan apakah telah tertutup dengan baik dan yakin bahwa tidak ada lubang sedikit pun. Jangan letakkan perforated tile dekat-dekat dengan DC air handler, karena kebanyakan handler membutuhkan buffer sekitar 36-42 in (91.4-106.7 cm).

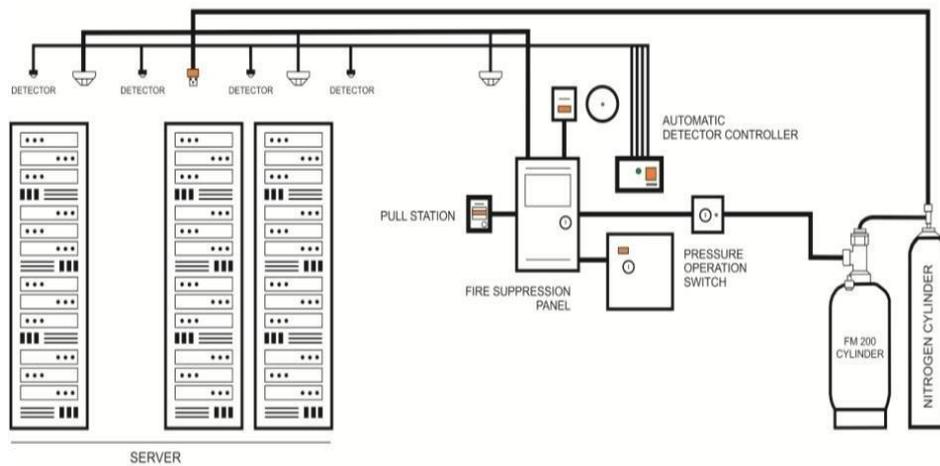
### 3. Kelembaban

Kelembaban sendiri merupakan konsentrasi uap air di udara, yang penting untuk dijaga terkait dengan sistem HVAC pusat data adalah Kelembaban relatif dalam ruangan pusat data. Kelembaban relatif adalah persentase perbandingan dari jumlah uap air yang ada di udara dengan jumlah uap air di udara kering. Perangkat server dan jaringan dapat berfungsi pada rentang level Kelembaban yang cukup panjang yaitu sekitar 20%-80%. Menjaga Kelembaban relatif dalam keadaan normal berfungsi untuk mencegah terjadinya karatan pada beberapa perangkat di pusat data karena penguapan (Kelembaban tinggi) atau mencegah munculnya elektrostatik pada beberapa perangkat metal (Kelembaban yang rendah). Cara yang dilakukan adalah melengkapi AH dengan kemampuan humidification atau melalui penggunaan unit-unit humidification yang terpisah dari AH. Kelembaban relatif yang memungkinkan untuk suatu ruangan pusat data adalah sekitar 45%-55%, yaitu level Kelembaban relatif normal sebesar 50% dengan tingkat sensitivitas sekitar 10%, yang memungkinkan variasi pada level kelembaban sehingga komponen infrastruktur tidak konstan berada level tersebut.

#### I. Fire Suppression System

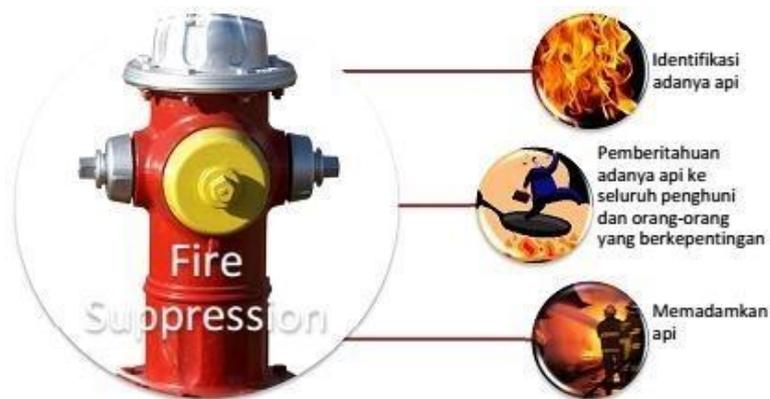
Data center yang bekerja secara maksimal selama hampir 24 jam setiap hari, memiliki potensi terjadinya kebakaran. Peralatan server yang bekerja terus menerus di wilayah yang suhu udaranya tinggi, terlebih lagi minim perawatan, akan membuat temperatur peralatan menjadi sangat tinggi.

system fire suppression memang didesain untuk mencegah, dan atau memadamkan terjadinya kebakaran secara otomatis, untuk gambaran umum instalasi fire suppression bisa dilihat pada gambar dibawah:



Gambar 48 : Instalasi Fire Suppression Untuk Data Center

Solusi perlindungan data center dari api mempunyai tiga tujuan utama, yaitu:



Gambar 49 : Solusi Fire Fighting System

Secara umum, sistem fire suppression terdiri atas elemen-elemen sebagai berikut:

- Deteksi panas yang linier (kabel sensor panas), ditempatkan sepanjang tray wire dan jalur elektrik baik diatas maupun dibawah raised-floor. Alarm pada sensor dibunyikan pada sistem kontrol bukan untuk memicu bekerjanya sistem fire suppression
- Deteksi tipe spot secara intelligent
- Deteksi asap
- Portabel fire extinguisher

- Agen pembersih sistem fire suppression
- Pull station, perangkat sinyal, dan sistem control

Dari lima kelas handheld extinguisher, yang paling tepat untuk dipasang pada pusat data adalah handheld extinguisher tipe C (untuk kebakaran yang diakibatkan oleh sistem listrik). Material CO2 dan halogenated adalah material suppression yang dipilih karena meninggalkan sedikit sisa ketika sudah tidak digunakan lagi. Komponen minimum fire suppression yang harus digunakan pada pusat data sederhana sekalipun adalah sebuah sistem sprinkler biasa (yang bertindak sebagai pre-action sprinkler) dengan clean-agent fire extinguishers yang cocok. Kemudian meningkat pada level yang lebih tinggi, maka sistem fire suppression yang lebih canggih akan meliputi air sampling smoke detection systems, pre-action sprinkler systems, dan clean agent suppression systems.

Sistem peringatan proteksi dini sangat penting untuk menghindari kerusakan dan kehilangan yang dapat terjadi selama status kebakaran belum benar benar terjadi (atau awal terjadinya kebakaran), karena kerusakan peralatan yang signifikan dapat semata-mata terjadi karena asap atau pembakaran produk-produk lain terhadap peralatan elektronik. Contoh sebuah sistem peringatan proteksi dini adalah air sampling smoke detection systems yang menyediakan proteksi level lain untuk ruang komputer dan fasilitas-fasilitas pintu masuk terkait, ruang mekanik, dan ruang listrik. Sistem itu juga disediakan sebagai pengganti smoke detectors biasa, karena kesensitifannya dan kapabilitas deteksinya jauh melampaui detektor konvensional.

Penempatan perangkat pada pusat data akan mempengaruhi aliran udara yang terjadi pada pusat data, kemudian perancangannya akan terkait dengan layout ruangan yang sudah ditetapkan, susunan kabinet, dan perangkat dingin apa saja yang ada. Pengaturan layout ruangan dan penempatan berbagai perangkat di pusat data dapat mengoptimalkan fungsi sistem pendingin pada pusat data bahkan hingga tipe lantai yang digunakan ataupun tipe kabinet yang akan dikembangkan. Kunci utama untuk mengurangi panas adalah menyebarkan udara di sekitar ruangan.

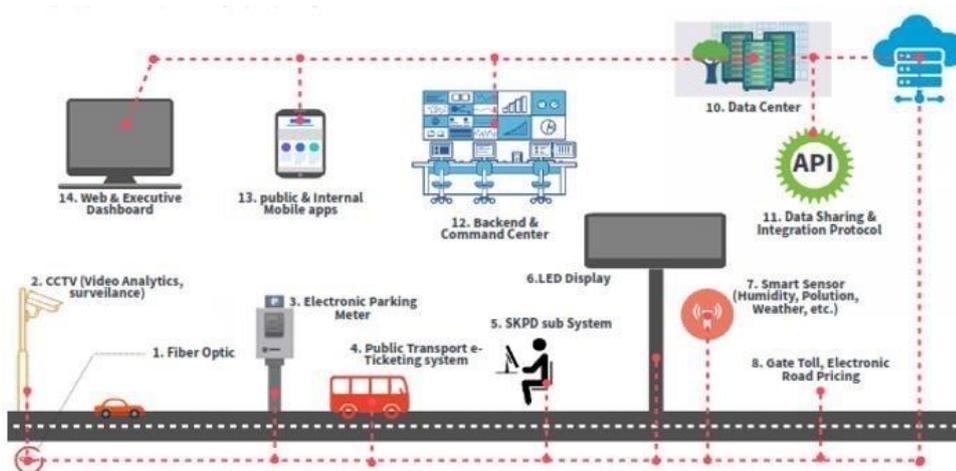
Hot spot merupakan hal yang harus dihilangkan pada pusat data agar aliran udara dingin tersebar merata di seluruh ruangan pusat data. Oleh karenanya, harus didesain dengan sumber panas yang terjadi di lokasi-lokasi yang telah diprediksi, sehingga proses

pendinginan dapat langsung diarahkan ke titik tersebut. Hal ini disebut sebagai hot and cold aisle. Untuk menciptakannya, dilakukan langkah sebagai berikut:

- Letakkan barisan server berurutan dengan arah berhadap-hadapan (back of server dan front of server).
- Pasang perforated floor tile di depan setiap lokasi kabinet server.
- Pasang saluran pada atap yang dimulai dengan pemasangan lubang angin diatas aisle di belakang setiap barisan server dan menghubungkan kembali ke lubang air handler.

## J. Control Room & Command Center

Command Center merupakan fasilitas yang diperlukan oleh institusi dalam menjalankan *Crisis Management* atau *Business Continuity Management*. Command Center adalah sebuah lokasi yang lengkap dengan infrastruktur yang diperlukan, dimana seorang pimpinan bersama dengan tim melakukan rapat, mengambil keputusan, menugaskan, mengkoordinasi, memonitor dan mengontrol seluruh tindakan yang diperlukan sebagai respon terhadap suatu hal yang dihadapi, meliputi : tindakan tanggap darurat, *action plan* untuk perbaikan dan pemulihan, langkah pengadaan, dan langkah penyediaan informasi publik.



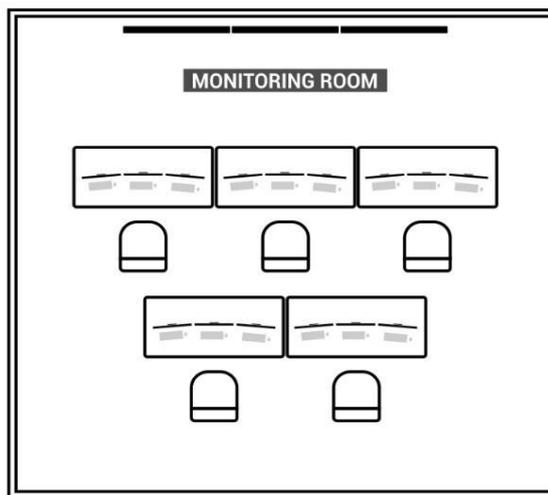
Gambar 50 : Fungsi Command and Center

Dibangunnya command center bertujuan untuk :

1. *Data center management*, mengatur manajemen pusat dan pengendalian operasi untuk sistem komputer yang biasanya berbentuk pusat data.

2. *Business application management* , memantau dan menampilkan data dan aplikasi yang sangat penting bagi pemerintah daerah untuk keperluan pengambilan keputusan
3. *Civil management*, mengatur manajemen pusat dan pengendalian fungsi fungsi operasi sipil. Para staf selalu memonitor lingkungan di Kota Magelang agar dapat menjamin keamanan masyarakat.
4. *Emergency (crisis) management*, pusat komando untuk menangani dan mengendalikan kejadian untuk mencegah suatu krisis/kondisi darurat serta meminimumkan berbagai dampak dari suatu kejadian.

Display command center terbagi atas 3 layer utama yaitu :



Gambar 51 : Display Command Center

1. Wall Space : display utama yang menyajikan seluruh pantauan aktivitas dan komunikasi secara realtime
2. PC Desktop/Laptop : tempat pengoperasian dan pengaturan lalu lintas data dan informasi dan pesan sehingga mudah di akses dan disebarkan dengan efektif dan efisien
3. Tablets/smartphone : mobile device yang dibutuhkan setiap pengambil keputusan terkait command center tersebut

Network Operation Center (NOC) Adalah tempat administrator yang mengawasi, memantau dan mengamankan jaringan komunikasi. Berupa sebuah ruangan yang berisi visualisasi dari jaringan atau jaringan yang sedang dipantau, workstation di mana status rinci jaringan dapat dilihat, dan perangkat lunak yang diperlukan untuk mengelola jaringan.

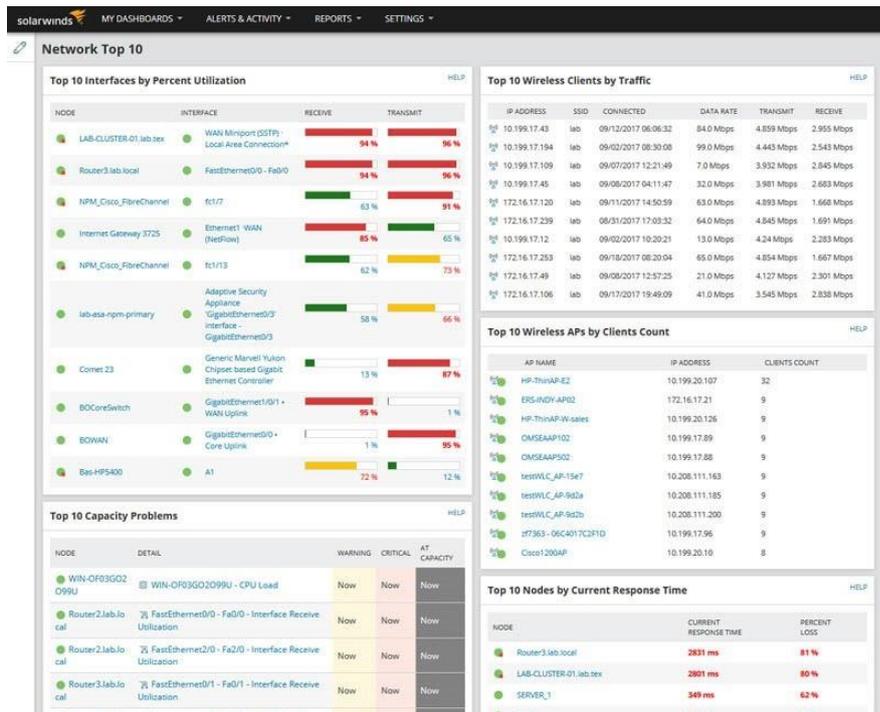


Gambar 52 : Control Room Data Center

Dengan adanya NOC, NOC memberikan kemudahan kepada user dalam melakukan aktivitas koordinasi operasi dengan semua pendukung dan vendor terkait dengan fungsi network. Kegiatan pada NOC adalah memberikan support selama 24 jam dengan aktivitas sebagai berikut:

1. Memonitor operasi semua hubungan backbone dan pendukung jaringan lainnya.
2. Menjamin bahwa server dan pelayanan bekerja secara terus menerus selama 24 jam.
3. Memberi jaminan untuk mendukung kualitas layanan jaringan kepada pengguna.
4. Perbaiki semua masalah jaringan dan sistem terkait.
5. Membuka pelacakan dan resolusi dokumentasi permasalahan pada sistem jaringan.

