



**Analisa Risiko Dengan COBIT 5**

**Studi Kasus Dinas Perindustrian dan Tenaga Kerja Kabupaten Trenggalek**

**Mata Kuliah Manajemen Risiko Teknologi Informasi KS141318**

**KELOMPOK 2 – MRTI [A]**

|  |  |
| --- | --- |
| **Evia Nanda Irawati** | **5215100056** |
| **Finsa Ayu Firnanda** | **5215100068** |
| **Almira Filiazsanti** | **5215100075** |
| **Fadhila Alfi** | **5215100092** |

**Dosen Pengampu :**

**Eko Wahyu Tyas Darmaningrat S. Kom, M.BA**

**DEPARTEMEN SISTEM INFORMASI**

Fakultas Teknologi Informasi

Institut Teknologi Sepuluh Nopember Surabaya 2017

# DAFTAR ISI

[DAFTAR GAMBAR 3](#_bookmark0)

[DAFTAR TABEL](#_bookmark0) 4

[BAB I PENDAHULUAN 5](#_bookmark1)

* 1. [Latar Belakang 5](#_bookmark2)
  2. [Rumusan Masalah 7](#_bookmark4)
  3. [Batasan Masalah 7](#_bookmark5)
  4. [Identifikasi Masalah](#_bookmark6) 8
  5. [Tujuan 8](#_bookmark7)
  6. [Manfaat 8](#_bookmark8)
  7. [Relevensi 9](#_bookmark9)

[BAB II KAJIAN LITERATUR 10](#_bookmark10)

[2. 1 Resiko 10](#_bookmark11)

[2. 1. 1 Value Creation 10](#_bookmark12)

[2. 1. 2 Resiko 10](#_bookmark13)

[2. 1. 3 Scope of COBIT 5 12](#_bookmark14)

[2. 1. 4 Penerapan COBIT 5 untuk Mengelola Resiko 13](#_bookmark16)

[2.2 PERSPEKTIF RESIKO 13](#_bookmark17)

[2. 2. 1 Perspektif Fungsi Resiko 14](#_bookmark19)

[2. 2. 1.1 Manage Security Service (DSS05) 14](#_bookmark19)

[2. 2. 2 Perspektif Manajemen Resiko 17](#_bookmark20)

[2. 2. 2.1 Memastikan Optimalisasi Risiko (EDM03) 17](#_bookmark20)

[2. 2. 2.2 Memanage Resiko (APO12) 17](#_bookmark20)

[2. 3 Risk Scenario 18](#_bookmark21)

[2. 3. 1 Risk Scenarios 18](#_bookmark22)

[2. 3. 2 Risk Response 222](#_bookmark26)

[2. 3. 2.1 Risk Avoidance 222](#_bookmark26)

[2. 3. 2.2 Risk Acceptance 222](#_bookmark26)

[2. 3. 2.3 Risk Sharing/Transfer 22](#_bookmark26)

[2. 3. 2.4 Risk Mitigation 23](#_bookmark26)

[2. 4 Perbanding COBIT 5 Dengan Standar Lain 25](#_bookmark28)

[BAB III METODOLOGI 27](#_bookmark29)

* 1. [Melakukan Interview 28](#_bookmark31)
  2. [Studi Literature 28](#_bookmark32)
  3. [Analisis Kondisi Eksisting 28](#_bookmark33)
  4. [Analisis Risiko 29](#_bookmark34)
     1. [Identifikasi Risiko Setiap Aktivitas DSS05 29](#_bookmark35)
     2. [Mengidentifikasi Kategori dan Tipe Risiko 29](#_bookmark36)
     3. [Analisis Penyebab Risiko 29](#_bookmark37)
  5. [Perumusan Skenario Resiko 29](#_bookmark38)

[BAB IV HASIL DAN PEMBAHASAN 30](#_bookmark39)

