

eduparx

inixindo  
JOGJA

LINDUNGI DATA DARI SERANGAN CYBER

# MANAJEMEN RISIKO & KEPATUHAN PUSAT DATA

eduparx.id



# CITRA ARFANUDIN

TRAINING, SERTIFIKASI & KONSULTAN IT

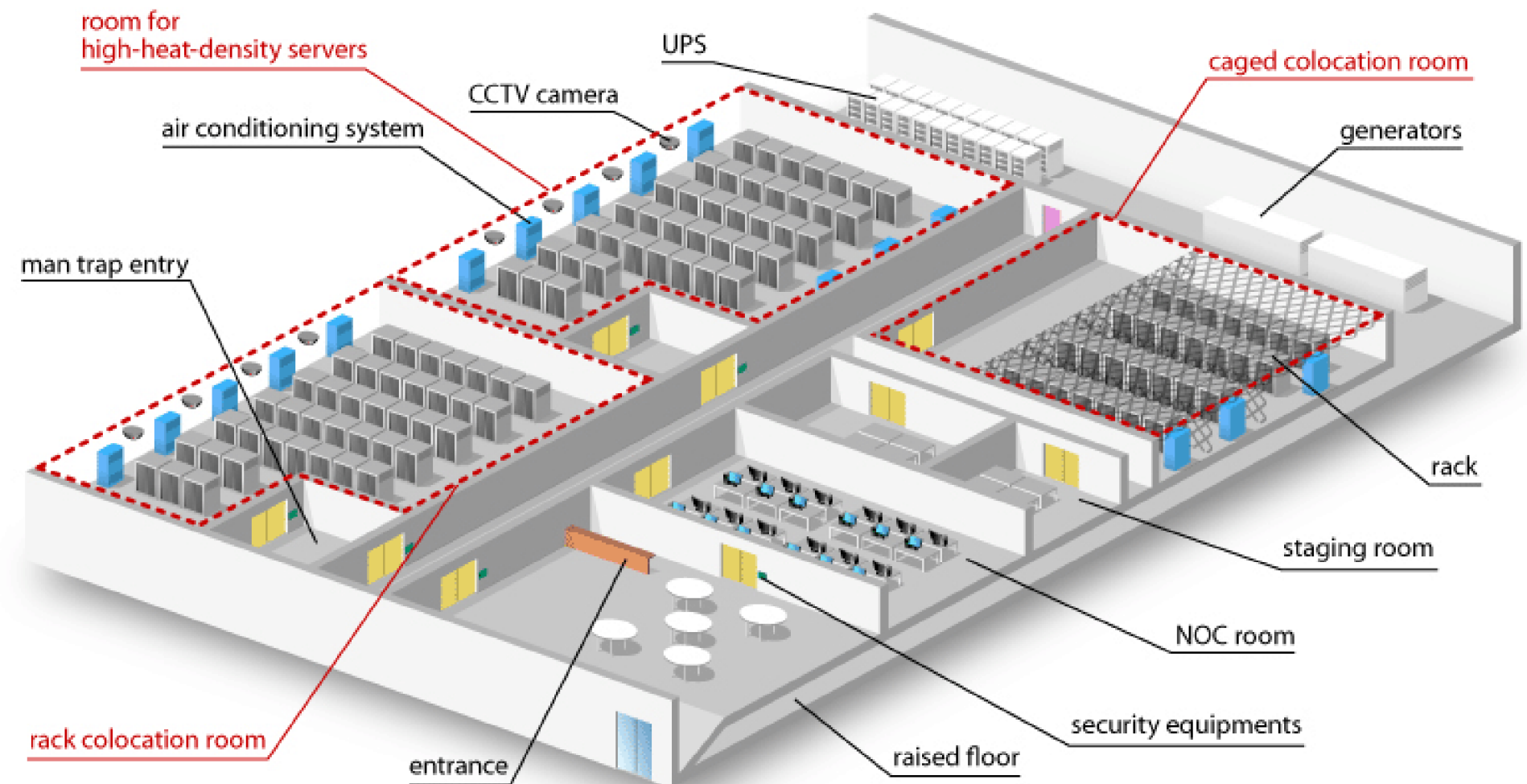


## ASET VITAL

# PUSAT DATA

Bagi perusahaan, organisasi, dan pemerintah, **Pusat Data** adalah **Aset Vital** yang mendukung berjalannya proses bisnis, transformasi digital dan inovasi.

Banyak organisasi **tidak sadar** akan **risiko** yang ada di pusat datanya dengan banyaknya ekpektasi yang ada terhadap pusat data.





# EKSPEKTASI PUSAT DATA 2024

1

## Sumber Energi Terbarukan

Mengurangi emisi karbon dengan menggunakan energi terbarukan dan sumber berkelanjutan lainnya.

2

## Solusi Pendinginan Canggih

Peningkatkan efisiensi dan keandalan pusat data dengan teknologi pendinginan yang canggih