NOC merupakan perangkat infrastruktur yang melakukan fungsi-fungsi pengaturan, pengendalian, dan pengawasan jaringan (network) sedemikian rupa sehingga dapat berfungsi sesuai dengan standar pelayanan yang diberikan. Berikut merupakan gambaran monitoring system yang ada di NOC.



Gambar 53 : Contoh Hasil Monitoring Jaringan



Gambar 54 : Contoh Monitoring Server dan Aplikasi

Hal-hal yang memerlukan monitoring antara lain:

#### **1. IT + Automation + Security**

Menyediakan pemantauan menyeluruh dan manajemen insiden untuk peralatan industri, infrastruktur jaringan, dan sistem keamanan fisik pusat data Anda dengan menggunakan solusi payung yang solid. Singkirkan banyak sistem dan banyak titik integrasi di antara merek, Menyediakan pemantauan menyeluruh dan manajemen insiden untuk peralatan industri, infrastruktur jaringan, dan sistem keamanan fisik pusat data Anda dengan menggunakan solusi payung yang solid. Singkirkan banyak sistem dan banyak titik integrasi di antara merek

#### **2. Data Center Environment Monitoring**

Pantau suhu, kelembaban, tekanan udara panas / dingin, aliran udara, emisi karbon dioksida secara keseluruhan. Deteksi kebocoran, asap dan banjir. Menyediakan tampilan lingkungan per rak, pemetaan aliran udara khusus, KPI lingkungan keseluruhan, dasbor lingkungan, dan banyak lagi. Manfaatkan garis dasar dinamis dan peringatan pelanggaran ambang batas.

#### **3. Genset Monitoring**

Terhubung ke generator melalui protokol otomasi apa pun, bukan hanya SNMP. Menyediakan penyimpanan, visualisasi, peringatan, dan pelaporan untuk level bahan bakar, tekanan oli, suhu air dan oli, status baterai internal, detail keluaran daya, alarm, kesalahan, dan status perawatan.

#### **4. Energy Performance Analysis**

Buat model KPI daya pusat data secara keseluruhan dan analisis efisiensi energi. Secara otomatis mengevaluasi KPI gabungan untuk beberapa pusat data dalam penginstalan terdistribusi. Hasilnya, manfaatkan tren dan laporan Power Usage Effectiveness (PUE).

#### **5. Video Monitoring**

Integrasikan dengan sistem Pengawasan Video dan tambahkan aliran video kamera dan kontrol PTZ ke dasbor ruang kontrol. Manfaatkan konektivitas kamera IP

langsung, buka sembulan video dari denah lantai. Integrasikan dengan sistem analisis video dan gunakan sebagai satu lagi sumber insiden keamanan

#### **6. Traffic Monitoring**

Memfasilitasi pemecahan masalah bandwidth, verifikasi SLA dan perencanaan kapasitas. Lihat grafik historis dan laporan untuk lalu lintas / bandwidth. Gunakan analisis lalu lintas jaringan dan telusuri informasi terperinci tentang dekomposisi lalu lintas (NetFlow, sFlow). Gunakan pembuat tampilan lalu lintas jaringan visual, yang memberi tahu saat pembicaraan jaringan yang cocok dengan kriteria tertentu terdeteksi, dan banyak lagi.

#### **7. Storage Monitoring**

Temukan dan pantau array RAID, perpustakaan pita, HBA, dan perangkat penyimpanan jaringan lainnya. Kelola kesehatan perangkat penyimpanan, pengoperasian, kesalahan, kapasitas, dan kinerja. Perkirakan pertumbuhan penggunaan melalui analisis trend.

#### **8. Alerting And Event Processing**

Kemampuan manajemen acara yang fleksibel, termasuk pemfilteran, agregasi, deduplikasi, masking, korelasi, pengakuan, dan analisis akar penyebab. Peringatan yang dapat disesuaikan mendukung berbagai jenis pemberitahuan (suara, pesan popup, email, SMS, dll.). Dukungan untuk lansiran dan eskalasi yang tertunda. Binding peringatan-untuk-tindakan memastikan berbagai jenis remediasi saat peringatan dimunculkan.

#### **9. Monitoring Server dan Aplikasi**

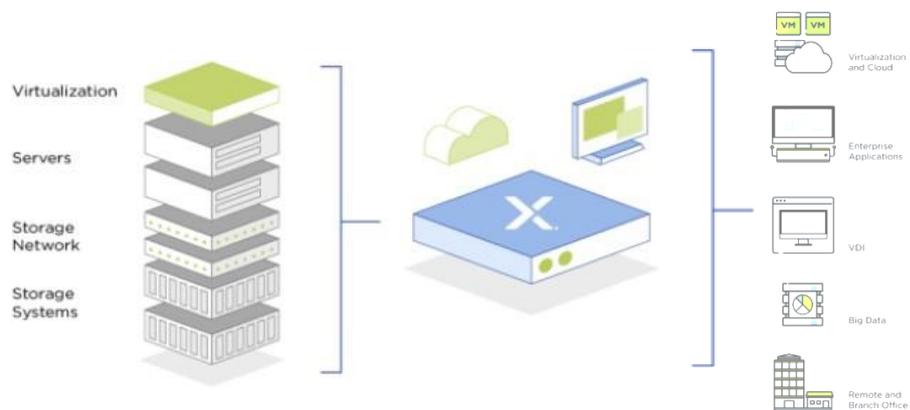
Melakukan monitoring terhadap server (kinerja) dan aplikasi yang berjalan di dalam server tersebut. Menggunakan aplikasi yang ditentukan port nya untuk mengakses resource di dalam server baik yang berada di dalam *cloud* atau *on premise*.

### 5.3.3 Diagram Server dan Storage

#### K. Host

##### 1. Hyper Converged Infrastructure (HCI) Server

Hyper-converged infrastructure (HCI) merupakan infrastruktur IT yang didefinisikan sebagai software yang memvirtualisasi semua elemen sistem hardware konvensional. HCI tersebut mencakup virtualized computing (hypervisor), virtualized SAN (software-defined storage) dan virtualized networking (software-defined networking).



Gambar 55 : Hyper Converged Infrastructure (HCI) Server Concept

Dengan menggunakan HCI, Pemerintah Kota Magelang dapat dengan mudah menghadapi sejumlah data center menjadi *single appliance*.

##### 2. Flexibility and scale

Karena hyperconvergence didasarkan pada software, dapat memberikan tingkat fleksibilitas dan kelincahan untuk pemerintahan ketika dibandingkan dengan legacy infrastructure. Selain itu untuk ekspansi kapasitas dan pengembangan data center dapat jauh lebih mudah dan simple jika dibandingkan dengan legacy infrastructure.

##### 3. Workload consolidation

Sistem hyper-converged menyatukan core storage, jaringan dan fungsi komputasi menjadi satu solusi yang sangat ter virtualisasi.

##### 4. Data protection

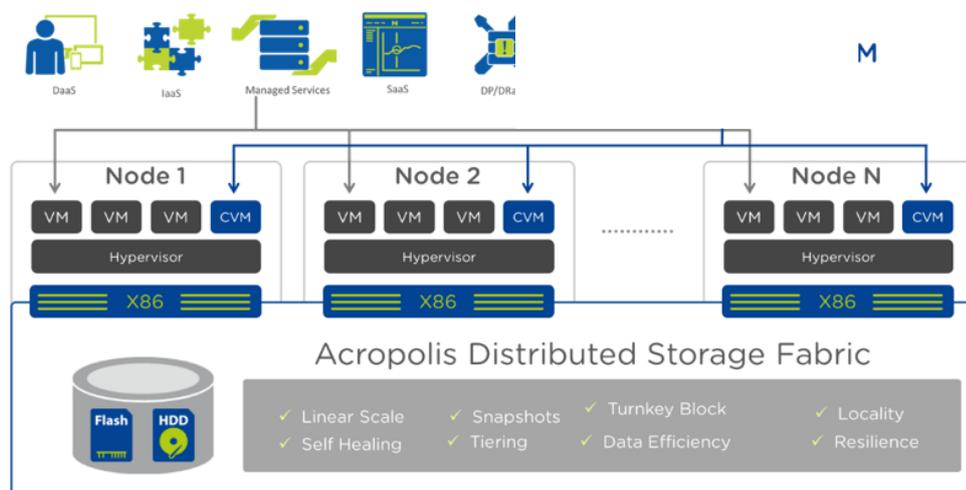
HCI juga bermanfaat dalam hal efisiensi dan penyimpanan data. Snapshotting, data deduplication dan fitur perlindungan data lainnya yang sering dibangun, membuat upaya pemulihan dari bencana menjadi jauh lebih mudah.

5. Software-defined  
Pemerintahan Daerah dapat menggunakan penyimpanan public cloud sebagai target untuk melakukan backups.
6. Automated Infrastructure  
Banyak legacy IT infrastructure yang sangat bervariasi dan rumit sehingga otomatisasi tidak mungkin dilakukan. Namun HCI dapat digunakan pada prinsip software-defined data centre (SDDC), dimana segala sesuatu termasuk storage, servers dan supporting services yang di virtualisasi.

## L. High Availability & Fault Tolerant

### 1. Redundance Hypervisor (Cluster Availability)

*Cluster High Availability* (HA) memungkinkan Pemerintahan menyediakan ketersediaan layanan untuk aplikasi apa pun yang berjalan di mesin virtual. Dengan menggunakan



Gambar 56 : Arsitektur Cluster HA pada Hyperconverged

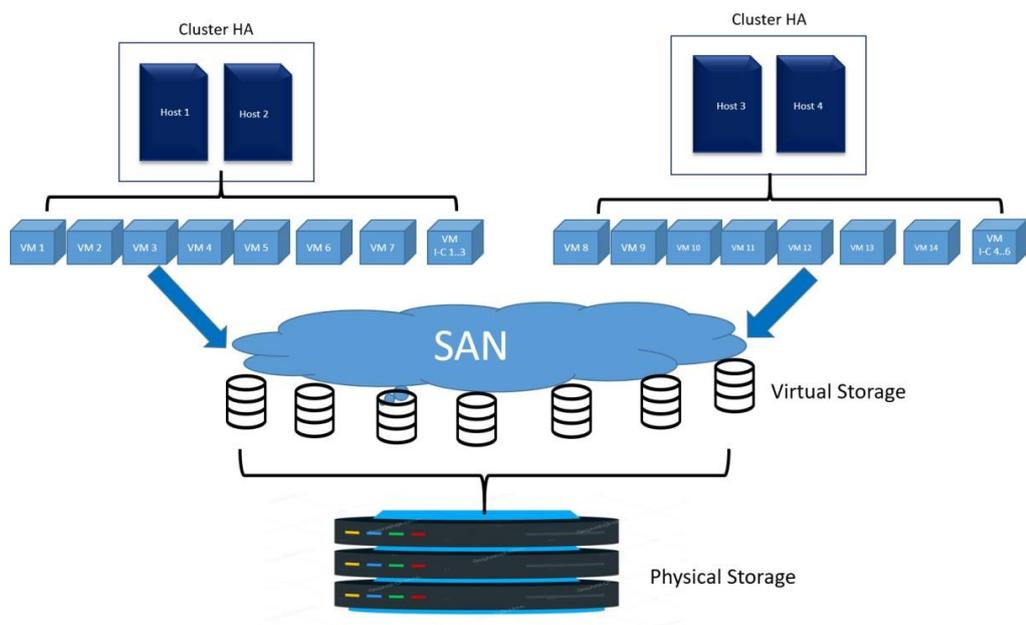
### 2. Redundance Storage Server

Arsitektur *storage* dan *Server* memberikan gambaran tentang kebutuhan dan implementasi *software defined data center* atau virtualisasi *Server*. Teknologi virtualisasi memberikan kemudahan dalam pengelolaan dan pemeliharaan layanan *Server*.

Dibutuhkan minimal 4 (empat) *host Server* yang dijadikan 2 (dua) cluster HA (*High Availability*), dengan masing-masing cluster berisi 2 (dua) *host Server*. Dalam hal

teknologi penyimpanan, membutuhkan *SAN Storage* untuk menyuplai *storage Server host* dengan 2 (dua) cluster di atasnya. Layanan *Server* diberikan dalam bentuk *virtual machine (VM)*.

Arsitektur *storage* dan *Server* ditunjukkan oleh gambar 6. Arsitektur *storage* dan *Server* ini diharapkan mampu memberikan tingkat keandalan dan ketersediaan yang tinggi terhadap *Server* dan penyimpanan data di pemerintahan Kota Magelang .



Gambar 57 : Arsitektur Storage dan Server

Beberapa target layanan yang dapat difasilitasi adalah:

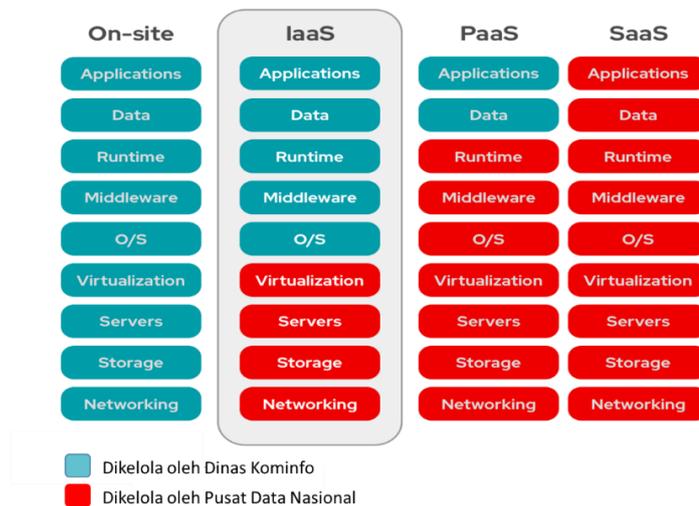
- Hosting *Web* – menyediakan standar CMS berbasis *web* yang digunakan untuk membuat *website* OPD dengan nama subdomain di bawah *kotamagelang.go.id*
- Hosting Aplikasi – menyediakan standar *Platform as a Service (PaaS)* yang menyediakan platform aplikasi dengan platform *web* dan *database mysql*
- Hosting *Data Warehouse* - menyediakan solusi PaaS untuk *data mining, query* dan pelaporan dengan data historis dari data transaksional.
- Layanan *Server File* – menyediakan solusi penyimpanan online terpusat, yang aman dan terkelola dengan baik. Layanan ini menyediakan penyimpanan virtual dengan kapasitas tertentu untuk data-data file tertentu dari masing-masing OPD dengan berbagai perlindungan seperti antivirus dan *backup* harian secara otomatis

- e. Layanan *Operational Recovery* – menyediakan kapasitas penyimpanan untuk *backup* data yang digunakan secara *point-in-time* dan mampu memulihkan sistem jika terjadi kegagalan dan kehilangan data.
- f. Arsip Data – Untuk memenuhi kebutuhan terhadap modul dan database

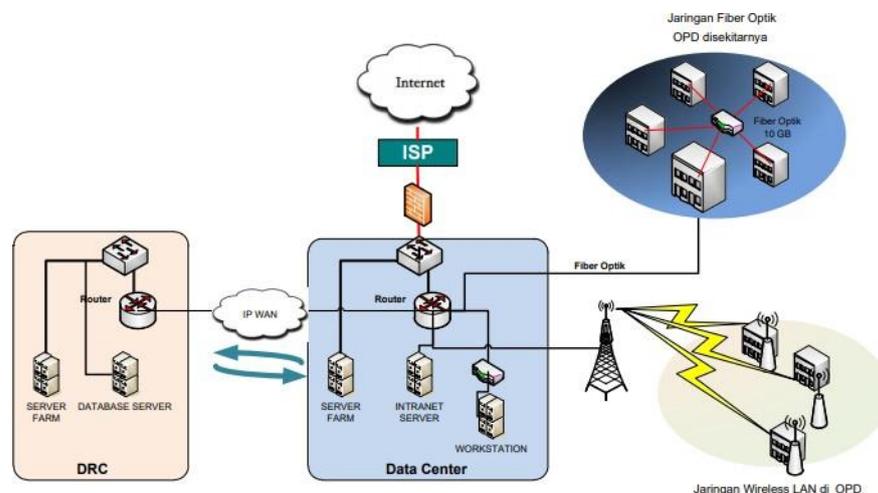
**3. Disaster Recovery Center (Pusat Data Nasional/ DRC Provinsi Jateng)**

DRC (*Disaster Recovery Center*) adalah sebuah tempat yang mana ditujukan untuk menempatkan perangkat IT, sistem, aplikasi dan data cadangan untuk bisa menghadapi bencana yang diperlukan oleh pemerintahan. Bencana yang serius ini tidak hanya bisa menimpa satu unit kerja saja namun bisa beberapa unit. Unit yang sering terserang adalah penyimpanan data dan juga pengolahan data maupun informasi.