* 1. [Melakukan Studi Literatur 30](#_bookmark40)
  2. [Analisis Kondisi Eksisting 30](#_bookmark41)
     1. [Struktur Organisasi Dinas Perindustrian dan Tenaga Kerja Kabupaten Trenggalek 30](#_bookmark41)
     2. [Proses Bisnis SiskoTKLN 32](#_bookmark41)
     3. [Pemilihan dan Pemetaan Proses Bisnis sesuai COBIT 5 Enabling Process 35](#_bookmark46)
  3. [Analisis Risiko Perusahaan 44](#_bookmark49)
     1. [Identifikasi Risiko Setiap Aktivitas DSS05 44](#_bookmark50)
     2. [Mengidentifikasi Kategori dan Tipe Risiko 52](#_bookmark52)
     3. [Analisis Penyebab Risiko 56](#_bookmark54)
  4. [Perumusan Skenario Risiko 60](#_bookmark56)

[BAB 5 PENUTUP](#_bookmark58) 71

* 1. [Kesimpulan 71](#_bookmark59)
  2. [Saran 72](#_bookmark60)

[Referensi 74](#_bookmark61)

# DAFTAR GAMBAR

[**Gambar 1*.*1** Logo Kabupaten Trenggalek 5](#_bookmark3)

[**Gambar 2. 1** Kategori Resiko IT 12](#_bookmark15)

[**Gambar 2. 2** Scope dari COBIT 5 12](#_bookmark15)

[**Gambar 2. 3** Perspektif Risiko 13](#_bookmark18)

[**Gambar 2. 4** Processes for Management of Enterprise IT 13](#_bookmark18)

[**Gambar 2. 5** Skenario dari Risiko 19](#_bookmark23)

[**Gambar 2. 6** Hal-Hal yang Mempengaruhi Risk Scenario 20](#_bookmark24)

[**Gambar 2. 7** Contoh Risk Scenario 222](#_bookmark25)

[**Gambar 2. 8** Alur Kerja Respon Risiko 24](#_bookmark27)

[**Gambar 3. 1** Metodologi APO12 27](#_bookmark30)

[**Gambar 4. 1** Struktur Organisasi Dinas Perindustrian dan Tenaga Kerja 31](#_bookmark42)

[**Gambar 4. 2** Alur Pelayanan SISKOTKLN 32](#_bookmark43)

[**Gambar 4. 3** Aplikasi SISKOTKLN 33](#_bookmark44)

# DAFTAR TABEL

[**Tabel 4.1** Proses Bisnis dan Sub Proses Bisnis 35](#_bookmark45)

[**Tabel 4.2** Pemetaan Proses Bisnis Sesuai COBIT 5 37](#_bookmark47)

[**Tabel 4.3** Activity GAP 37](#_bookmark48)

[**Tabel 4.4** Risiko pada Aktivitas DSS05 52](#_bookmark51)

[**Tabel 4.5** Identifikasi Tipe Risiko 56](#_bookmark53)

[**Tabel 4.6** Penyebab Risiko 60](#_bookmark55)

[**Tabel 4.7** Skenario Risiko 60](#_bookmark57)

# BAB I PENDAHULUAN

# Latar Belakang

Organisasi baik profit maupun non-profit akan terus mengalami perkembangan pada setiap periodenya, baiknya jika perkembangan organisasi ini juga diiringi dengan pengembangan dan juga perbaikan manajemen organisasinya dan bahkan teknologi, dikarenakan pada jaman kini segala sesuatunya hampir 90% dikomputasikan dan menggunakan perangkat teknologi.

Salah satunya adalah teknologi informasi dimana diperlukan untuk membantu pekerjaan individu atau organisasi dalam mengolah data angka, data visual, data audio, atau data visual-audio. Dan juga umumnya, dalam sebuah organisasi dibentuk departemen IT yang dikhususkan untuk mengerjakan, mengelola, merawat baik sumber informasi maupun teknologi infomasi.



**Gambar 1*.*1** Logo Kabupaten Trenggalek

Dinas Perindustrian dan Tenaga Kerja merupakan salah satu dinas yang berada di kota Trenggaek, Kabupaten Trenggalek. Kabupaten Trenggalek sendiri merupakan

kabupaten yang menjadi bagian provinsi Jawa Timur dimana kabupaten ini memiliki logo kabupaten sesuai dengan yang ditampilkan pada Gambar 1.1 Dinas Perindustrian dan Tenaga Kerja merupakan dinas yang bergerak di bidang ketenaga kerjaan. Mengelola sumber daya manusia dengan cara menyalurkan antara pencari kerja dan perusahaan/organisasi/pabrik yang membutuhkan pekerjaan. Dinas Perindustrian dan Tenaga Kerja Kabupaten Trenggalek juga mengurusi Tenaga Keja Indonesia (TKI) dimana sebelum keberangkatan para TKI akan tinggal di asrama dan mendapatkan beberapa pelatihan.