3

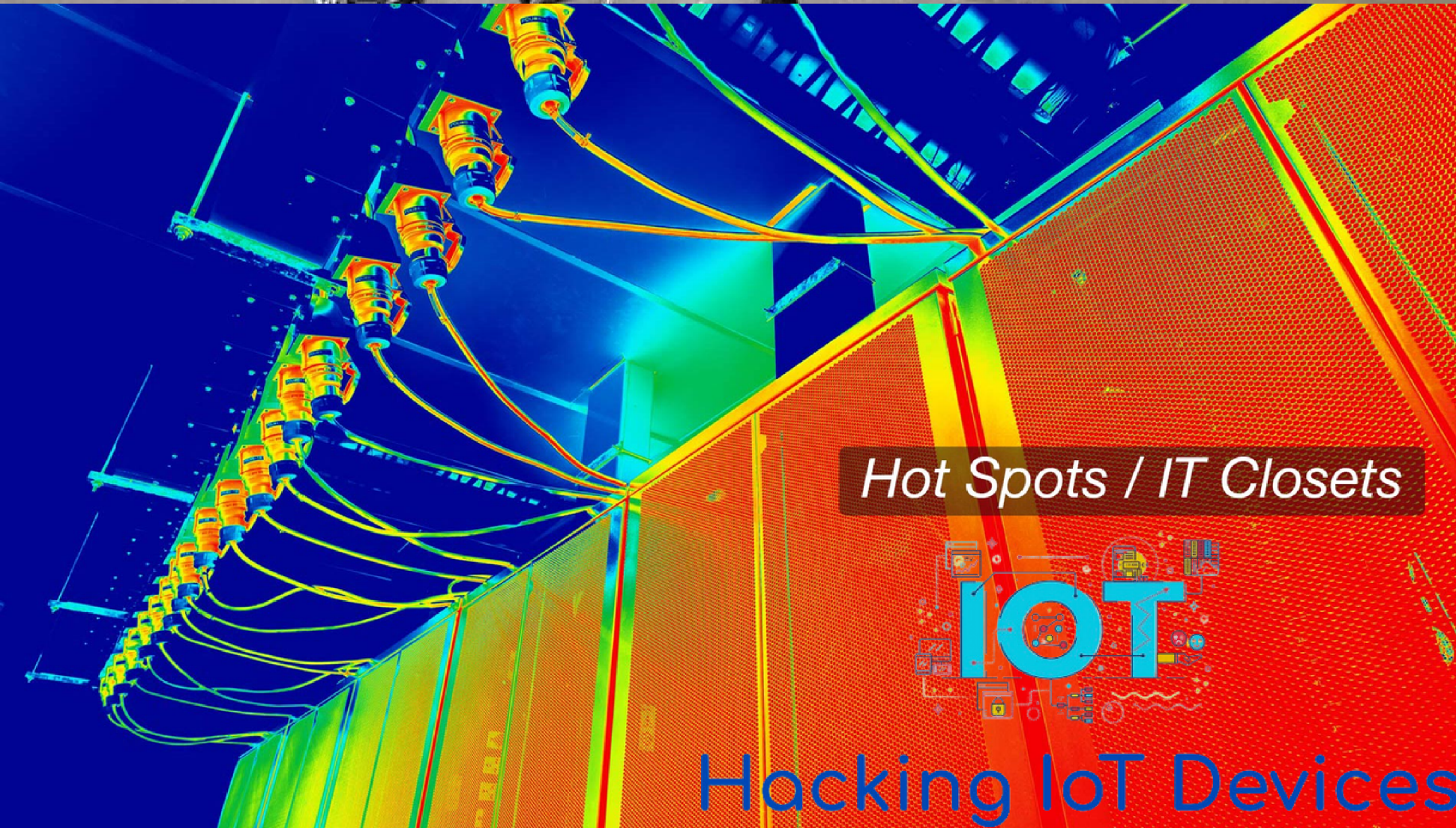
## Inovasi dalam Efisiensi Energi

Teknologi terbaru untuk mengurangi konsumsi energi dan biaya operasional pusat data.

4

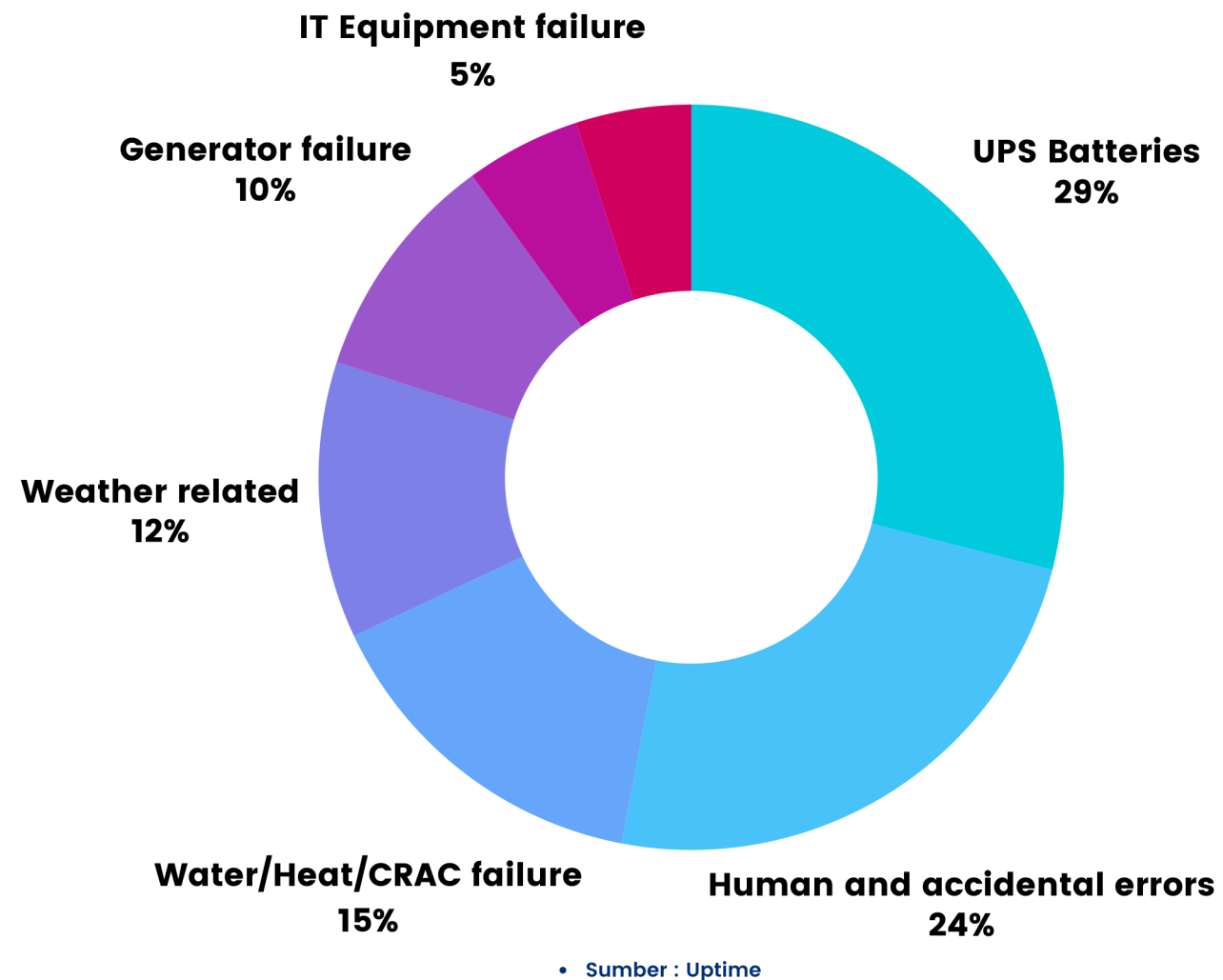
## Kepatuhan Regulasi

Pemenuhan Standar Nasional Indonesia terkait desain Pusat Data dan manajemen Pusat Data;



## Downtime PUSAT DATA

Downtime menyebabkan kerugian finansial, kehilangan data, Penurunan produktivitas, reputasi, dan meningkatkan risiko keamanan organisasi



Baterai UPS Bermasalah,  
Server mati, Data hilang,  
operasional terganggu.