Terkait dengan regulasi dari Pusat terkait Pusat Data, maka Kota Magelang menggunakan Pusat Data Nasional untuk meletakkan aplikasi dan database yang diperlukan dalam arsitektur aplikasi. Pusat Data Nasional merupakan sebuah cloud, dengan model IaaS, PaaS dan SaaS. Layanan yang digunakan oleh Kota Magelang adalah IaaS (*Infrastructure as a Service*) dan PaaS (*Platform as a Service*). Dan bentuk layanan yang diberikan di pusat data nasional dan DRC Provinsi Jawa tengah adalah seperti digambarkan sebagai berikut:



Gambar 58 : Layanan Cloud Pusat Data Nasional dan Diskominsta



Gambar 59 : Replikasi layanan di DRC

Berdasarkan cara kerjanya, DRC memiliki beberapa jenis, antara lain:

a. *Cold DRC*

Menyediakan sistem yang sama seperti di lokasi data center di Pemerintah dimana aplikasi dan data akan diupload sebelum fasilitas drc bisa digunakan, namun proses pemindahan dari data center ke lokasi DRC akan dilakukan secara manual.

b. *Warm DRC*

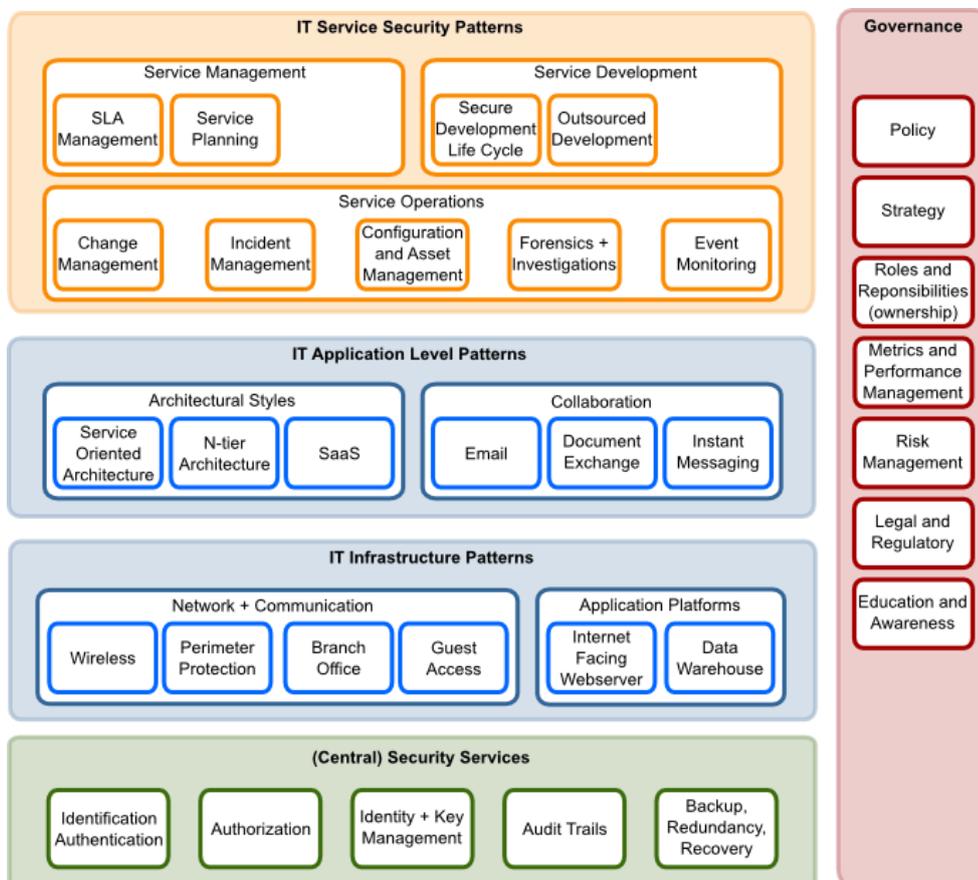
Menyediakan komputer dengan segala komponennya, aplikasi, link komunikasi, dan backup data yang paling update, dimana system tidak otomatis berpindah tetapi masih terdapat proses manual meskipun dilakukan seminimal mungkin.

c. *Hot DRC*

Mengatur secepat mungkin operasional pemerintahan, system dengan aplikasi, link komunikasi yang sama sudah dipasang dan sudah tersedia di lokasi DRC, data secara terus menerus di-backup menggunakan koneksi live antara data center dan lokasi DRC, dan operasional pemerintahan akan berjalan pada saat itu juga, tanpa harus mematikan sistem di data center lama.

## 5.4 Arsitektur Keamanan

Untuk membantu Pemerintahan Kota Magelang agar memiliki suatu sistem keamanan informasi yang sesuai dengan standar ISO/IEC 27001 sehingga berbagai risiko penggunaan TI untuk menunjang kegiatan Pemerintahan Kota Magelang bisa diminimalisir, maka disusunlah Arsitektur Keamanan Informasi ini demi menjaga kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) dari data/informasi Pemerintahan Kota Magelang .



Gambar 60 : Arsitektur Keamanan

Tata kelola keamanan (*security governance*) yang dilakukan meliputi :

- Pembuatan peraturan keamanan TI;
- Strategi keamanan;
- SOP keamanan TI;
- Manajemen kinerja keamanan;
- Manajemen risiko keamanan;
- Kepatuhan terhadap aturan dan undang-undang yang berlaku (UU ITE); dan

- Peningkatan edukasi dan *awareness* terhadap pengguna.

Arsitektur *Security* menjelaskan 3 domain atau wilayah keamanan TI, meliputi:

1. *IT Service Security Patterns*

*IT Service Security Patterns* merupakan keamanan di wilayah layanan TI (*IT Service*).

Jaminan keamanan harus sudah dilakukan pada saat fase awal pengembangan sistem (*development*) baik pengembangan yang dilakukan oleh internal maupun pengembangan di pihak ketiga (*outsourcing*).

Jaminan keamanan juga dilakukan pada fase operasional yang meliputi :

- *Change Management*;
- *Incident Management*;
- *Configuration and Asset Management*;
- *Forensics investigation*;
- *Event Monitoring*.

Pada saat perencanaan suatu layanan dan penetapan SLA (*Service Level Agreement*) juga harus mempertimbangkan aspek keamanan terutama dari segi jaminan ketersediaan (*availability*).

2. *IT Application Level Patterns*

*IT Application Level Patterns* merupakan aspek keamanan yang diterapkan pada level aplikasi. Jaminan tingkat keamanan yang tinggi apabila arsitektur aplikasi yang digunakan berbasis *services oriented architecture (SOA)*, *N-Tier Architecture*, dan *Software as a Service* dimana setiap layanan aplikasi bertukar data melalui jaringan. Jaminan keamanan juga harus diterapkan untuk aplikasi yang bersifat *collaboration* seperti *email*, pertukaran dokumen, dan *instant messaging*, karena rawan terhadap aspek kerahasiaan, keutuhan data dan data *spam*.

3. *IT Infrastructure Patterns*

*IT Infrastructure Patterns* merupakan jaminan tingkat keamanan level infrastruktur IT, terutama pada level jaringan dan *Server*. Bagian jaringan yang membutuhkan tingkat keamanan tertinggi adalah pada jaringan *wireless*, perangkat *firewall (border network)*, jaringan kantor cabang, dan akses tamu (*guest access*). Jaminan keamanan *Server* yang harus diperhatikan adalah pada level *web Server* yang diakses melalui jaringan internet dan *Server data warehouse*.

Arsitektur Keamanan Informasi untuk Pemerintahan Kota Magelang dibagi menjadi 2 (dua) kategori, yaitu:

1. **Arsitektur Keamanan Defensif (*Defensive Security Architecture*)**
2. **Arsitektur Keamanan Ofensif (*Offensive Security Architecture*)**

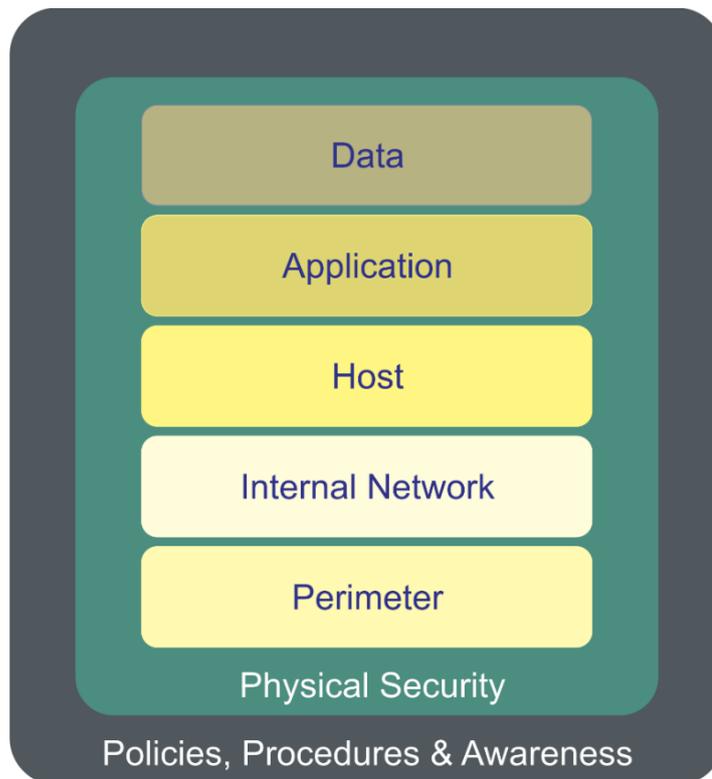
Arsitektur Keamanan Informasi ini akan direvisi sesuai kebutuhan dan tingkat kematangan penerapan keamanan informasi di lingkungan Pemerintahan Kota Magelang .

#### 5.4.1 **Arsitektur Keamanan Defensif**

Arsitektur Keamanan Defensif (*Defensive Security Architecture*) mencakup rancangan ideal yang sebaiknya diterapkan oleh Pemerintahan Kota Magelang untuk melakukan perlindungan terhadap keamanan data/informasi dari berbagai ancaman terhadap pelanggaran kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) dari data/informasi yang menjadi milik Pemerintahan Kota Magelang .

Arsitektur Keamanan Defensif memiliki 7 lapis perlindungan (*defensive layer*) sebagai berikut:

1. Data
2. Aplikasi (*Application*)
3. Host
4. Jaringan Internal (*Internal Network*)
5. Perbatasan (*Perimeter*)
6. Keamanan Fisik (*Physical Security*)
7. Kebijakan, Prosedur dan Kesadaran (*Policies, Procedures and Awareness*)



Gambar 61 : Arsitektur Keamanan

### 1. Data

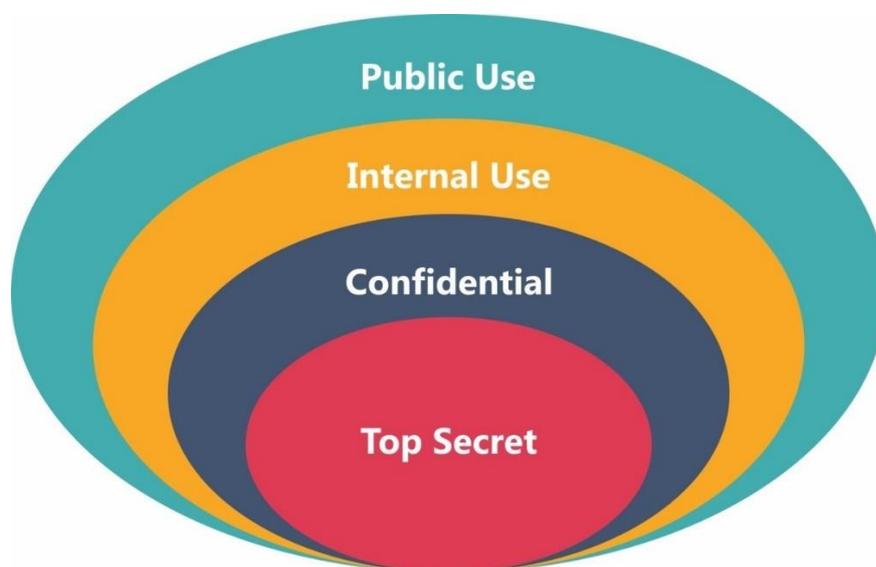
Lapisan atau *layer* Data mencakup semua data dan informasi yang dimiliki dan dibutuhkan oleh Pemerintahan Kota Magelang untuk menunjang proses bisnis. Data merupakan sebuah aset yang berharga dan mempunyai nilai yang tinggi sehingga harus dilindungi terhadap berbagai ancaman yang dapat melanggar kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*).

Bila terjadi pelanggaran terhadap kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) terhadap data/informasi tersebut, maka pasti akan menyebabkan kerugian bagi Pemerintahan Kota Magelang dalam penyelenggaraan Bisnis. Aset berupa data dan informasi tersebut harus dijaga agar tidak terjadi pengurangan nilai terhadapnya, misalnya:

1. Pelanggaran kerahasiaan (*confidentiality*): data yang seharusnya bersifat sensitif harus dijaga jangan sampai bisa diakses oleh pihak yang tidak memiliki wewenang untuk mengakses data tersebut. Nilai dari data tersebut akan berkurang bila sampai diketahui oleh pihak yang tidak boleh mengetahuinya.