Berdasar hasil wawancara kepada tiga narasumber yaitu Ibu Sutji selaku Kepala Subbagian Pelaporan dan Perencanaan, Ibu Apsari selaku Staff Pelaporan dan Perencanaan serta Bapak Suparman selaku Kepala Bidang Penempatan Tenaga Kerja dan Transmigrasi dari Dinas Perindustrian dan Tenaga Kerja Kabupaten Trenggalek, didalam kegiatan organisasinya, Dinas Perindustrian dan Tenaga Kerja memanfaatkan teknologi informasi. Seperti contoh, proses pendataan TKI atau tenaga kerja biasa menggunakan *software* atau aplikasi yang bernama SiskoTKLN (Sistem Komputerisasi Tenaga Kerja Luar Negeri) yang dapat melakukan *input* pada data-data calon tenaga kerja untuk perusahaan/organisasi/pabrik maupun yang akan kerja keluar negeri.

Namun dengan adanya penggunaan teknologi informasi seperti ini tentunya terdapat tantangan pula untuk kegiatan mengelola dan melakukan *maintenance* terhadap *software* maupun perangkat *hardware* yang digunakan. Salah satu hal yang perlu diperhatikan adalah risiko-risiko yang mungkin saja terjadi dikarenakan adanya teknologi informasi tersebut. Mengingat aset-aset teknologi informasi merupakan hal yang bisa dikatakan tidak murah dan perlu penanganan khusus, maka perlu ditinjau pula dari segi manajemen risiko pula.

Salah satu *framework* yang dapat digunakan untuk membantu dalam hal manajemen risiko adalah COBIT 5, adalah suatu panduan standar praktek manajemen teknologi informasi dan sekumpulan dokumentasi *best practices*

untuk tata kelola TI yang dapat membantu auditor, manajemen, dan pengguna untuk menjembatani pemisah (*gap*) antara risiko bisnis, kebutuhan pengendalian, dan permasalahan-permasalahan teknis[1].

Pada praktik dari COBIT 5, terdapat perbedaan roles dari keamanan informasi pemerintahan dan manajemen yang dapat digambarkan pada gambar 2 dimana terdapat proses-proses yang dilakukan pemerintahan dan proses-proses yang dilakukan manajemen. Masing-masing memiliki responsibilities atau tanggung jawab yang berbeda[1].

# Rumusan Masalah

Berdasarkan uraian latar belakang tersebut, rumusan masalah yang akan diselesaikan pada penelitian ini adalah :

1. Bagaimana proses bisnis dari Dinas Perindustrian dan Tenaga Kerja Kabupaten Trenggalek?
2. Bagaimanakah proses manajemen risiko IT pada Dinas Perindustrian dan Tenaga Kerja Kabupaten Trenggalek saat ini?
3. Bagaimanakah membuat rancangan manajemen risiko IT pada Dinas Perindustrian dan Tenaga Kerja Kabupaten Trenggalek dengan menggunakan *framework* COBIT 5?

# Batasan Masalah

Berdasarkan rumusan permasalahan tersebut, batasan masalah terkait rumusan masalah pada penelitian ini adalah :

1. Objek pada penelitian ini berfokus pada layanan publik pada bidang penempatan tenaga kerja dan transmigrasi
2. Analisa manajemen risiko yang dilakukan menggunakan domain COBIT 5 APO12.01 dan APO 12.02
3. Rancangan manajemen resiko yang akan dibangun hanya terbatas pada tahap skenario risiko.