**29 %**

UPS Batteries

Kurangnya pelatihan  
keselamatan dan  
operasional Pusat Data

**24 %**

Human & Accident

Suhu ruang server naik drastis,  
mendekati batas berbahaya.  
Kebocoran air terdeteksi.

**15 %**

Water/Heat/CRAC

# PUSAT DATA STANDAR

Pedoman dan spesifikasi infrastruktur, operasi, dan keamanan pusat data memenuhi kriteria keandalan, efisiensi, dan keamanan.

|                                         | Uptime                       | TIA-942                                                                                                                | BICSI-002                                                                                              | SS507                                                                                                  | EN-50600                                                                                                               | SNI-8799                                                                                                               |
|-----------------------------------------|------------------------------|------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| Origin                                  | USA                          | USA                                                                                                                    | USA                                                                                                    | Singapore                                                                                              | Europe                                                                                                                 | Indonesia                                                                                                              |
| Main scope of Topology                  | - Electrical<br>- Mechanical | - Electrical<br>- Mechanical<br>- Architectural<br>- Telecom<br>- Site Location<br>- Safety & Security<br>- Efficiency | - Electrical<br>- Mechanical<br>- Architectural<br>- Telecom<br>- Site Location<br>- Safety & Security | - Electrical<br>- Mechanical<br>- Architectural<br>- Telecom<br>- Site Location<br>- Safety & Security | - Electrical<br>- Mechanical<br>- Architectural<br>- Telecom<br>- Site Location<br>- Safety & Security<br>- Efficiency | - Electrical<br>- Mechanical<br>- Architectural<br>- Telecom<br>- Site Location<br>- Safety & Security<br>- Efficiency |
| Type of Conformity                      | Tier (I-IV)                  | Rated (1-4)                                                                                                            | Class (FO-F4)                                                                                          | Pass / Fail                                                                                            | Class (1-4)                                                                                                            | Strata (1-4)                                                                                                           |
| Detail Spec public. Available           | Guideline or Standard        | YES (Standard Document)                                                                                                | YES (Standard Document)                                                                                | YES (Standard Document)                                                                                | YES (Standard Document)                                                                                                | YES (Standard Document)                                                                                                |
| Type of organisation                    | Commercial                   | Non-profit                                                                                                             | Non-profit                                                                                             | Non-profit                                                                                             | Non-profit                                                                                                             | Non-profit                                                                                                             |
| Official Standard Accreditation Process | NO                           | YES - ANSI                                                                                                             | YES - ANSI                                                                                             | YES - Spring                                                                                           | YES - EN, CENELEC                                                                                                      | YES - BSN                                                                                                              |
| Official Standard                       | NO                           | YES                                                                                                                    | YES                                                                                                    | YES                                                                                                    | YES                                                                                                                    | YES                                                                                                                    |
| Certificate Data Center                 | YES                          | YES (EPI)                                                                                                              | NO                                                                                                     | YES                                                                                                    | NO                                                                                                                     | NO                                                                                                                     |
| Auditors                                | Uptime Only                  | Multiple Organisations                                                                                                 | n/a                                                                                                    | Multiple Organisations                                                                                 | n/a                                                                                                                    | n/a                                                                                                                    |



# SNI 8799 – Series

Standar Nasional Indonesia yang berkaitan dengan pusat data yang dibuat oleh Badan Standarisasi Nasional (BSN).

Standar ini mencakup berbagai aspek teknis, manajemen, dan audit untuk memastikan pusat data di Indonesia memenuhi kriteria keandalan, efisiensi, dan keamanan yang tinggi

## **SNI 8799 – 1** **2023**

Spesifikasi teknis pusat data  
Spesifikasi teknis pusat data untuk desain fisik, pengelolaan termal, listrik, dan keamanan.

## **SNI 8799 – 2** **2023**

Sistem manajemen pusat data mencakup prosedur operasional, manajemen risiko, dan perawatan.

## **SNI 8799 – 3** **2023**

Panduan audit pusat data untuk evaluasi kepatuhan teknis dan sistem manajemen.