2. Pelanggaran keutuhan (*integrity*): data yang seharusnya kritis harus dijaga jangan sampai bisa diubah oleh pihak yang tidak memiliki wewenang untuk mengubah data tersebut. Nilai dari data tersebut akan berkurang bila sampai diubah oleh pihak yang tidak boleh mengubah sehingga data tersebut tidak bisa lagi dipercaya.
3. Pelanggaran ketersediaan (*availability*): data yang seharusnya kritis harus dijaga jangan sampai dirusak atau dihapus oleh pihak lain tanpa otorisasi pemilik data. Organisasi akan mengalami kerugian bila terjadi gangguan sehingga tidak bisa mengakses data yang dibutuhkan tersebut.

Untuk menentukan tingkat sensitivitas dan tingkat kritikalitas dari semua data/informasi yang dimiliki oleh Pemerintahan Kota Magelang , maka harus disusun definisi Klasifikasi Data (*Data Classification*) yang terdokumentasi secara formal sehingga tingkat kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) dari tiap kategori data/informasi terdefinisi dengan jelas untuk menentukan cara penanganannya secara tepat.



Gambar 62 : Tingkat sensitivitas dan tingkat kritikalitas data

Hanya bila sudah terdapat Klasifikasi Data (*Data Classification*) yang sesuai dengan kebutuhan proses bisnis Pemerintahan Kota Magelang , penentuan tingkat keamanan baru bisa ditentukan untuk dapat memastikan penanganan yang tepat untuk tiap data/informasi milik Pemerintahan Kota Magelang .



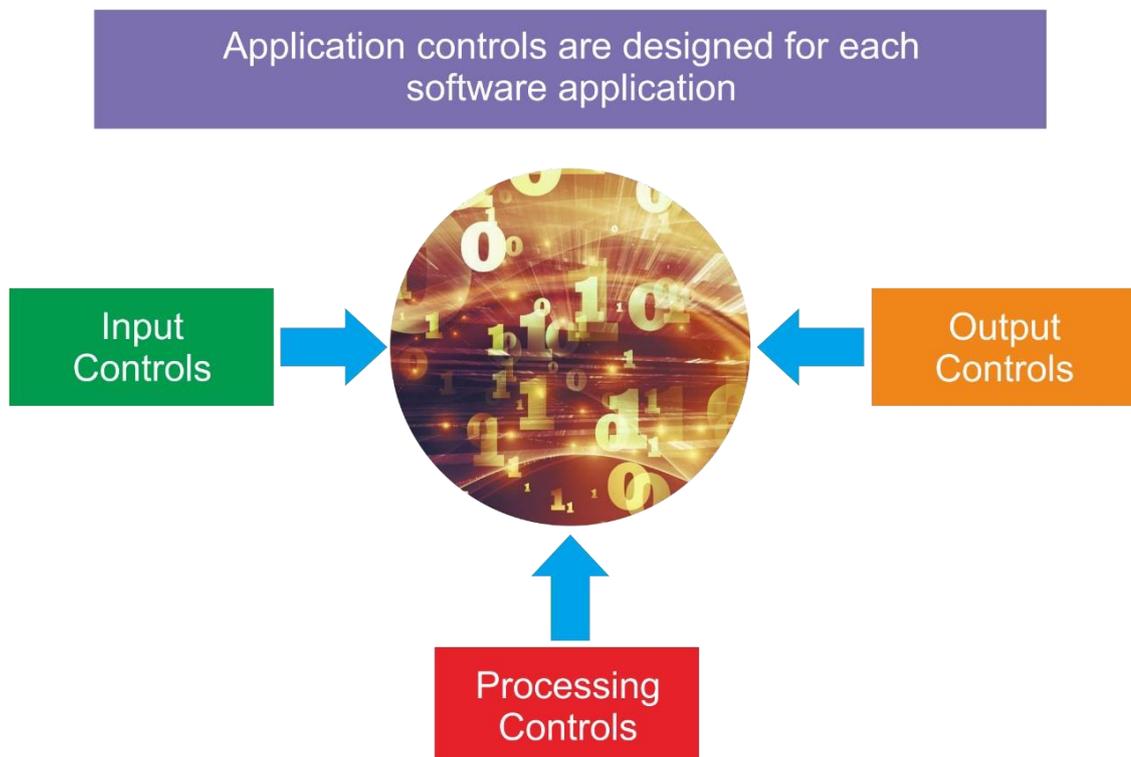
Gambar 63 : Data Classification

## 2. Aplikasi

Lapisan atau layer Aplikasi (*Application*) perlu memiliki perlindungan terhadap berbagai ancaman yang melakukan eksploitasi terhadap berbagai kelemahan (*vulnerability*) yang terdapat di aplikasi akibat kesalahan (*bug*) di kode sumber (*source code*) atau kurangnya kendali (*control*) input, proses dan output yang dibuat oleh *programmer*.

Tiap aplikasi yang digunakan oleh Pemerintahan Kota Magelang harus memiliki 3 (tiga) jenis kendali aplikasi (*application control*) sebagai berikut:

## Application Controls



Gambar 64 : Application control

1. Kendali Input (*Input Control*) : Kendali untuk memastikan bahwa masukan atau input berasal dari sumber yang otentik dan sudah terotorisasi.
2. Kendali Proses (*Processing Control*) : Kendali untuk memastikan bahwa data/informasi yang akan diproses sudah akurat, lengkap, dan sesuai dengan aturan yang berlaku.
3. Kendali Output (*Output Control*) : Kendali untuk memastikan bahwa data/informasi diterima oleh penerima yang benar dan terotorisasi.

Penerapan kendali aplikasi (*application controls*) perlu cukup efektif untuk menangkal *OWASP Top Ten Vulnerability* sebagai berikut:

1. *Injection*
2. *Broken Authentication & Session Management*
3. *Cross-Site Scripting (XSS)*
4. *Insecure Direct Object References*
5. *Security Misconfiguration*
6. *Sensitive Data Exposure*
7. *Missing Function Level Access Control*
8. *Cross-Site Request Forgery (CSRF)*
9. *Using Known Vulnerable Components*
10. *Unvalidated Redirects & Forwards*

Untuk memastikan bahwa aplikasi tidak memiliki kerentanan berdasarkan *OWASP Top Ten Vulnerability* di atas, maka tiap aplikasi perlu lulus uji berdasarkan *OWASP Application Security Verification Standard (ASVS)* dalam 16 (enam belas) kategori berikut:

1. V1. *Architecture, design and threat modeling*
2. V2. *Authentication*
3. V3. *Session management*
4. V4. *Access control*
5. V5. *Malicious input handling*
6. V7. *Cryptography at rest*
7. V8. *Error handling and logging*
8. V9. *Data protection*
9. V10. *Communications*
10. V11. *HTTP security configuration*
11. V13. *Malicious controls*
12. V15. *Business logic*
13. V16. *File and resources*
14. V17. *Mobile*

15. V18. *Web services*
16. V19. *Configuration*

### 3. *Host*

Lapisan atau *layer Host* merupakan perlindungan terhadap komputer, baik sisi client maupun *Server*. Bila terdapat kelemahan (*vulnerability*) pada sistem operasi (*operating system*) atau layanan (*service*) yang jalan di *host*, maka ada risiko bahwa lubang keamanan tersebut bisa dieksploitasi oleh penyerang untuk menguasai atau mengambil alih *host* tersebut.

Untuk melindungi *host* dari berbagai ancaman serangan, maka perlu menerapkan berbagai kendali (*control*) untuk melindungi *host* tersebut berupa:



Gambar 65 : *Security Control*

1. Proteksi terhadap *malicious software (malware)* berupa anti-virus dan anti-malware yang mampu mendeteksi dan menangkal masuknya virus atau malware ke dalam *host*.
2. Pemasangan *Host-based Intrusion Detection System (HIDS)* atau *Host-based Intrusion Prevention System (HIPS)* yang mampu mendeteksi dan menangkal upaya intrusi atau penembusan terhadap *host* yang mengubah berbagai file penting yang terdapat di *host* tersebut.
3. Pemasangan *personal/host firewall* yang mampu menutup dan memblokir berbagai serangan terhadap *host* melalui jaringan.
4. Penerapan *patch* atau *update* secara berkala terhadap sistem operasi, layanan, dan aplikasi yang terdapat di *host* sehingga berbagai lubang keamanan baru bisa segera ditutup melalui instalasi *patch* atau *update* yang teratur.

5. Memastikan bahwa hanya berbagai fitur, aplikasi dan layanan penting saja yang terinstal di *host*. Berbagai fitur dan layanan yang tidak digunakan perlu dihapus atau dihilangkan (*uninstall*) dari *host* supaya tidak aktif sehingga tidak akan ada kemungkinan untuk dieksploitasi oleh penyerang bila terdapat lubang keamanan (*vulnerability*).
6. Melakukan enkripsi terhadap berbagai data sensitif yang terdapat pada *host* sehingga pihak yang tidak memiliki wewenang tidak dapat membaca data/informasi sensitif tersebut meskipun berhasil mendapatkan akses terhadap *host*.
7. Penerapan *Threat Intelligence Exchange* (TIE) yang mampu mengikuti perkembangan *ancaman* (threat) terbaru secara operasional di seluruh organisasi sehingga mampu menangani serangan-serangan baru secara cepat.

#### 4. Jaringan Internal

Lapisan atau *layer* Jaringan Internal (*Internal Network*) perlu dilindungi untuk mencegah penyalahgunaan dari penyerang internal atau yang sudah berhasil mengakses jaringan dari dalam.

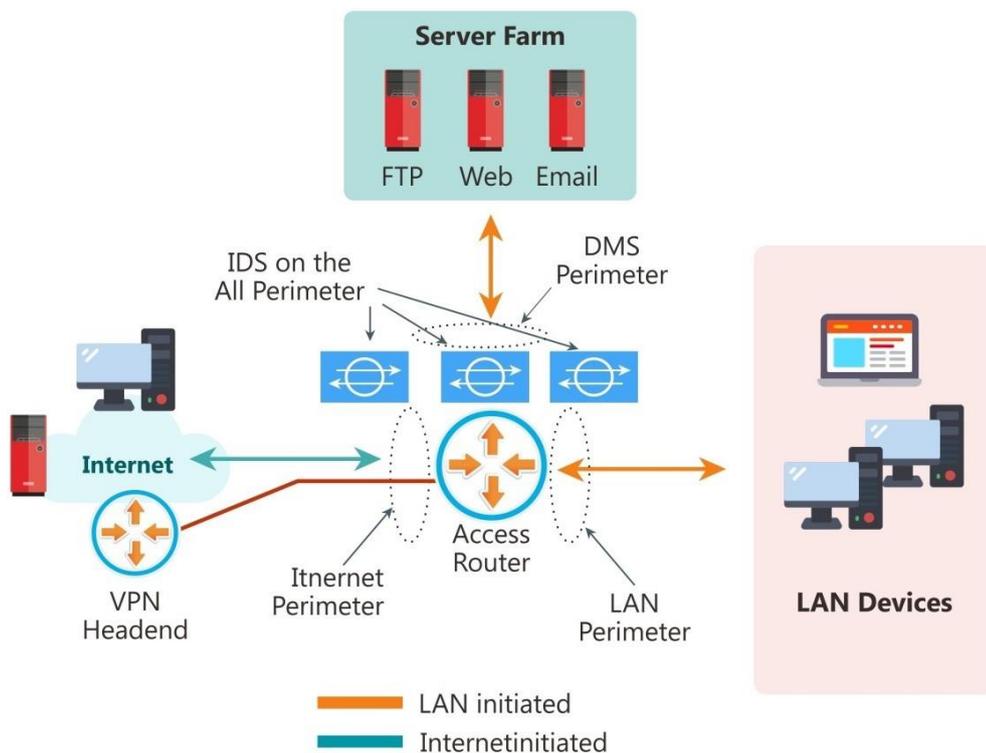
Beberapa kendali untuk jaringan internal:

1. *Internal Firewall*
2. *Internal Network-based Intrusion Detection System* (NIDS) atau *Network-based Intrusion Prevention System* (NIPS)
3. *Internal Network Access Control List*
4. *Internal Network Encryption*

## 5. Perbatasan

Lapisan atau *layer* Perbatasan (*Perimeter*) perlu menjadi pagar yang kuat dan kokoh antara jaringan dalam (*intranet*) dan jaringan publik (*Internet*) sehingga mampu mencegah dan menangkal berbagai serangan yang berasal dari luar ingin masuk ke dalam jaringan milik Pemerintahan Kota Magelang .

Beberapa kendali untuk *perimeter* adalah:



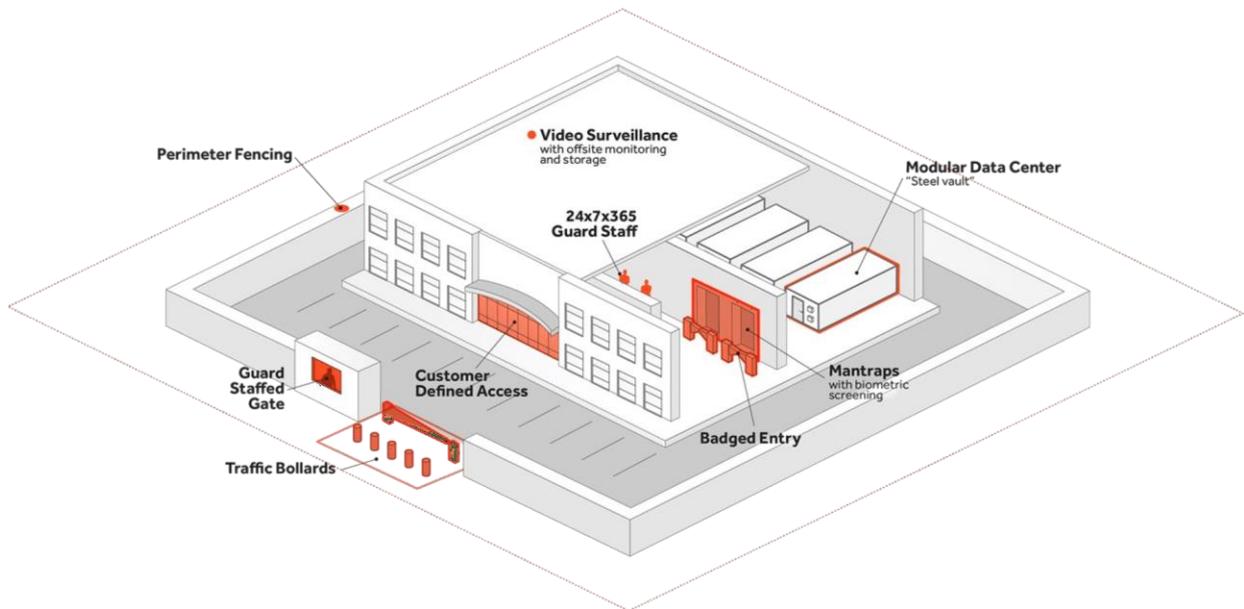
Gambar 66 : Kendali Perimeter

1. Pembentukan *Demilitarized Zone* (DMZ)
2. *Network Perimeter Firewall*
3. *Perimeter Network-based Intrusion Detection System* (NIDS) atau *Network-based Intrusion Prevention System* (NIPS)
4. *Perimeter Network Access Control List*
5. *Virtual Private Network* (VPN)

## 6. Keamanan Fisik

Lapisan atau *layer* Keamanan Fisik (*Physical Security*) merupakan segala sesuatu berbentuk fisik yang dapat melindungi terhadap berbagai serangan yang berbentuk nyata terhadap semua aset fisik termasuk perangkat keras TI.