# Identifikasi Masalah

Adapun permsalahan-permasalahan yang ditemui pada Dinas Perindustrian dan Tenaga Kerja Kabupaten Trenggalek yang berpotensi mengalami risiko adalah :

1. *Server* yang digunakan pada perangkat teknologi Dinas Perindustrian dan Tenaga Kerja Kabupaten Trenggalek masih menumpang pada Dinas Komunikasi dan Informasi. Hal ini menyebabkan berpotensinya risiko jika terjadi kerusakan pada *server*, pihak Dinas Perindustrian dan Tenaga Kerja Kabupaten Trenggalek tidak dapat dengan tanggap mengetahui atau melakukan perbaikan dan risiko-risiko lainnya.
2. Selain itu pada Dinas Perindustrian dan Tenaga Kerja Kabupaten Trenggalek juga tidak ada petugas khusus IT ataupun divisi IT yang nantinya dapat membantu atau menangani jika terjadi masalah IT. Petugas yang berhubungan dengan perangkat IT hanyalah sebatas petugas operasional.
3. Untuk masalah keamanan dari *software* terdapat banyak celah didalamnya karena kembali lagi pada poin kedua identifikasi masalah yaitu Dinas Perindustrian dan Tenaga Kerja Kabupaten Trenggalek tidak memiliki tenaga ahli untuk melakukan perawatan divisi IT.

# Tujuan

Berdasarkan latar belakang dan permasalahan yang telah dijelaskan, maka tujuan dari *final project* ini adalah sebagai berikut:

1. Mengetahui proses manajemen risiko IT pada Dinas Perindustrian dan Tenaga Kerja Kabupaten Trenggalek saat ini.
2. Membuat rancangan manajemen risiko IT pada Dinas Perindustrian dan Tenaga Kerja Kabupaten Trenggalek dengan menggunakan *framework* COBIT 5.

# Manfaat

Melalui tugas akhir ini diharapkan dapat memberikan manfaat, yaitu :

# Bagi penulis :

Mendapatkan pengetahuan mengenai cara menggunakan dan melakukan implementasi *framework* COBIT 5 dalam kegiatan manejemen risiko IT pada umumnya.

# Bagi instansi :

Hasil pengerjaan dari tugas ini diharapkan dapat membantu instansi terkait dalam manajemen risiko IT dengan menggunakan *framewrok* COBIT 5.

# Bagi masyarakat :

Mendapatkan informasi mengenai manajemen risiko IT dengan menggunakan framework OCTAVE.

# Relevensi

Tugas ini berkaitan dengan *final project* untuk mata kuliah Manajemen Risiko TI pada bab penggunaan framework dalam manajemen risiko TI.

# BAB II KAJIAN LITERATUR

# 2. 1 Resiko

# 2. 1. 1 Value Creation

Keberadaan perusahaan pastinya untuk menciptakan *value* untuk *stakeholder* mereka. Akibatnya setiap perusahaan baik perusahaan komersil atau tidak akan memiliki *value creation* sebagai tujuan tata kelola. *Value creation* dapat diartikan sebagai manfaat pada biaya sumber daya optimal untuk mengoptimalkan resiko. Manfaat tersebut dapat dilihat dari berbagai bentuk, seperti contoh manfaat pada keuangan perusahaan komersil atau layanan publik.

Kebutuhan *stakeholder* mendorong untuk menciptakan *value creation*. *Value creation* tersebut diantaranya yaitu Menyadari manfaat/benefit, Mengoptimalkan resiko, serta mengoptimalkan sumber daya.

Perusahaan memiliki banyak *stakeholder*, dan diantara perusahaan dan *stakeholder* dalam mengartikan *value creation* berbeda-beda bahkan terkadang saling bertentangan. Komponen optimalisasi resiko menunjukkan bahwa mengoptimalkan resiko merupakan bagian yang sangat penting dari sistem pemerintahan. Pengoptimalan resiko tidak dapat dilihat secara terpisah, yaitu tindakan yang diambil sebagai bagaian dari manajemen resiko akan mempengaruhi proses *benefit realization* dan pengoptimalan sumber daya[2].

# 2. 1. 2 Resiko

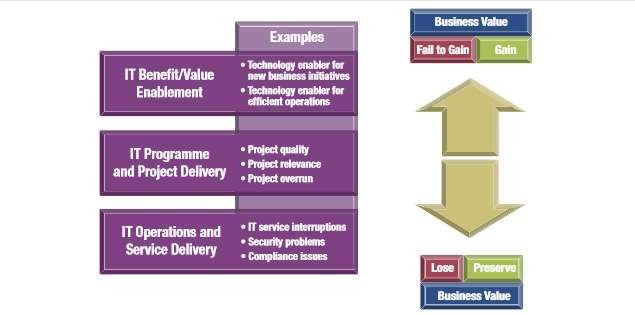
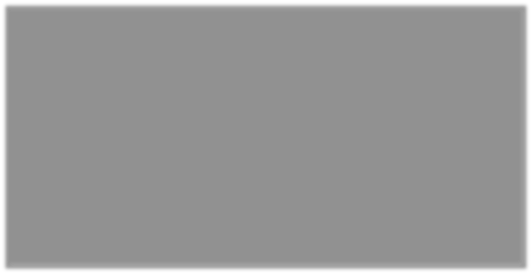
Resiko umumnya didefinisikan sebagai kombinasi antara probabilitas kejadian dan konsekuensinya. Konsekuensi menunjukkan bahwa tujuan