PUSAT DATA

# MANAJEMEN RISIKO

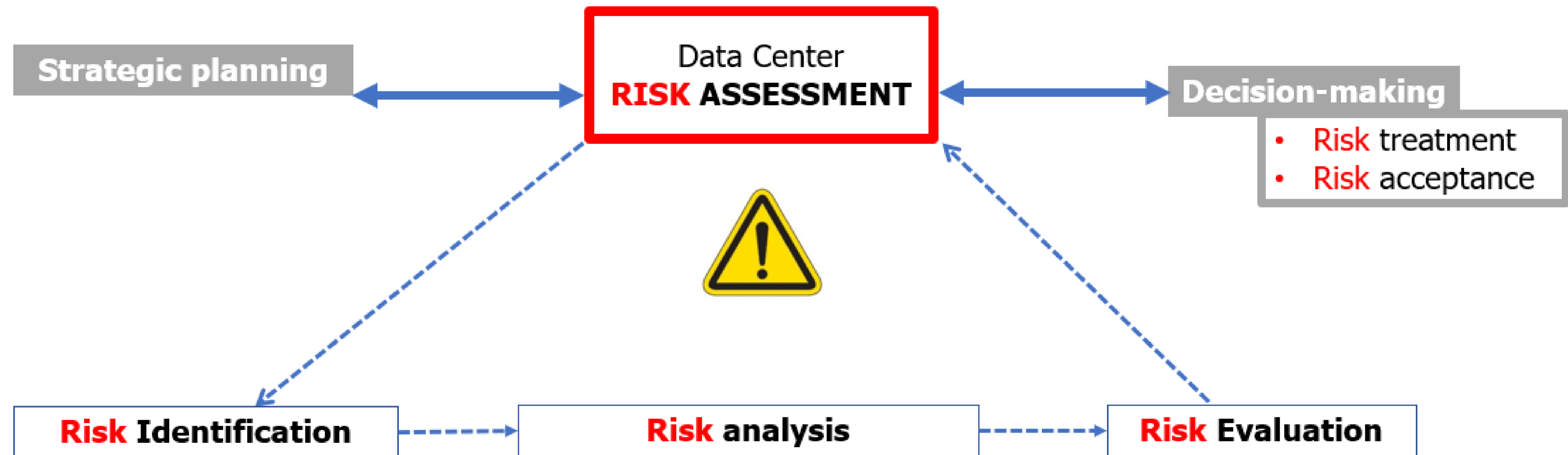
Penyelenggara pusat data harus menetapkan, mengimplementasikan, memelihara, dan meningkatkan secara berkelanjutan sistem manajemen risiko nya

## SNI 8799 – 2

| No | Persyaratan             | Strata 1       | Strata 2       | Strata 3       | Strata 4       |
|----|-------------------------|----------------|----------------|----------------|----------------|
| 1. | Penerapan SNI ISO 31000 | Dipersyaratkan | Dipersyaratkan | Dipersyaratkan | Dipersyaratkan |



# DATA CENTER RISK ASSESSMENT FRAMEWORK



# Risk Frameworks Management

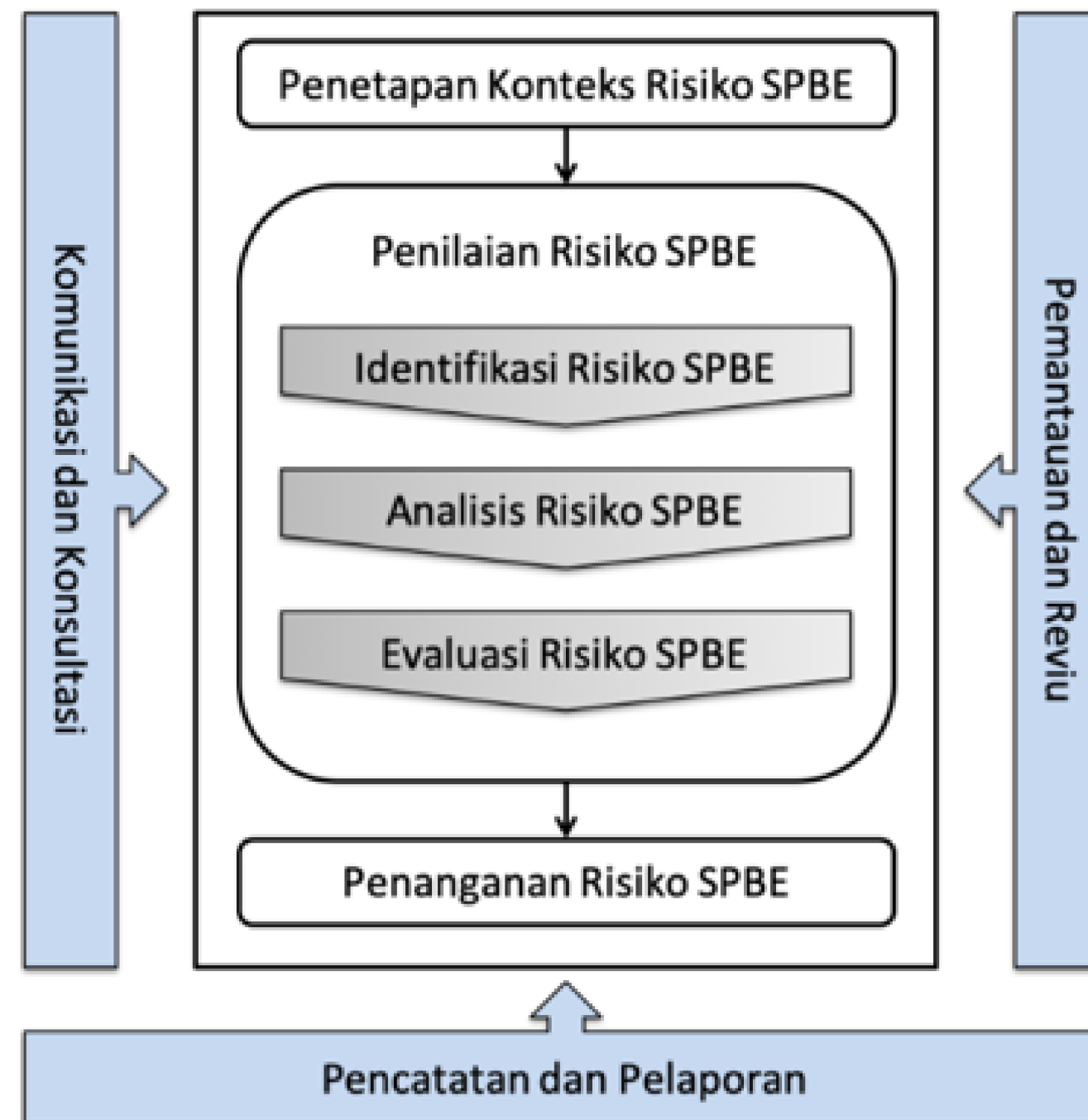


## RISK MANAGEMENT

# ISO 31000

Standar panduan umum dan prinsip untuk mengidentifikasi, mengevaluasi, dan mengelola risiko organisasi.

ISO 31000 memberikan kerangka kerja untuk mengelola risiko secara sistematis dan efektif



## Komunikasi & Konsultasi

Melibatkan semua pihak terkait dalam diskusi risiko dan strategi mitigasi.