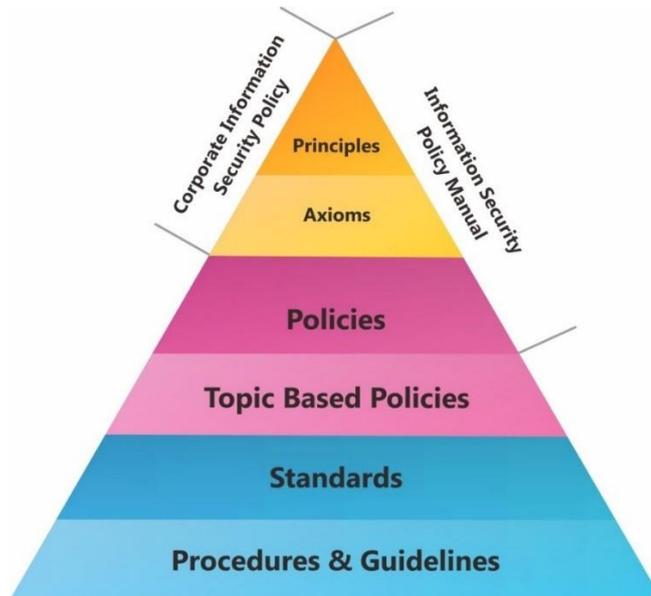
Beberapa kendali untuk keamanan fisik mencakup:



Gambar 67 : Physical Security

## 7. Kebijakan, Prosedur dan Kesadaran

Lapisan atau *layer* Kebijakan, Prosedur dan Kesadaran (*Policies, Procedures and Awareness*) mencakup penerapan berbagai kendali administratif (*administrative control*) untuk memastikan bahwa penerapan keamanan informasi benar-benar dilakukan serta dilakukan dengan benar.



Gambar 68 : *Policies, Procedures and Awareness*

Beberapa kebijakan yang perlu disusun untuk memastikan legalitas penerapan keamanan informasi adalah sebagai berikut:

1. *General Policy*
  - a. *Acceptable Encryption Policy*: Menguraikan persyaratan seputar algoritma enkripsi mana (misalnya, mendapat tinjauan publik yang substansial dan telah terbukti berhasil secara efektif) dapat diterima untuk digunakan dalam perusahaan.
  - b. *Acceptable Use Policy*: Mendefinisikan penggunaan peralatan dan layanan komputasi yang dapat diterima, dan tindakan keamanan pegawai yang sesuai untuk melindungi sumber daya dan informasi kepemilikan Pemerintahan Kota Magelang .
  - c. *Clean Desk Policy*: Mendefinisikan persyaratan minimum untuk menjaga "meja bersih" dimana informasi sensitif/kritis tentang pegawai, kekayaan intelektual, penduduk dan vendor aman di area yang terkunci dan tidak terlihat.

- d. *Data Breach Response Policy*: Mendefinisikan tujuan dan visi untuk proses respon pelanggaran. Kebijakan ini mendefinisikan siapa yang berlaku dan dalam keadaan apa, dan mencakup definisi pelanggaran, peran dan tanggung jawab staf, standar dan metrik (misalnya, untuk memungkinkan prioritas insiden), serta pelaporan, remediasi, dan umpan balik.
- e. *Disaster Recovery Plan Policy*: Mendefinisikan persyaratan untuk rencana pemulihan bencana yang akan dikembangkan dan dilaksanakan oleh instansi Pemerintahan Kota Magelang , yang menggambarkan proses pemulihan Sistem Informasi, Aplikasi dan Data dari segala jenis bencana yang menyebabkan pemadaman besar.
- f. *Digital Signature Acceptance Policy*: Mendefinisikan persyaratan ketika tanda tangan digital dianggap sebagai sarana yang dapat diterima untuk memvalidasi identitas penandatanganan dalam dokumen elektronik dan korespondensi, dan dengan demikian merupakan pengganti tanda tangan "basah" tradisional, di dalam instansi Pemerintahan Kota Magelang .
- g. *Email Policy*: Mendefinisikan persyaratan untuk penggunaan yang tepat dari sistem *email* instansi Pemerintahan Kota Magelang dan membuat pengguna mengetahui apa yang dianggap dapat diterima dan tidak dapat diterima dalam penggunaan sistem *email*.
- h. *Password Protection Policy*: Mendefinisikan standar untuk pembuatan password yang kuat, perlindungan password tersebut, dan frekuensi perubahannya.
- i. *Removable Media Policy*: Mendefinisikan persyaratan penggunaan media removable.

## 2. *Network Security Policy*

- a. *Remote Access Policy*: Mendefinisikan standar untuk menghubungkan ke jaringan instansi Pemerintahan Kota Magelang dari *host* atau jaringan di luar instansi.
- b. *Router & Switch Security Policy*: Mendefinisikan standar untuk konfigurasi keamanan minimal untuk *router* dan *switch* di dalam jaringan yang digunakan instansi Pemerintahan Kota Magelang .
- c. *Wireless Communication Policy*: Mendefinisikan persyaratan perangkat infrastruktur nirkabel untuk mematuhi kebijakan komunikasi nirkabel agar dapat terhubung ke jaringan instansi Pemerintahan Kota Magelang .
- d. *Internet Usage Policy*: Menentukan standar untuk sistem yang memantau dan membatasi penggunaan *web* dari *host* mana pun di dalam jaringan instansi Pemerintahan Kota Magelang .

### 3. *Server Security Policy*

- a. *Database Credentials Policy*: Mendefinisikan persyaratan untuk menyimpan dan mengambil username dan password basis data dengan aman untuk digunakan oleh program yang akan mengakses basis data yang berjalan di salah satu jaringan instansi Pemerintahan Kota Magelang .
- b. *Technology Equipment Disposal Policy*: Mendefinisikan persyaratan untuk pembuangan peralatan elektronik yang benar, termasuk hard drive, drive USB, CD-ROM dan media penyimpanan lainnya yang mungkin berisi berbagai jenis data instansi Pemerintahan Kota Magelang , beberapa di antaranya dapat dianggap sensitif.
- c. *Information Logging Standard*: Mendefinisikan persyaratan spesifik untuk sistem informasi untuk menghasilkan log audit sesuai yang akan diintegrasikan dengan fungsi pengelolaan log instansi Pemerintahan Kota Magelang .
- d. *Server Security Policy*: Mendefinisikan standar untuk konfigurasi keamanan minimum untuk *Server* di dalam jaringan yang digunakan instansi Pemerintahan Kota Magelang .
- e. *Email Retention Policy*: Mendefinisikan panduan untuk membantu pegawai menentukan informasi yang dikirim atau diterima melalui *email* harus disimpan dan untuk berapa lama.

### 4. *Application Security Policy*

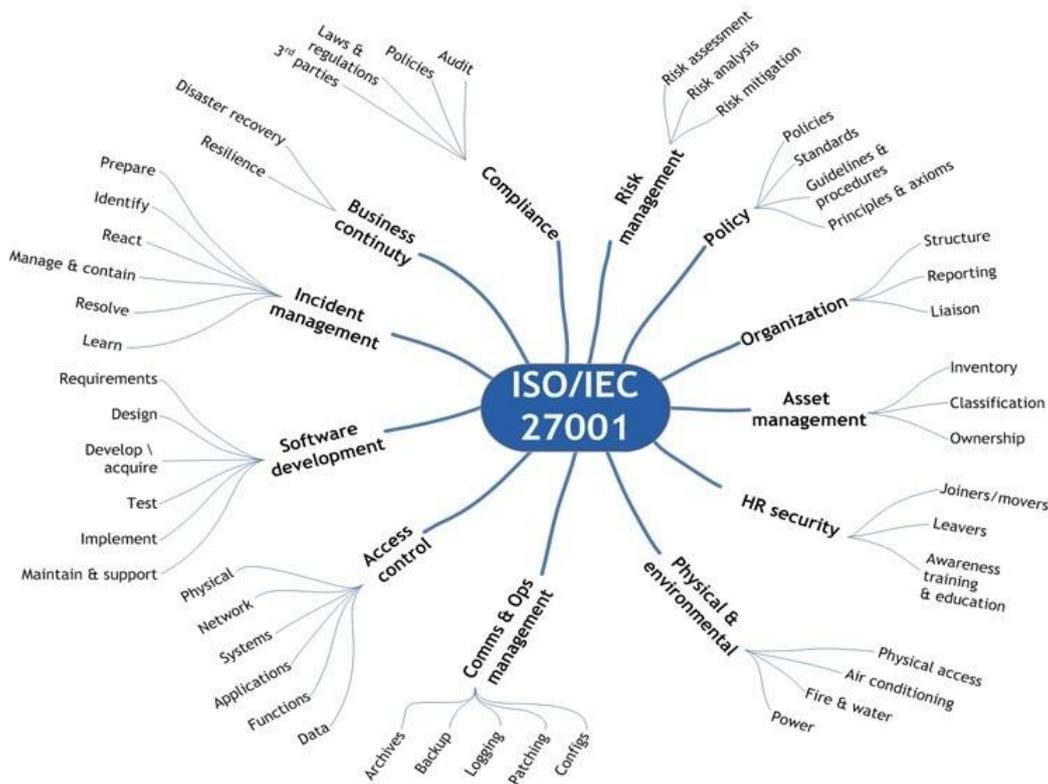
- a. *Software Installation Policy*: Mendefinisikan persyaratan seputar pemasangan perangkat lunak pihak ketiga pada perangkat yang dimiliki instansi Pemerintahan Kota Magelang .
- b. *Web Application Security Policy*: Mendefinisikan persyaratan untuk melengkapi penilaian dan pedoman keamanan aplikasi *web* untuk melaksanakan penilaian tersebut.
- c. *Anti-Virus Policy*: Mendefinisikan pedoman untuk secara efektif mengurangi ancaman virus komputer di jaringan instansi Pemerintahan Kota Magelang .

### 5.4.2 Arsitektur Keamanan Ofensif

Arsitektur Keamanan Ofensif (*Offensive Security Architecture*) mencakup rancangan ideal yang sebaiknya diterapkan oleh Pemerintahan Kota Magelang untuk melakukan kegiatan pengujian terhadap implementasi arsitektur keamanan defensif (*defensive security architecture*) serta kegiatan penanganan terhadap serangan ofensif (*offensive attack*) yang telah terjadi.

Arsitektur Keamanan Ofensif mencakup pelaksanaan berbagai kegiatan berikut:

1. *IT Security Audit*: Melakukan kegiatan audit terhadap Sistem Manajemen Keamanan Informasi dari sisi tata kelola keamanan informasi atau sisi non-teknis berbasis standar internasional ISO 27001.



Gambar 69 : ISO 27001

2. *Vulnerability Assessment & Penetration Test (VAPT)*: Melakukan kegiatan asesmen lubang keamanan dan tes penetrasi untuk menguji ketahanan terhadap kendali keamanan defensif (*defensive security control*) secara teknis serta menemukan lubang-lubang keamanan yang masih ada sehingga bisa dilakukan perbaikan untuk menutup berbagai lubang keamanan yang ditemukan.



Gambar 70 : *Vulnerability Assessment & Penetration Test (VAPT)*

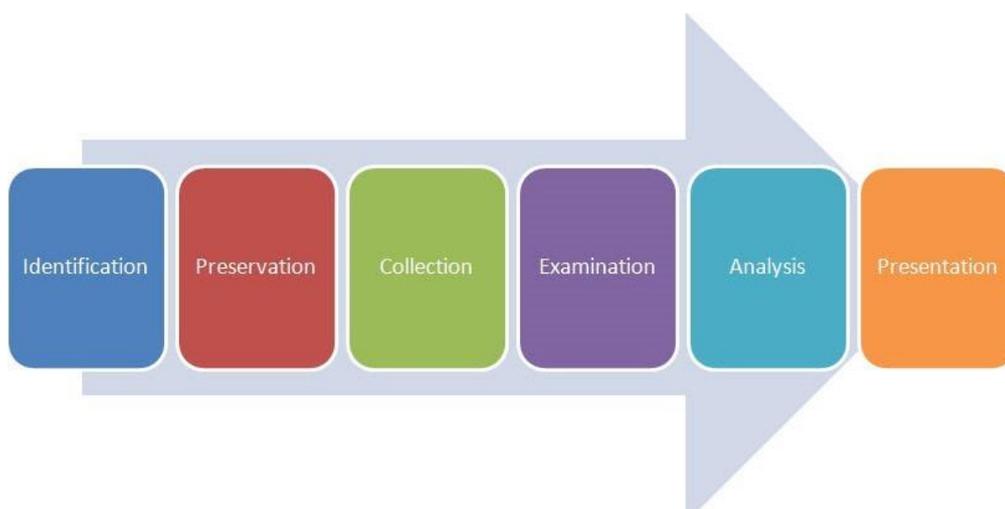
3. *Computer Security Incident Handling*: Melibatkan pemantauan dan deteksi kejadian keamanan di komputer atau jaringan komputer, dan pelaksanaan tanggapan yang tepat terhadap kejadian tersebut oleh anggota CSIRT (*Computer Security Incident Response Team*) sehingga dampak insiden pelanggaran keamanan informasi bisa diminimalisir dan Pemerintahan Kota Magelang dapat kembali menggunakan sistem informasi untuk menunjang proses bisnis Pemerintahan Kota Magelang .

## Incident Response/ & Handling



Gambar 71 : Incident Response & Handling

4. *Computer Hacking Forensic Readiness*: Memastikan Pemerintahan Kota Magelang memiliki kemampuan dan kesiapan untuk pelaksanaan kegiatan forensik bila terkena serangan yang melanggar kerahasiaan (*confidentiality*), keutuhan (*integrity*), atau ketersediaan (*availability*) terhadap data/informasi milik Pemerintahan Kota Magelang sehingga berbagai bukti dapat dihimpun, dianalisis, dan dipresentasikan dalam pengadilan untuk mempidanakan pelaku sehingga memberi efek jera.