## Konteks Risiko

Ruang lingkungan internal dan eksternal yang mempengaruhi pusat data

## Penilaian Risiko

Identifikasi, analisis, & evaluasi risiko untuk mengelola dan mengurangi risiko

## Penanganan Risiko

Pemilihan strategi untuk mengurangi atau mengelola risiko.

## Pemantauan & Reviu

Pemantauan dan Peninjauan risiko serta efektivitas strategi mitigasi secara berkala.

## Pencatatan & Pelaporan

Dokumentasi komunikasi, temuan, dan strategi penilaian risiko kepada pemangku kepentingan

# Konteks Risiko

## STAKEHOLDER

| No | Nama Unit/Instansi                      | Hubungan                                                                       |
|----|-----------------------------------------|--------------------------------------------------------------------------------|
| 1  | Badan Siber dan Sandi Negara            | Penyedia layanan repositori data evaluasi                                      |
| 2  | BRIN - Badan Riset dan Inovasi Nasional | Lembaga yang mengkaji masalah-masalah teknologi secara mendalam dan menyeluruh |

## ATURAN TERKAIT

| No | Nama Peraturan                                                                                                                                                                         | Amanat                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE)                                                                                          | <p>Pasal 42</p> <p>Layanan SPBE terdiri atas:</p> <p>a. Layanan administrasi pemerintahan berbasis elektronik; dan</p> <p>b. Layanan publik berbasis elektronik.</p> <p>Layanan administrasi pemerintahan berbasis elektronik sebagaimana dimaksud pada ayat (1) huruf a merupakan Layanan SPBE yang mendukung tata laksana internal birokrasi dalam rangka meningkatkan kinerja dan akuntabilitas pemerintah di Kementerian Pertanian.</p> |
| 2  | Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia Nomor 5 Tahun 2020 Tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik | <p>Pasal 3</p> <p>Evaluasi mandiri Sistem Pemerintahan Berbasis Elektronik pada Kementerian Pertanian sebagaimana dimaksud dalam Pasal 2 huruf a dikoordinasikan oleh Sekretaris pada Kementerian Pertanian atau pejabat yang memimpin unit sekretariat.</p>                                                                                                                                                                                |
| 3  | Peraturan Bupati (PERBUP) Kabupaten Kendal Nomor 57 Tahun 2023 tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik Di Lingkungan Pemerintah Kabupaten Kendal  | <p>Pasal 18</p> <p>(1) Manajemen risiko sebagaimana dimaksud dalam Pasal 2 ayat (3) huruf a dilakukan oleh setiap Perangkat Daerah.</p> <p>(2) Setiap Perangkat Daerah harus menyusun dokumen manajemen risiko atau daftar risiko (risk register) dengan substansi meliputi:</p> <p>(3) inventarisasi aset SPBE;</p> <p>(4) identifikasi ancaman dan kerentanan keamanan terhadap aset SPBE;</p>                                            |

## ISU INTERNAL EKTERNAL

| No | I/E* | Deskripsi Isu                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | E    | Mulai banyaknya ancaman cyber yang berpotensi mengganggu kelangsungan operasional Aplikasi Internal dan mengingat Surat Direktur Jenderal Dukcapil Kemendagri No 470/15192/Duckapil berkaitan dengan akses data kependudukan dan kewajiban, Pemenuhan terhadap Peraturan BSSN No.08 tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik dan Pemenuhan UU Nomor 27 Tahun 2022 mengenai Pelindungan Data Pribadi sehingga Top Management mengharuskan untuk menerapkan Sistem Manajemen Keamanan Informasi (SMKI) berbasis ISO/IEC 27001:2022 dan Penerapan |
| 2  | E    | Pemberian informasi yang lengkap dan jelas terkait apa saja yang harus dilakukan termasuk terkait apa yang boleh dan tidak boleh dilakukan dalam lingkup penerapan SMKI                                                                                                                                                                                                                                                                                                                                                                                                            |
| 3  | I    | Masih minimnya pemahaman personil internal terkait pengamanan data/ informasi Aplikasi internal sehingga kerentanan ini bisa memperbesar risiko terjadinya gangguan terkait munculnya ancaman cyber yang relevan.                                                                                                                                                                                                                                                                                                                                                                  |
| 4  | E    | Pelanggan juga menginginkan adanya ketersediaan layanan aplikasi dan pengendalian keamanan informasi yang relevan.                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

# Penilaian Risiko

## KATEGORI ASET

| No | Tipe Aset                  |
|----|----------------------------|
| 1  | Perangkat Keras (Hardware) |
| 2  | Perangkat Lunak (Software) |
| 3  | Infrastruktur Fisik        |
| 4  | Data                       |
| 5  | Sumber Daya Manusia        |
| 6  | Sistem Keamanan            |
| 7  | Jaringan Telekomunikasi    |

## KATEGORI RISIKO

| No | Tipe Risiko                |
|----|----------------------------|
| 1  | Risiko Fisik               |
| 2  | Risiko Lingkungan          |
| 3  | Risiko Teknologi           |
| 4  | Risiko Keamanan Siber      |
| 5  | Risiko Operasional         |
| 6  | Risiko Keuangan            |
| 7  | Risiko Kepatuhan           |
| 8  | Risiko Reputasi            |
| 9  | Risiko Penyedia Layanan    |
| 10 | Risiko Pasokan Listrik     |
| 11 | Risiko Jaringan            |
| 12 | Risiko Sumber Daya Manusia |
| 13 | Risiko Proyek              |
| 14 | Risiko Keamanan Fisik      |
| 15 | Risiko Kebijakan           |
| 16 | Risiko Pemeliharaan        |