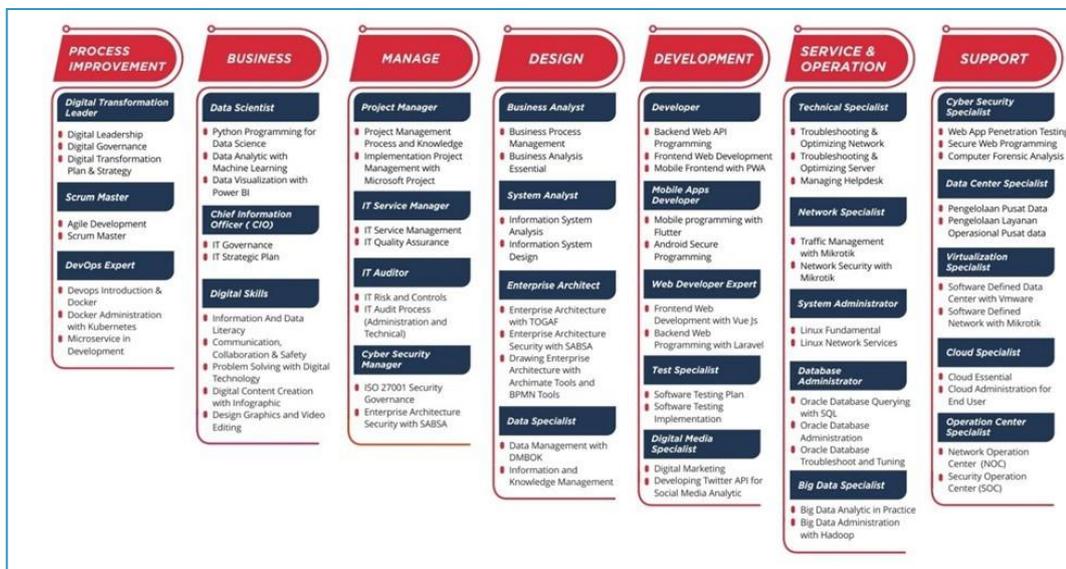


Gambar 72 : Computer Hacking Forensic Readiness

## 5.5 Arsitektur SDM

### 5.5.1 Job Role SDM Digital Transformation

Selain aspek Selain Faktor Budaya Teknologi SDM juga mempunyai peranan penting dalam Kebutuhan Pemerintahan Kota Magelang untuk dapat bertransformasi secara digital juga. Berikut merupakan kebutuhan SDM Pemerintahan Kota Magelang sesuai dengan job role untuk dapat bertransformasi secara digital.



Gambar 73 : Job Role SDM Digital Transformation

Dan berikut gambaran detail mengenai skill yang harus dimiliki oleh job role untuk menunjang transformasi digital.

Tabel 13 : Tabel Job Role Transformasi Digital

No	Dimensi Aspek	Job Role	Skill
1	Process Improvement	Digital Transformation Leader	<ul style="list-style-type: none"> <li>Bisa Menjelaskan Digital Leadership sebagai aspek penting keberhasilan Transformasi Digital</li> <li>Bisa Menyusun Strategi dan Penerapan Digitalisasi</li> <li>Bisa Menilai Kematangan Transformasi Digital</li> </ul>

			<ul style="list-style-type: none"> <li>• Bisa Mengilustrasikan bagaimana seorang Leader melakukan Transformasi Digital dengan kemampuan Digital Leadership</li> <li>• Bisa Menentukan Digital Competency Framework untuk pengembangan SDM</li> <li>• Bisa Menceritakan Digital Mastery dalam bentuk Digital Leadership dan Digital Capability</li> <li>• Bisa Menyusun rencana dan analisis resiko Transformasi Digital</li> <li>• Bisa Menjelaskan Transformasi Digital dalam rangka peningkatan layanan customer, proses bisnis internal organisasi, dan model bisnis suatu produk atau layanan yang baru.</li> <li>• Bisa Menjelaskan tata kelola Digital dalam membangun akuntabilitas yang jelas antara strategi, kebijakan dan standar di organisasi</li> <li>• Bisa Menjelaskan apa yang perlu diperhatikan dalam melakukan tata kelola IT</li> <li>• Bisa Menjelaskan faktor trend teknologi dalam melakukan inovasi dengan menggunakan Business Model Canvas</li> <li>• Bisa Menjelaskan pentingnya tata kelola Data dengan Machine Learning dan AI</li> <li>• Bisa Menjelaskan pentingnya validasi dan keamanan pada saat transmisi data</li> <li>• Bisa Menjelaskan faktor keberhasilan Transformasi Digital</li> <li>• Bisa Menceritakan besarnya peran organisasi dan individu dalam berkontribusi menciptakan Transformasi Digital</li> <li>• Bisa Mengidentifikasi penguasaan Digital Capability dan Leadership Capability dalam ranah bisnis dan organisasi</li> <li>• Bisa Mengkategorikan Sasaran Strategis Organisasi dan indikatornya</li> </ul>
--	--	--	--

			<p>dari berbagai perspektif berbasis Balance Scorecard</p> <ul style="list-style-type: none"> <li>• Bisa Menguraikan Sasaran Strategis Organisasi dan indikatornya berbasis Balance Scorecard</li> <li>• Bisa Menghasilkan Bisnis yang lebih terukur dengan Bisnis Model Canvas</li> <li>• Bisa Menyusun Formula Digital Transformation Plan yang terukur</li> <li>• Bisa Menyimpulkan Masalah Bisnis secara lebih akurat dengan pendekatan Design Thinking</li> </ul>
		Scrum Master	<ul style="list-style-type: none"> <li>• Bisa Membedakan 2 Metode Pengembangan: Waterfall SDLC vs Agile Development</li> <li>• Bisa Menjelaskan karakteristik Agile Development</li> <li>• Bisa Menceritakan Siklus Agile Development</li> <li>• Bisa Mempertimbangkan pilihan metode pengembangan berdasarkan karakteristik dan kebutuhan stakeholder</li> <li>• Bisa Menyimpulkan konsep Agile Development</li> <li>• Bisa Membandingkan 2 Metode Pengembangan: Waterfall SDLC vs Agile Development</li> <li>• Bisa Menguraikan Siklus dari Agile Development</li> <li>• Bisa Mendefinisikan Agile Development dengan jelas</li> <li>• Bisa Mengilustrasikan Siklus Kerja Scrum</li> <li>• Bisa Menyatakan Keunggulan Scrum</li> <li>• Bisa Mengidentifikasi peran dan tanggungjawab dari Anggota Scrum</li> <li>• Bisa Menentukan peran dan tanggungjawab dari Anggota Scrum</li> <li>• Bisa Menyimpulkan peran Scrum Master dalam Scrum Team</li> <li>• Bisa Mengkategorikan peran pada Scrum Team</li> <li>• Bisa Menguraikan Siklus Kerja Scrum</li> <li>• Bisa Mendefinisikan peran dan tanggung jawab Scrum Team</li> </ul>

			<ul style="list-style-type: none"> <li>• Bisa Menghitung estimasi poin pada User Story</li> <li>• Bisa Menilai ukuran poin pada User Story</li> <li>• Bisa Merangking prioritas backlog</li> <li>• Bisa Menyusun urutan backlog dan sprint</li> </ul>
		Devops Expert	<ul style="list-style-type: none"> <li>• Bisa Membedakan Virtual Machine dan Containerization</li> <li>• Bisa Menceritakan arsitektur software berbasis kontainerisasi</li> <li>• Bisa Mengidentifikasi Environment utama kontainerisasi</li> <li>• Bisa Mengenali Environment DevOps</li> <li>• Bisa Menyiapkan perangkat kontainerisasi</li> <li>• Bisa Membuat image kontainer untuk sebuah aplikasi</li> <li>• Bisa Mengoperasikan Container dari sebuah image</li> <li>• Bisa Mengklasifikasikan Siklus DevOps</li> <li>• Bisa Mengilustrasikan peran pada fitur Orkestrasi</li> <li>• Bisa Menjelaskan arsitektur Orkestrasi</li> <li>• Bisa Mengidentifikasi kebutuhan menjalankan container dengan</li> <li>• Bisa Mendesain konfigurasi untuk menjalankan sebuah Service</li> <li>• Bisa Mengembangkan container dan pod menjadi sebuah Service</li> </ul>
2	Business	Data Scientist	<ul style="list-style-type: none"> <li>• Bisa menjelaskan ilmu data science dan penggunaannya</li> <li>• Bisa memilih tools yang akan digunakan untuk mengolah data</li> <li>• Bisa mengidentifikasi data-data yang akan diolah</li> <li>• Bisa menentukan cara untuk mengolah data sesuai keadaan data</li> <li>• Bisa mengoperasikan tools pengolahan data</li> <li>• Bisa menyimpulkan hasil pengolahan data yang telah dilakukan</li> <li>• Bisa menjelaskan pengertian machine learning dan penggunaannya</li> <li>• Bisa memilih jenis machine learning sesuai dengan data yang diolah</li> </ul>

			<ul style="list-style-type: none"> <li>• Bisa mengenali permasalahan-permasalahan bisnis yang bisa ditangani dengan machine learning</li> <li>• Bisa mengkategorikan algoritma dan tools di dalam machine learning</li> <li>• Bisa menyiapkan data untuk digunakan machine learning</li> <li>• Bisa mengembangkan penggunaan machine learning untuk memecahkan permasalahan bisnis</li> <li>• Bisa menghasilkan prediksi berdasarkan machine learning yang digunakan</li> </ul>
		Chief Information Officer ( CIO )	<ul style="list-style-type: none"> <li>• Bisa menjelaskan konsep dan definisi IT Governance</li> <li>• Bisa mendefinisikan tujuan strategis, kebutuhan dan risiko bisnis</li> <li>• Bisa menentukan tujuan IT yang berkorelasi dengan bisnis</li> <li>• Bisa menentukan IT enabler untuk mencapai tujuan IT</li> <li>• Bisa mengidentifikasi risiko-risiko IT yang bisa menggagalkan tujuan IT</li> <li>• Bisa menjelaskan rencana strategis bisnis</li> <li>• Bisa membuat analisa balanced scorecard</li> <li>• Bisa membuat analisa PESTEL</li> <li>• Bisa membuat analisa value chain</li> <li>• Bisa menyusun kebutuhan informasi organisasi</li> <li>• Bisa menyusun perencanaan strategis IT</li> <li>• Bisa membuat arsitektur teknologi informasi (aplikasi, infrastruktur, keamanan)</li> <li>• Bisa menyusun roadmap proyek pengembangan</li> </ul>
		Digital Worker ( End User )	<ul style="list-style-type: none"> <li>• Bisa menghasilkan data dari sumber penyedia data</li> <li>• Bisa mengenali kebutuhan dari informasi</li> <li>• Bisa mengklasifikasikan informasi yang didapatkan</li> <li>• Bisa menyusun data yang didapatkan menjadi sebuah informasi</li> </ul>

			<ul style="list-style-type: none"> <li>• Bisa mengoperasikan tools untuk berkomunikasi</li> <li>• Bisa menyatakan suatu informasi secara baik</li> <li>• Bisa menguraikan Digital Citizenship</li> <li>• Bisa mengutarakan pendapat pada media kolaborasi di dunia digital</li> <li>• Bisa menyelesaikan masalah dengan menggunakan teknologi</li> <li>• Bisa mengklasifikasikan inovasi</li> <li>• Bisa menghasilkan solusi dari suatu studi kasus masalah</li> <li>• Bisa menyusun Business Canvas Model</li> <li>• Bisa menyusun Design Thinking</li> <li>• Bisa menyusun sumber data menjadi informasi</li> <li>• Bisa mengkombinasikan infografis</li> <li>• Bisa membuat desain dengan tool infografis</li> <li>• Bisa memilih ilustrasi yang sesuai</li> <li>• Bisa mengoperasikan tool untuk design graphics</li> </ul>
3	Manage	Project Manager	<ul style="list-style-type: none"> <li>• Bisa Mendefinisikan project dan project management</li> <li>• Bisa Mengorganisasikan task task yang dibutuhkan untuk menyelesaikan project</li> <li>• Bisa Menyelesaikan masalah yang muncul saat menjalani project</li> <li>• Bisa Menggambarkan goal project dan cara mendapatkan goal project</li> <li>• Bisa Menyusun perencanaan project</li> <li>• Bisa Memeriksa kesesuaian pelaksanaan project dengan perencanaan project</li> <li>• Bisa Menyiapkan kebutuhan dokumen-dokumen project</li> <li>• Bisa Membreakdown bidang knowledge dalam project</li> </ul>
		IT Service Manager	<ul style="list-style-type: none"> <li>• Bisa Menjelaskan Konsep layanan TI</li> <li>• Bisa Menjelaskan Konsep manajemen layanan TI</li> <li>• Bisa Mengenali faktor yang mempengaruhi layanan TI (PESTLE)</li> <li>• Bisa Mengkategorikan jenis-jenis Layanan TI</li> </ul>

		<ul style="list-style-type: none"> <li>• Bisa Menjelaskan secara general konsep ITIL4</li> <li>• Bisa Mendesain struktur layanan TI yang dibutuhkan dalam organisasi</li> <li>• Bisa Membandingkan kondisi nyata saat ini dengan kondisi ideal</li> <li>• Bisa Mengembangkan secara berkelanjutan kualitas layanan TI</li> <li>• Bisa Menentukan apa yang harus dilakukan dengan kondisi saat ini</li> </ul>
	IT Auditor	<ul style="list-style-type: none"> <li>• Bisa mengidentifikasi ancaman dan kerentanan TI</li> <li>• Bisa menilai risiko TI berdasarkan kecenderungan dan dampak</li> <li>• Bisa memilih kendali terhadap risiko TI secara tepat</li> <li>• Bisa mendaftarkan berbagai risiko TI dalam Risk Register</li> <li>• Bisa menentukan strategi penanganan risiko TI yang tepat</li> <li>• Bisa menjelaskan kebutuhan organisasi untuk audit TI</li> <li>• Bisa mengorganisasikan kegiatan audit TI sesuai standar</li> <li>• Bisa memeriksa kondisi penerapan TI di organisasi</li> <li>• Bisa menyimpulkan kesesuaian penerapan TI dengan standar</li> <li>• Bisa mengutarakan pendapat terhadap penerapan kontrol TI</li> <li>• Bisa menyatakan hasil audit TI dalam bentuk laporan</li> <li>• Bisa menguraikan temuan dan rekomendasi perbaikan TI</li> <li>• Bisa Menjelaskan konsep tatakelola TI</li> <li>• Bisa Menjelaskan hubungan tatakelola dan layanan TI</li> <li>• Bisa Menyiapkan kerangka jaminan layanan TI sebagai kerangka SLA</li> <li>• Bisa Menyimpulkan untuk memastikan kualitas TI memerlukan acuan COBIT</li> <li>• Bisa Menyusun proses alur kerja TI dalam dukungan terhadap organisasi</li> </ul>
	Cyber Security Manager	<ul style="list-style-type: none"> <li>• Bisa mengidentifikasi persyaratan standar ISO 27001</li> </ul>

			<ul style="list-style-type: none"> <li>• Bisa menentukan berbagai dokumentasi sesuai ISO 27001</li> <li>• Bisa memilih kendali ISO 27001 secara tepat</li> <li>• Bisa menilai kesesuaian organisasi dengan standar ISO 27001</li> <li>• Bisa menguraikan langkah implementasi Sistem Manajemen Keamanan Informasi</li> <li>• Bisa mengenali sasaran keamanan informasi</li> <li>• Bisa menjelaskan kerangka arsitektur keamanan SABSA</li> <li>• Bisa mengidentifikasi enam layer arsitektur keamanan</li> <li>• Bisa mendesain rancangan arsitektur keamanan SABSA</li> <li>• Bisa menentukan jenis kendali keamanan informasi</li> <li>• Bisa menggambarkan model rancangan arsitektur keamanan</li> <li>• Bisa menilai risiko keamanan informasi</li> </ul>
4	Design	Business Analyst	<ul style="list-style-type: none"> <li>• Bisa mengilustrasikan sasaran organisasi dengan Balanced Scorecard</li> <li>• Bisa mengorganisasikan proses bisnis di organisasi</li> <li>• Bisa menguraikan kondisi proses bisnis di organisasi</li> <li>• Bisa mendesain rancangan arsitektur proses bisnis</li> <li>• Bisa menggambarkan model rancangan arsitektur proses bisnis</li> <li>• Bisa menilai proses bisnis secara baik</li> <li>• Bisa menjelaskan kegiatan analisis bisnis</li> <li>• Bisa mengkategorikan pengetahuan analisis bisnis berbasis BABOK</li> <li>• Bisa menentukan transformasi digital yang tepat untuk bisnis</li> <li>• Bisa menguraikan permasalahan bisnis dengan tool dan teknik</li> <li>• Bisa menilai risiko bisnis</li> <li>• Bisa mengutarakan berbagai ide untuk inovasi bisnis</li> </ul>
		System Analyst	<ul style="list-style-type: none"> <li>• Bisa Mengkategorikan jenis sistem informasi</li> </ul>

		<ul style="list-style-type: none"> <li>• Bisa Mempertimbangkan pilihan pengembangan sistem informasi</li> <li>• Bisa Mengorganisasikan kebutuhan untuk pengembangan sistem informasi</li> <li>• Bisa Menghitung kebutuhan pembiayaan sistem informasi</li> <li>• Bisa Menggambarkan sistem yang perlu atau sedang dibuat</li> <li>• Bisa Memperjuangkan hasil analisis yang dibuat</li> <li>• Bisa Mengoperasikan alat bantu proses analisis sistem</li> <li>• Bisa Mengenali masalah yang dihadapi organisasi</li> <li>• Bisa Menjelaskan kebutuhan akan pemodelan yang baik dan benar</li> <li>• Bisa Mengidentifikasi model diagram sesuai dengan konteks</li> <li>• Bisa Mengoperasikan perangkat lunak pemodelan UML</li> <li>• Bisa Mendesain konsep menjadi model yang sesuai</li> <li>• Bisa Menilai kesesuaian implementasi dengan model</li> <li>• Bisa Mengilustrasikan konsep menjadi model yang sesuai</li> <li>• Bisa Menyelesaikan masalah performa dan kerusakan atau kehilangan data</li> </ul>
	Enterprise Architect	<ul style="list-style-type: none"> <li>• Bisa menjelaskan fungsi dan manfaat arsitektur enterprise</li> <li>• Bisa mengkategorikan empat jenis arsitektur enterprise</li> <li>• Bisa mengorganisasikan penyusunan arsitektur enterprise</li> <li>• Bisa mendesain rancangan arsitektur enterprise</li> <li>• Bisa menggambarkan model rancangan arsitektur enterprise</li> <li>• Bisa mengutarakan prinsip arsitektur enterprise untuk organisasi</li> <li>• Bisa menjelaskan kegiatan analisis bisnis</li> <li>• Bisa mengkategorikan pengetahuan analisis bisnis berbasis BABOK</li> <li>• Bisa menentukan transformasi digital yang tepat untuk bisnis</li> </ul>

			<ul style="list-style-type: none"> <li>• Bisa menguraikan permasalahan bisnis dengan tool dan teknik</li> <li>• Bisa menilai risiko bisnis</li> <li>• Bisa mengutarakan berbagai ide untuk inovasi bisnis</li> </ul>
		Data Specialist	<ul style="list-style-type: none"> <li>• Bisa membedakan Data, Informasi dan Knowledge</li> <li>• Bisa memilih teknologi penyimpanan data yang sesuai kebutuhan organisasi</li> <li>• Bisa membuat Tata Kelola Data menggunakan referensi dari DMBOK</li> <li>• Bisa mengetahui berbagai proses tata kelola data berdasarkan DMBOK</li> <li>• Bisa membedakan antara Informasi dan Knowledge</li> <li>• Bisa menjelaskan konsep manajemen Informasi</li> <li>• Bisa membedakan Kategori Knowledge</li> <li>• Bisa menyatakan fitur dari learning organization</li> </ul>
5	Development	Web Developer	<ul style="list-style-type: none"> <li>• Bisa menjelaskan pengembangan web front-end</li> <li>• Bisa mengoperasikan tools pengembangan web front-end</li> <li>• Bisa mendesain tampilan web front-end</li> <li>• Bisa mengembangkan aplikasi web front-end</li> <li>• Bisa memodifikasi template front-end untuk digunakan</li> <li>• Bisa menghasilkan aplikasi web front-end</li> <li>• Bisa membuat tampilan dan aplikasi web front-end</li> <li>• Bisa menjelaskan pengertian dan cara kerja PWA</li> <li>• Bisa mengoperasikan tools pengembangan aplikasi PWA</li> <li>• Bisa mengkombinasikan teknologi untuk menyusun aplikasi PWA</li> <li>• Bisa mengembangkan aplikasi PWA</li> <li>• Bisa menghasilkan aplikasi PWA</li> <li>• Bisa memodifikasi aplikasi web front-end menjadi PWA</li> </ul>

		Mobile Developer	<ul style="list-style-type: none"> <li>• Bisa mengembangkan aplikasi</li> <li>• Bisa membuat aplikasi untuk Sistem Operasi Android</li> <li>• Bisa menghasilkan aplikasi untuk digunakan pada perangkat Mobile Android</li> <li>• Bisa mendefinisikan kebutuhan dasar Lingkup Aplikasi</li> <li>• Bisa mendesain antar muka aplikasi</li> <li>• Bisa membuat form untuk aplikasi</li> <li>• Bisa memilih tampilan yang sesuai untuk aplikasi yang dibuat</li> <li>• Bisa menjelaskan keamanan aplikasi android</li> <li>• Bisa mengklasifikasikan jenis keamanan aplikasi</li> <li>• Bisa mengembangkan keamanan aplikasi</li> <li>• Bisa mendesain keamanan aplikasi</li> <li>• Bisa mendesain aplikasi back-end web api</li> <li>• Bisa menghasilkan aplikasi back-end web api</li> <li>• Bisa membedakan aplikasi untuk back-end web api dan front-end web</li> <li>• Bisa menyimpulkan penggunaan aplikasi monolitik dan back-end serta front-end web</li> <li>• Bisa mengembangkan back-end web api</li> <li>• Bisa mengkombinasikan kebutuhan lingkungan aplikasi dengan aplikasi yang dibuat</li> </ul>
		Web Developer Expert	<ul style="list-style-type: none"> <li>• Bisa menjelaskan penggunaan framework</li> <li>• Bisa mengoperasikan tools untuk menggunakan framework</li> <li>• Bisa mengenal elemen-elemen framework</li> <li>• Bisa mempertimbangkan penggunaan framework</li> <li>• Bisa membuat aplikasi front-end menggunakan framework</li> <li>• Bisa mengembangkan aplikasi front-end menggunakan framework</li> <li>•</li> </ul>

		Test Specialist	<ul style="list-style-type: none"> <li>• Bisa Mendefinisikan Proses-proses yang ada pada Software Development dan Software Testing</li> <li>• Bisa Menjelaskan proses yang dibutuhkan pada saat melakukan Software Testing</li> <li>• Bisa Mendaftarkan Input dan Output dari sebuah Software Test Plan</li> <li>• Bisa Mengidentifikasi kebutuhan, Tujuan dan Batasan Software Testing</li> <li>• Bisa Membuat Strategi Test Case untuk Software Testing di Dalam Perusahaan</li> <li>• Bisa mendefinisikan konsep Software Testing</li> <li>• Bisa mengoperasikan Tools untuk Static maupun Dynamic Testing</li> <li>• Bisa Memilih proses dan tools Software Testing sesuai jenis Aplikasi yang akan di test</li> <li>• Bisa menyiapkan langkah-langkah Software Testing</li> <li>• Bisa menghasilkan Dokumen hasil Software Testing</li> </ul>
		Digital Media Specialist	<ul style="list-style-type: none"> <li>• Bisa Mengidentifikasi kebutuhan Digital Marketing untuk keberhasilan Marketing Organisasi</li> <li>• Bisa Membuat perencanaan Digital Marketing</li> <li>• Bisa memilih Digital Channel untuk Digital Marketing</li> <li>• Bisa Mengkombinasikan Digital Channel yang digunakan Organisasi</li> <li>• Bisa menilai dan menganalisis keberhasilan Konversi Digital Marketing Organisasi</li> </ul>
6	Service & Operation	Technical Specialist	<ul style="list-style-type: none"> <li>• Bisa Menjelaskan Masalah jaringan dan isu-isu penting ke organisasi</li> <li>• Bisa Memilih Solusi Permasalahan Jaringan dan Optimalisasi Jaringan</li> <li>• Bisa Mengenal Permasalahan di jaringan Sesuai dengan OSI 7 Layer</li> <li>• Bisa Menyelesaikan masalah Keamanan Jaringan, Lambatnya Jaringan dan Optimalisasi Jaringan</li> </ul>

			<ul style="list-style-type: none"> <li>• Bisa Menentukan Solusi Permasalahan Sesuai dengan kebutuhan organisasi (QOS, Security, Monitoring Jaringan)</li> <li>• Bisa Memeriksa Keadaan dan performance jaringan apakah sudah sesuai dengan ekpektasi organisasi</li> <li>• Bisa Mengoperasikan Tool Monitoring System</li> <li>• Bisa Menguraikan Permasalahan dan kebutuhan optimalisasi jaringan sesuai dengan keadaan infrastruktur organisasi</li> <li>• Bisa Menyusun Perencanaan Jaringan (Pembagian Segmen, Design Logik dan Fisik Jaringan) dengan Tujuan optimalisasi jaringan</li> <li>• Bisa Membuat Konfigurasi jaringan sesuai dengan kebutuhan jaringan (QOS, Security, Monitoring Jaringan)</li> <li>• Bisa Menyimpulkan Kelemahan dan Isu isu jaringan yang ada di organisasinya</li> <li>• Bisa Merangking Masalah dan isu jaringan serta membuat prioritas solusi</li> <li>• Bisa Mengenali Bagaimana Cara Kerja Server Secara Mendalam (Arsitektur Server, Managemen Server, Hardisk dll)</li> <li>• Bisa Mengidentifikasi Masalah masalah pada server</li> <li>• Bisa Menentukan Kapasitas dan kemampuan Server dalam menyediakan layanan (Web Server, Database, Syslog, SSH dan FTP)</li> <li>• Bisa Memeriksa Masalah yang ada di server secara akurat (Top 5 Problem)</li> <li>• Bisa Menjelaskan Masalah server dan isu isu penting ke organisasi</li> <li>• Bisa Menentukan Solusi Permasalahan Server Sesuai dengan kebutuhan organisasi</li> <li>• Bisa Memeriksa Keadaan dan performance jaringan apakah sudah sesuai dengan ekpektasi organisasi</li> <li>• Bisa Mengoperasikan dan Monitoring Tool Monitoring System</li> </ul>
--	--	--	---

		<ul style="list-style-type: none"> <li>• Bisa Menguraikan Permasalahan dan kebutuhan optimalisasi Server</li> <li>• Bisa Membuat Konfigurasi Server untuk tujuan Optimalisasi Server (Tunning, Run Leve, SELinux, Firewall, File System Tunning)</li> <li>• Bisa Menyimpulkan Kelemahan dan Isu isu keamanan server yang ada di organisasinya</li> <li>• Bisa Merangking Masalah dan Isu Server serta membuat prioritas solusi</li> <li>• Bisa Membreakdown Masalah dan Berkomunikasi dengan Efektif dan Efisien</li> <li>• Bisa Membuat Database Permasalahan Semua Insident di Organisasi (Service Desk and Helpdesk Software)</li> <li>• Bisa Mendefinisikan dan berkomunikasi dengan baik kepada pengguna</li> <li>• Bisa Menentukan Solusi yang Relevan dengan Masalah yang dilaporkan</li> <li>• Bisa Mengidentifikasi Permasalahan dan Memberikan layanan kepada pengguna dengan baik</li> <li>• Bisa Mengkategorikan Level masalah yang di terima oleh Helpdesk/Service Desk</li> <li>• Bisa Mengklasifikasikan Masalah yang ada di organisasi</li> <li>• Bisa Mengutarakan Solusi dengan baik sesuai dengan SOP dan Aturan Intenal Organisasi</li> <li>• Bisa Menjelaskan Ruang Lingkup dan Tanggung Jawab Service Desk</li> <li>• Bisa Menyusun SOP dan dokumen Kerja</li> <li>• Bisa Merangking Masalah Berdasarkan Dokumen Internal Organisasi</li> </ul>
	Network Specialist	<ul style="list-style-type: none"> <li>• Bisa menyusun aset di Jaringan dan membuat konfigurasi sesuai dengan pembagian aset tersebut</li> <li>• Bisa Memilih Fitur Network yang cocok dengan kebutuhan organisasi Jaringan Sesuai dengan Kebutuhan Organisasi</li> </ul>

		<ul style="list-style-type: none"> <li>• Bisa Melihat Keadaan dan Monitoring Jaringan dengan NMS</li> <li>• Bisa Melihat Kebutuhan Jaringan dan Fitur yang ada di dalam Network</li> <li>• Bisa mengonfigurasi Jaringan dengan RouterOS Mikrotik (QOS, Firewall, Ip Management dll)</li> <li>• Bisa Memahami Konsep TCP/IP dan OSI (TCP, UDP, ICMP, ARP dan DHCP)</li> <li>• Bisa Menghubungkan semua komponen jaringan di organisasi (Routing Static dan Dynamic)</li> <li>• Bisa Memilih Feature mikrotik dan kebutuhan keamanan jaringan organisasi (VPN, QOS, Firewall dll)</li> <li>• Bisa mengonfigurasi Network apakah sudah sesuai rekomendasi keamanan atau tidak</li> <li>• Bisa mengonfigurasi Pengamanan Jaringan dengan firewall (Basic Security Filter, Mangle, Filter, Nat,Address-list)</li> <li>• Bisa mengonfigurasi Mekanisme Monitoring jaringan dan Network management (NMS, Userman dll)</li> <li>• Bisa mengonfigurasi Mekanisme Pertahanan Keamanan Wireless (Security Profile, Mac Limit, Mode AP, Hotspot Login)</li> <li>• Bisa Melihat Resiko Keamanan Jaringan (DHCP Starvation, Arp Poisoning, Netcut, DoS, SSH,Telnet Brute Force dll)</li> <li>• Bisa Melihat Resiko Keamanan jaringan dan efeknya terhadap organisasi</li> <li>• Bisa Melihat Resiko Keamanan jaringan dan Solusi Keamanan yang relevan</li> <li>• Bisa Membuat Security Perimeter Jaringan dengan menggunakan Mikrotik Tools (Firewall, Hardening Mikrotik, Anti Ddos dll)</li> </ul>
	System Administrator	<ul style="list-style-type: none"> <li>• Bisa Memilih Distro yang sesuai untuk kebutuhan Organisasi</li> <li>• Bisa Mengenali Jenis dan Varian Linux System</li> </ul>