## MATRIKS ANALISIS RISIKO

| Matriks Analisa Risiko 5 x 5 |   |                                        | Level Dampak            |                                   |                                  |                            |                           |
|------------------------------|---|----------------------------------------|-------------------------|-----------------------------------|----------------------------------|----------------------------|---------------------------|
|                              |   |                                        | 1                       | 2                                 | 3                                | 4                          | 5                         |
|                              |   |                                        | Tidak Signifikan (<20%) | Kurang Signifikan (20% s.d < 40%) | Cukup Signifikan (40% s.d < 60%) | Signifikan (60% s.d < 80%) | Sangat Signifikan (>=80%) |
| Level Kemungkinan            | 5 | Hampir Tidak Terjadi (X < 2 kali)      | 9                       | 15                                | 18                               | 23                         | 25                        |
|                              | 4 | Jarang Terjadi (2 ≤ X ≤ 5 kali)        | 6                       | 12                                | 16                               | 19                         | 24                        |
|                              | 3 | Kadang-Kadang Terjadi (6 ≤ X ≤ 9 kali) | 4                       | 10                                | 14                               | 17                         | 22                        |
|                              | 2 | Sering Terjadi (10 ≤ X ≤ 12 kali)      | 2                       | 7                                 | 11                               | 13                         | 21                        |
|                              | 1 | Hampir Pasti Terjadi (> 12 kali)       | 1                       | 3                                 | 5                                | 8                          | 20                        |

## LEVEL RISIKO

| Level Risiko |               | Rentang Besaran Risiko | Keterangan Warna |
|--------------|---------------|------------------------|------------------|
| 1            | Sangat Rendah | 1-5                    | Biru             |
| 2            | Rendah        | 6-10                   | Hijau            |
| 3            | Sedang        | 11-15                  | Kuning           |
| 4            | Tinggi        | 16-20                  | Jingga           |
| 5            | Sangat Tinggi | 21-25                  | Merah            |

# Penilaian & Penanganan Risiko

| PROBABILITY   1 – 5 | IMPACT   1 – 16   | PI SCORES   1 – 80 |
|---------------------|-------------------|--------------------|
| 1 - RARE            | 1 - INSIGNIFICANT | 1 – 2 • NEGUGIBLE  |
| 2 - UNLIKELY        | 2 - MINOR         | 3 – 8 • LOW        |
| 3 - POSSIBLE        | 4 - MODERATE      | 10 – 16 • MEDIUM   |
| 4 - LIKELY          | 8 - MAJOR         | 20 – 32 • HIGH     |
| 5 - ALMOST CERTAIN  | 16 - SEVERE       | 40 – 80 • EXTREME  |

|        |    | PROBABILITY |    |    |    |    |
|--------|----|-------------|----|----|----|----|
|        |    | 1           | 2  | 3  | 4  | 5  |
| IMPACT | 1  | 1           | 2  | 3  | 4  | 5  |
|        | 2  | 2           | 4  | 6  | 8  | 10 |
|        | 4  | 4           | 8  | 12 | 16 | 20 |
|        | 8  | 8           | 16 | 24 | 32 | 40 |
|        | 16 | 16          | 32 | 48 | 64 | 80 |

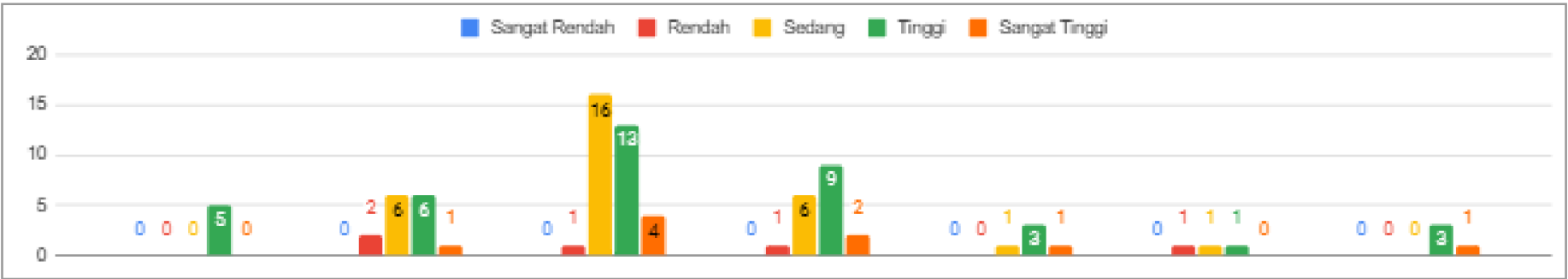
Enter Risk Category titles on the Dropdown Key tab to populate the Risk Register Dropdown Menu.

DO NOT ALTER SCORE CELLS  
Outcomes populate automatically.

| REF ID | DATE RAISED | RISK CATEGORY         | RISK DESCRIPTION (INCLUDING IF / THEN STATEMENT)                                                                       | PROBABILITY 1 – 5 | IMPACT 1 – 16 | RISK SEVERITY SCORE Prob x Impact | LIKELY TIMING OF RISK                                                                                                                                                   | RISK TRIGGER                                                 | MITIGATION / RESPONSE PLAN                                                                                                                                                                | STATUS OF MITIGATION / RESPONSE                                                   | OWNER                          |
|--------|-------------|-----------------------|------------------------------------------------------------------------------------------------------------------------|-------------------|---------------|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|--------------------------------|
| 10001  | MM/DD/YY    | Planning              | If there are changes in plans that require additional or different resources, then there will be delays.               | 1                 | 8             | 8                                 | The risk is present throughout the process of finalizing plans.                                                                                                         | There are changes in the plans.                              | A designated team member will continually monitor any proposed changes in plans and ensure communication between teams about proposed changes.                                            | No current issues                                                                 | Joe Smith; liaison             |
| 10002  | MM/DD/YY    | Contracts             | If contractual issues among contractors, subcontractors, or vendors arise, then there will be delays or cost overruns. | 2                 | 4             | 8                                 | The risk is present before most contract work commences. However, the risk will also be present when additional contracts are added in the early phases of the project. | The contracts manager reports any potential contract issues. | The contracts manager will continually monitor contracts, alert the team when there are issues, and ensure that the team addresses and resolves contract issues before they cause delays. | Working on one unresolved issue with vendor A's contract; meeting set for May 2nd | Sue Johnson, contracts manager |
| 10003  | MM/DD/YY    | Permits / Regulations | If obtaining appropriate construction permits takes longer than planned, then there will be delays.                    | 2                 | 8             | 16                                | The risk is present throughout phase A of the project, including when securing required permits.                                                                        | Permits do not arrive within the required timeframe.         | The manager, or another designated team member, will monitor the project schedule and deadlines and ensure that all permits can accommodate the project's schedule.                       | All deadlines currently being monitored                                           | Dale Swenson, manager          |