			<ul style="list-style-type: none"> <li>• Bisa Menjelaskan Komponen Sistem Operasi Linux</li> <li>• Bisa Mengoperasikan Linux dan Berinteraksi dengan command Basic Linux (File Managemen, Proses Managemen, Software Managemen dll)</li> <li>• Bisa Mendemonstrasikan Proses Instalasi Linux</li> <li>• Bisa Membuat Shell Script Untuk Kebutuhan Otomasi System di Linux</li> <li>• Bisa Mengenali Berbagai macam jenis server Linux (Apache, Mysql, Syslog, SMB, DNS Server dll)</li> <li>• Bisa Menjelaskan Jenis dan Varian Linux Server</li> <li>• Bisa Menyiapkan kebutuhan hardware dan software Linux Server</li> <li>• Bisa Mencocokkan Kebutuhan Linux Server dan Pilihan Service (Layanan Server Linux)</li> <li>• Bisa Mengoperasikan Linux Server Harian</li> <li>• Bisa Membuat Shell Script Untuk Kebutuhan Otomasi System di Linux</li> <li>• Bisa Menyimpulkan Solusi Teknologi Server yang sesuai ( Replikasi, Backup Restore dll)</li> </ul>
		Big Data Specialist	<ul style="list-style-type: none"> <li>• Bisa Menjelaskan tentang big data dan ekosistemnya</li> <li>• Bisa Mengklasifikasikan jenis-jenis data dan cara pengolahannya</li> <li>• Bisa Memilih jenis algoritma machine learning yang tepat untuk masalah yang dihadapi</li> <li>• Bisa Mengoperasikan alat bantu data analytic</li> <li>• Bisa Membuat rancangan alur pemrosesan data</li> <li>• Bisa Menghasilkan kesimpulan dari data yang dimiliki</li> <li>• Bisa Menjelaskan big data dan peran teknologi hadoop dalam big data</li> <li>• Bisa Memilih perangkat lunak sesuai dengan data yang dimiliki</li> </ul>

			<ul style="list-style-type: none"> <li>• Bisa Mengoperasikan perangkat lunak hadoop dan pendukungnya</li> <li>• Bisa Memodifikasi data yang didapatkan menjadi data yang dapat diproses hadoop</li> <li>• Bisa Membuat perintah /script untuk transformasi data</li> <li>• Bisa Menggambarkan cara kerja hadoop</li> <li>• Bisa Menyiapkan perangkat lunak pendukung hadoop</li> </ul>
7	Support	Cyber Security Specialist	<ul style="list-style-type: none"> <li>• Bisa Mengklasifikasikan Alat-alat yang digunakan untuk melakukan pentest web app</li> <li>• Bisa Mengoperasikan Alat pentest web</li> <li>• Bisa Memeriksa Kerentanan yang terdapat didalam aplikasi web</li> <li>• Bisa Menjelaskan Langkah langkah melakukan pentest aplikasi web</li> <li>• Bisa Mendemonstrasikan Cara melakukan pentest aplikasi web</li> <li>• Bisa Menilai Kerentanan yang terdapat didalam aplikasi web</li> <li>• Bisa Menyiapkan Alat pentest web</li> <li>• Bisa Mengenali Jenis kerentanan dalam aplikasi web</li> <li>• Bisa Membandingkan Kegiatan pentes yang legal dan tidak legal</li> <li>• Bisa Membuat Laporan pentest web menggunakan template aplikasi</li> <li>• Bisa Mengklasifikasikan kode program yang aman</li> <li>• Bisa Mengkategorikan penyebab kerentanan didalam kode program</li> <li>• Bisa Menyiapkan development environment</li> <li>• Bisa Memberikan contoh Kode program yang aman dan kode program yang tidak aman</li> <li>• Bisa Mengkombinasikan library beberapa library untuk mengamankan kode program</li> <li>• Bisa Memodifikasi Hak akses user database</li> <li>• Bisa Menjelaskan Pengertian Komputer Forensic</li> </ul>

			<ul style="list-style-type: none"> <li>• Bisa Mengenali komponen komputer forensik</li> <li>• Bisa Mendefinisikan komponen barang bukti</li> <li>• Bisa Mengidentifikasi barang bukti digital</li> <li>• Bisa Membedakan Barang bukti digital yang rentan dan tidak rentan</li> <li>• Bisa Menyiapkan laboratorium digital</li> <li>• Bisa Mendemonstrasikan cara mengumpulkan barang bukti digital</li> <li>• Bisa Memberikan contoh barang bukti digital</li> <li>• Bisa Menghasilkan Barang bukti digital</li> <li>• Bisa Mengoperasikan software forensik</li> <li>• Bisa Membuat laporan digital forensik</li> </ul>
		Data Center Specialist	<ul style="list-style-type: none"> <li>• Bisa Menjelaskan konsep pusat data</li> <li>• Bisa Mendefinisikan pusat data</li> <li>• Bisa Mengidentifikasi persyaratan ideal pusat data</li> <li>• Bisa Mengkategorikan kelas/tier/level/strata pusat data sesuai standard pusat data</li> <li>• Bisa Menilai kondisi pusat data saat ini bila telah memiliki</li> <li>• Bisa Menyusun perencanaan membangun pusat data</li> <li>• Bisa Menggambarkan kebutuhan-kebutuhan membangun pusat data</li> <li>• Bisa Menjelaskan pentingnya mengikuti standarisasi pusat data</li> <li>• Bisa Menjelaskan konsep pusat data</li> <li>• Bisa Mendefinisikan konsep layanan pada pusat data</li> <li>• Bisa Mengkategorikan kelas/tier/level/strata pusat data sesuai standard layanan pusat data</li> <li>• Bisa Mengoperasikan pusat data sesuai harapan pada kategori layanan pusat data</li> <li>• Bisa Menyusun perencanaan tindakan pendukung layanan</li> <li>• Bisa Menentukan kebutuhan untuk mendukung layanan pusat data</li> <li>• Bisa Membuat SOP komponen pendukung layanan pusat data</li> </ul>

			<ul style="list-style-type: none"> <li>• Bisa Mengorganisasikan tindakan yang diperlukan dalam penyelesaian kendala layanan pusat data</li> </ul>
		Virtualization Specialist	<ul style="list-style-type: none"> <li>• Bisa Menjelaskan Konsep SDDC</li> <li>• Bisa Menjelaskan pengertian Virtualisasi</li> <li>• Bisa Mengoperasikan vshpere client, web client, dan fitur-fitur dasar vmware vsphere</li> <li>• Bisa Mengidentifikasi kebutuhan membangun SDDC</li> <li>• Bisa Membuat Virtual mesin</li> <li>• Bisa Menjelaskan konsep High Availability</li> <li>• Bisa Membandingkan tradisional datacenter dan modern datacenter</li> <li>• Bisa Mendemonstrasikan aktifitas modern datacenter secara general</li> </ul>
		Cloud Specialist	<ul style="list-style-type: none"> <li>• Bisa menjelaskan cloud computing dan virtualisasi</li> <li>• Bisa mengklasifikan jenis layanan Cloud (IaaS, PaaS, SaaS)</li> <li>• Bisa menjelaskan layanan cloud (komputasi, penyimpanan, database)</li> <li>• Bisa mengoperasikan layanan komputasi</li> <li>• Bisa mengoperasikan layanan penyimpanan</li> <li>• Bisa mengoperasikan layanan database</li> </ul>
		Operation Center Specialist	<ul style="list-style-type: none"> <li>• Bisa menjelaskan peran dan fungsi NOC</li> <li>• Bisa mengidentifikasi komponen-komponen NOC</li> <li>• Bisa mengoperasikan NMS</li> <li>• Bisa menjelaskan peran dan fungsi SOC</li> <li>• Bisa mengidentifikasi komponen-komponen SOC</li> <li>• Bisa mengoperasikan tools SIEM</li> </ul>

## BAB VI

### KEBUTUHAN TIK

#### 6.1 Daftar Kebutuhan TIK ( 2022-2026 )

Tabel 14 : Daftar Kebutuhan TIK dan Timeline

No	Kategori	Kebutuhan TIK	2022	2023	2024	2025	2026
<b>1</b>	<b>Infrastruktur</b>	Pembuatan Fasilitas Data Center bersertifikasi pada Rated 3 TIA 942/Tier 3			🎯	🎯	🎯
		Peremajaan dan Pengembangan jaringan interkoneksi tertutup antar OPD sampai ke Kelurahan	🎯	🎯	🎯	🎯	🎯
		Sistem Penghubung Layanan		🎯	🎯	🎯	🎯
		Implementasi Sistem Manajemen Backup Data secara terpusat	🎯	🎯	🎯	🎯	🎯
<b>2</b>	<b>Aplikasi</b>	Layanan Ekonomi	🎯	🎯	🎯	🎯	🎯
		Layanan Industri					
		Layanan Perdagangan		🎯	🎯	🎯	🎯
		Layanan Pertanian		🎯	🎯	🎯	🎯
		Layanan Investasi		🎯	🎯	🎯	🎯
		Layanan Koperasi					
		Layanan Usaha Kecil dan Menengah		🎯	🎯	🎯	🎯
		Layanan Pariwisata		🎯	🎯	🎯	🎯
Layanan Perizinan dan Akreditasi							

	Layanan Pekerjaan Umum		🎯	🎯	🎯	🎯
	Layanan Transportasi	🎯	🎯	🎯	🎯	🎯
	Layanan Perumahan		🎯	🎯	🎯	🎯
	Layanan Pertanahan					
	Layanan Kependudukan	🎯	🎯	🎯	🎯	🎯
	Layanan Kesehatan	🎯	🎯	🎯	🎯	🎯
	Layanan Sosial	🎯	🎯	🎯	🎯	🎯
	Layanan Pemberdayaan Perempuan					
	Layanan Keamanan		🎯	🎯	🎯	🎯
	Layanan Pendidikan	🎯	🎯	🎯	🎯	🎯
	Layanan Ketenagakerjaan	🎯	🎯	🎯	🎯	🎯
	Layanan Ilmu Pengetahuan		🎯	🎯	🎯	🎯
	Layanan Teknologi	🎯	🎯	🎯	🎯	🎯
	Layanan Pemuda			🎯	🎯	🎯
	Layanan Olahraga			🎯	🎯	🎯
	Layanan Pertambangan					
	Layanan Lingkungan Hidup	🎯	🎯	🎯	🎯	🎯
	Layanan Agama					
	Layanan Kebudayaan				🎯	🎯
	Layanan Informasi	🎯	🎯	🎯	🎯	🎯
	Layanan Komunikasi	🎯	🎯	🎯	🎯	🎯
	Portal Aplikasi Terpadu Publik Adanya portal pusat layanan service desk terdiri dari layanan pengguna (keluhan/masalah, permintaan/perubahan layanan), layanan infrastruktur (memastikan operasional layanan berjalan (perbaikan kerusakan))					

		Single Sign On		🎯	🎯	🎯	🎯
<b>3</b>	<b>Data</b>	Standar Data untuk SDI	🎯	🎯	🎯	🎯	🎯
		Format Interoperability untuk SDI	🎯	🎯	🎯	🎯	🎯
		Basis Data tabular per sektor	🎯	🎯	🎯	🎯	🎯
<b>4</b>	<b>Keamanan Informasi</b>	Kebijakan keamanan informasi <ul style="list-style-type: none"> <li>- Pembuatan SMKI dengan referensi framework Keamanan Informasi dengan ISO 27001</li> <li>- Penyusunan SOP Pengembangan dan Pengujian Sistem Informasi yang Aman</li> <li>- Penyusunan kebijakan, standar dan SOP Keamanan Informasi</li> <li>- Penyusunan SLA dan SOP Pelayanan Data, Keamanan Informasi, Jaringan, Server dan Perangkat</li> </ul>		🎯	🎯	🎯	🎯
		Pembuatan Perimeter Security untuk Jaringan Server		🎯	🎯	🎯	🎯
		Penambahan IDS (Intrusion Detection System) / IPS (Intrusion Prevention System)		🎯	🎯	🎯	🎯
		Penerapan VPN ( <i>Virtual Private Network</i> ) untuk akses jaringan secara jarak jauh		🎯	🎯	🎯	🎯
		Penerapan sistem SIEM ( <i>Security Information and Event Management</i> )		🎯	🎯	🎯	🎯
		Pemantauan server dengan NMS ( <i>Network Monitoring System</i> )		🎯	🎯	🎯	🎯
		Pelaksanaan Asesmen Kerentanan dan Uji Penetrasi ( <i>Vulnerability Assessment and Penetration Test</i> ) terhadap Sistem Informasi secara berkala		🎯	🎯	🎯	🎯
		Pelaksanaan Audit Keamanan Informasi secara berkala (Internal dan Eksternal)	🎯	🎯	🎯	🎯	🎯

		Penyediaan IT Help Desk / Service Desk		🎯	🎯	🎯	🎯
<b>5</b>	<b>SDM</b>	Pelatihan & Sertifikasi SDM Tata Kelola Untuk Role ( <i>Business Analyst, IT Service Manager, Enterprise Architect, GCIO</i> )		🎯	🎯	🎯	🎯
		Pelatihan & Sertifikasi SDM Infrastruktur Untuk Role ( <i>Data Center Specialist, Cloud Specialist, Network Specialist, System Administrator, Technical Specialist, Operation Center Specialist</i> )		🎯	🎯	🎯	🎯
		Pelatihan & Sertifikasi SDM Keamanan Informasi Untuk Role ( <i>Cyber Security Manager, Cyber Security Specialist, Operation Center Specialist</i> )		🎯	🎯	🎯	🎯
		Pelatihan & Sertifikasi SDM Pengembangan Aplikasi Untuk Role ( <i>Web Developer, System Analyst, Database Administrator</i> )	🎯	🎯	🎯	🎯	🎯
		Pelatihan & Sertifikasi SDM Big Data Untuk Role ( <i>Role Big Data Specialist, Data Specialist</i> )		🎯	🎯	🎯	🎯
		Pelatihan & Sertifikasi SDM Literasi Digital untuk seluruh ASN ( <i>Digital Skill - Digital Worker</i> )		🎯	🎯	🎯	🎯

## BAB VII

### PENUTUP

Keinginan Pemerintah Daerah untuk menjadi organisasi yang modern, akibat tuntutan masyarakat dan perkembangan teknologi, membuat fungsi dan peran teknologi informasi menjadi penting dalam keberlangsungan organisasi. Fungsi dan peran teknologi informasi tersebut adalah :

1. Fungsi Operasional
2. Fungsi Pengawasan dan Kontrol
3. Fungsi Perencanaan dan Pengambil Keputusan
4. Fungsi Komunikasi
5. Fungsi Interorganisasi

Hal tersebut juga didukung oleh beberapa kebijakan yang mendorong dan memayungi penggunaan teknologi informasi di pemerintahan , antara lain SPBE, Smart City dan Satu Data Indonesia. Faktor regulasi, anggaran dan sumber daya manusia tentu saja menjadi enabler bagi terlaksananya penggunaan teknologi informasi di pemerintah. Kebutuhan teknologi informasi dapat dikategorikan sebagai berikut :

1. Aplikasi
2. Infrastruktur
3. Data
4. Keamanan Informasi
5. SDM

Dengan menggunakan latar belakang dan Analisa yang tepat, maka dapat ditemukan kebutuhan sumber daya TIK yang akan membantu menjadi enabler bagi pencapaian visi misi pembangunan kota magelang yang tertera dalam RPJMD 2021 -2026