# Pemantauan Risiko

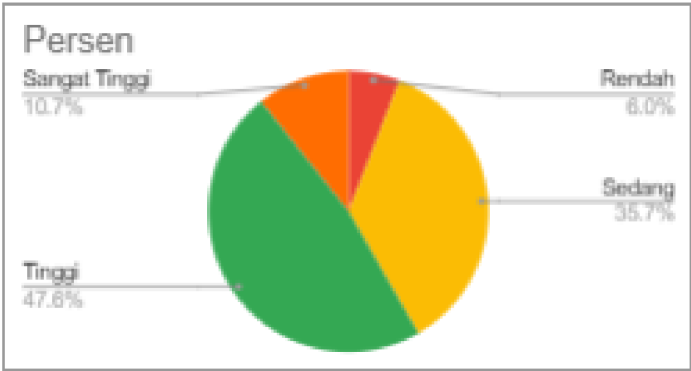
| No | Tipe Aset                  | Sangat Rendah | Rendah | Sedang | Tinggi | Sangat Tinggi | Jumlah |
|----|----------------------------|---------------|--------|--------|--------|---------------|--------|
| 1  | Perangkat Keras (Hardware) | 0             | 0      | 0      | 5      | 0             | 5      |
| 2  | Perangkat Lunak (Software) | 0             | 2      | 6      | 6      | 1             | 15     |
| 3  | Infrastruktur Fisik        | 0             | 1      | 16     | 13     | 4             | 34     |
| 4  | Data                       | 0             | 1      | 6      | 9      | 2             | 18     |
| 5  | Sumber Daya Manusia        | 0             | 0      | 1      | 3      | 1             | 5      |
| 6  | Sistem Keamanan            | 0             | 1      | 1      | 1      | 0             | 3      |
| 7  | Jaringan Telekomunikasi    | 0             | 0      | 0      | 3      | 1             | 4      |



| No | Tipe Risiko                | Sangat Rendah | Rendah | Sedang | Tinggi | Sangat Tinggi | Jumlah |
|----|----------------------------|---------------|--------|--------|--------|---------------|--------|
| 1  | Risiko Fisik               | 0             | 0      | 0      | 0      | 0             | 0      |
| 2  | Risiko Lingkungan          | 0             | 0      | 0      | 0      | 0             | 0      |
| 3  | Risiko Teknologi           | 0             | 0      | 0      | 0      | 0             | 0      |
| 4  | Risiko Keamanan Siber      | 0             | 0      | 0      | 0      | 0             | 0      |
| 5  | Risiko Operasional         | 0             | 0      | 0      | 0      | 0             | 0      |
| 6  | Risiko Keuangan            | 0             | 0      | 0      | 0      | 0             | 0      |
| 7  | Risiko Kepatuhan           | 0             | 0      | 1      | 0      | 0             | 1      |
| 8  | Risiko Reputasi            | 0             | 1      | 0      | 1      | 0             | 2      |
| 9  | Risiko Penyedia Layanan    | 0             | 0      | 0      | 1      | 0             | 1      |
| 10 | Risiko Pasokan Listrik     | 0             | 0      | 3      | 7      | 3             | 13     |
| 11 | Risiko Jaringan            | 0             | 2      | 11     | 8      | 0             | 21     |
| 12 | Risiko Sumber Daya Manusia | 0             | 2      | 6      | 8      | 2             | 18     |
| 13 | Risiko Proyek              | 0             | 0      | 3      | 2      | 1             | 6      |
| 14 | Risiko Keamanan Fisik      | 0             | 0      | 0      | 1      | 0             | 1      |
| 15 | Risiko Kebijakan           | 0             | 0      | 6      | 5      | 2             | 13     |
| 16 | Risiko Pemeliharaan        | 0             | 0      | 0      | 7      | 1             | 8      |

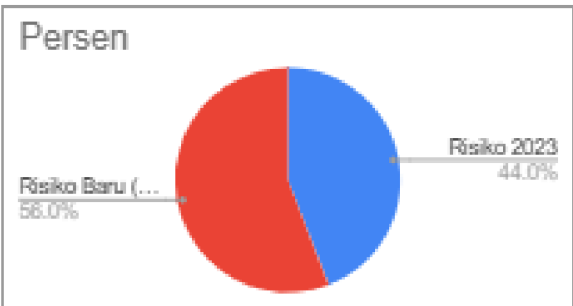
TABEL PERSENTASE LEVEL RISIKO 2024

| Level         | Jumlah | Persen        |
|---------------|--------|---------------|
| Sangat Rendah | 0      | 0             |
| Rendah        | 5      | 0.05952380952 |
| Sedang        | 30     | 0.3571428571  |
| Tinggi        | 40     | 0.4761904762  |
| Sangat Tinggi | 9      | 0.1071428571  |



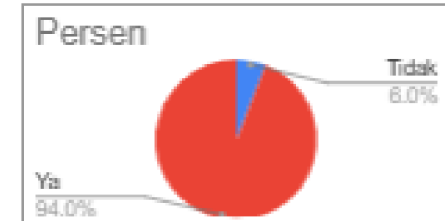
TABEL JUMLAH RISIKO BERDASAR TAHUN

| Tahun              | Jumlah |
|--------------------|--------|
| Risiko 2023        | 37     |
| Risiko Baru (2024) | 47     |
| TOTAL              | 84     |



TABEL PERSENTASE PENANGANAN RISIKO KEAMANAN SPBE (Ya/Tidak)

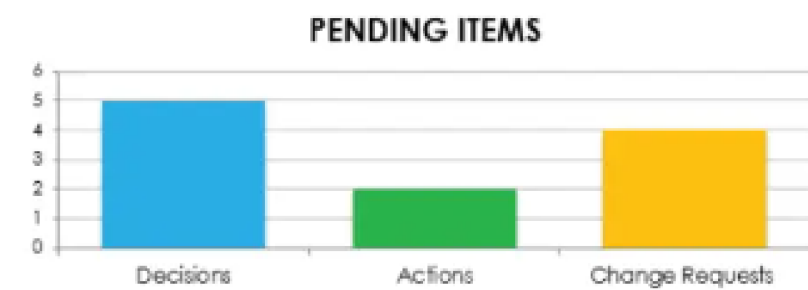
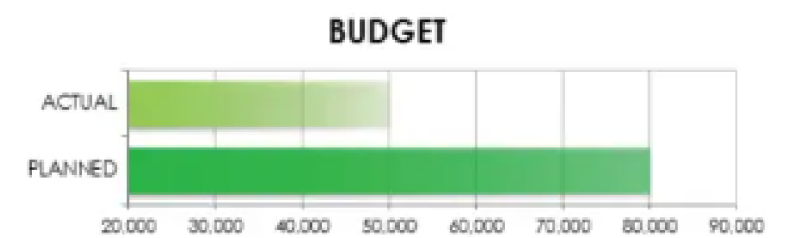
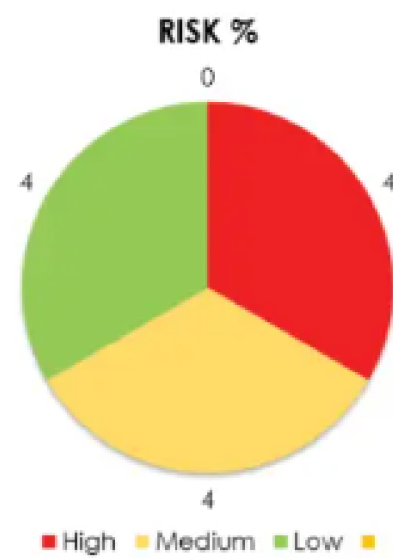
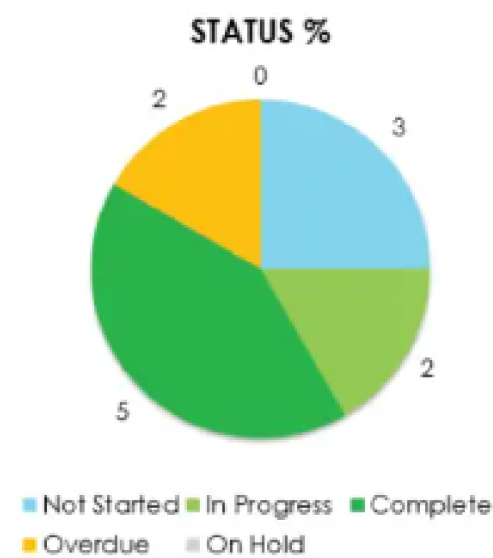
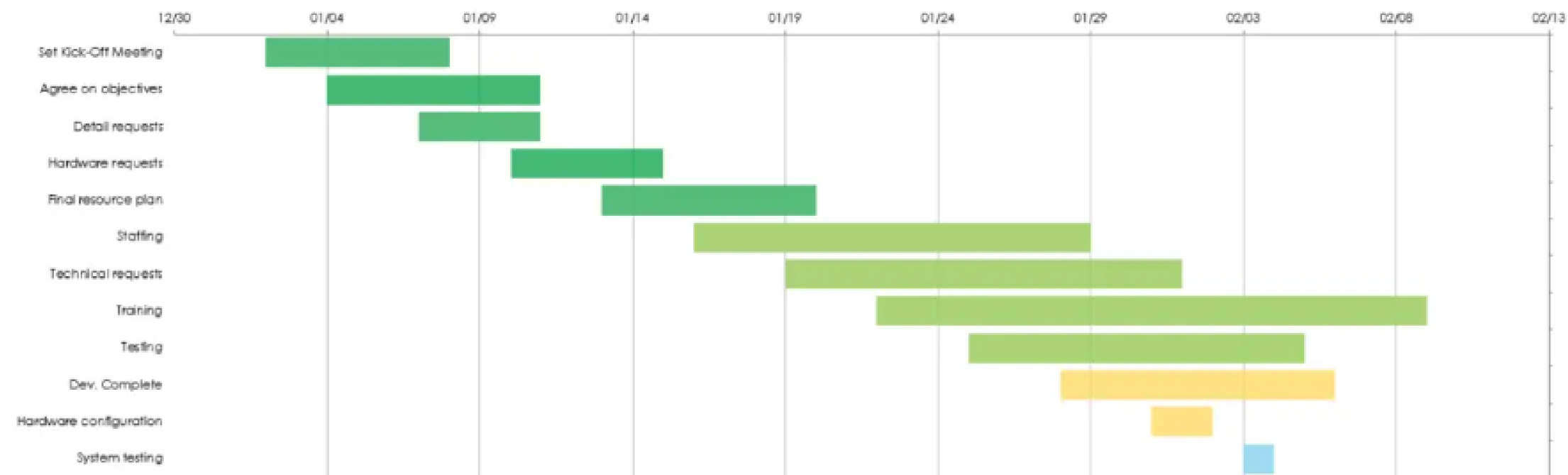
| Level | Jumlah | Persen |
|-------|--------|--------|
| Tidak | 5      | 5.95%  |
| Ya    | 79     | 94.05% |



# Pemantauan Risiko

| PROJECT NAME  | DATE     | PROJECT STATUS | % COMPLETE |
|---------------|----------|----------------|------------|
| PROJECT ALPHA | MM/DD/YY | ON TRACK       | 72%        |

## TASK TIMELINE





# REKOMENDASI

## Pusat Data

01

### Gunakan Standar Pusat Data (SNI 8799)

Adanya standar spesifikasi dan tata kelola pusat data membuat kualitas layanan pusat data sesuai best practice international

02

### Implementasi Manajemen Risiko

Lakukan manajemen risiko secara reguler dan konsisten setiap tahunnya dengan Standar/Framework Terbaik

03

### Standar SDM

Tetapkan standar untuk perekrutan, pelatihan, dan sertifikasi staf operasional di pusat data untuk keahlian yang memadai.

04

### Monitoring dan Pemantauan

Implementasi sistem monitoring dan pemantauan yang canggih untuk mendeteksi dini ancaman keamanan dan kegagalan sistem, Data Center Infrastructure Management (DCIM)

Citra Arfanudin

# Thank You

Naik Ke IT Level Global?

Eduparx membantu Anda mengembangkan skill terdepan, trend terkini, dan teknologi paling baru untuk mengantarkan IT Anda ke level global.