perusahaan tidak terpenuhi. COBIT 5 For Risk mendefinisikan resiko IT sebagai resiko dari bisnis khususnya resiko bisnis yang terkait dengan penggunaan, kepemilikan, operasi, keterlibatan, pengaruh dan adopsi IT dalam suatu perusahaan.

Resiko IT terdiri atas kejadian terkait dengan TI yang berpotensi berdampak pada bisnis. Resiko IT dapat terajadi dengan frekuensi dan dampak yang tidak pasti dan yang pasti menimbulkan tantangan dalam mencaoai sasaran dan tujuan perusahaan. Resiko IT akan selalu ada, entah perusahaan dapat mendeteksi dan mengenali resiko tersebut atau tidak.

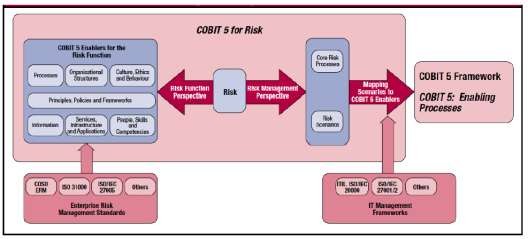
Resiko TI dapat dikategorikan sebagai berikut[2]:

1. *IT benefit / value enablement risk* – terkait dengan kehilangan kesempatan menggunakan teknologi untuk meningkatkan efisiensi atau efektivitas proses bisnis
2. *IT Programme and project delivery risk* – terkait dengan kontribusi IT untuk solusi bisnis yang lebih baik, biasanya berbentuk proyek atau program sebagai bagian portfolio.
3. *IT operations and service delivery risk* – terkait dengan semua aspek kinerja bisnis seperti sistem dan layanan TI, yang dapat membawa pengurangan nilai bagi perusahaan.



**Gambar 2. 1** Kategori Resiko IT

# 2. 1. 3 Scope of COBIT 5



**Gambar 2.2** Scope dari COBIT 5

COBIT 5 *for Risk* memiliki cakupan yang salah satu diantaranya berfokus pada penerapan pengambil keputusan COBIT 5 *for Risk* melalui perspektif fungsi risiko (*bagaimana menggunakan COBIT 5*).

Selain itu COBIT 5 juga memungkinan tata kelola dan manajemen resiko yang efektif serta efisien. Dimana COBIT 5 memberikan panduan mengenai identifikasi, analisis dan merespon risiko melalui penerapan proses manajemen risiko di COBIT 5 dan melalui penggunaan skenario risiko seperti yang terlihat pada gambar 2.2.

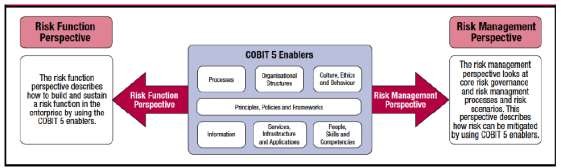
COBIT 5 juga sesuai dengan sumber referensi pasar ERM yang ada (standar, kerangka kerja dan panduan) dan juga inisiatif ERM. Selain itu, disediakan pula hubungan antar skenario risiko dan *enablers* dari COBIT 5 yang dapat digunakan untuk mengurangi risiko [3].

# 2. 1. 4 Penerapan COBIT 5 Untuk Mengelola Resiko

Untuk menerapkan COBIT 5 untuk melakukan manajemen risiko dalam sebuah organisasi. Disini COBIT 5 dapat dimanfaatkan untuk mendorong manajemen eksektif untuk menunjukkan dukungan terhadap program manajemen risiko. Selain itu COBIT 5 juga dapat membantu identifikasi struktur atau peran kunci organisasi yang diperlukan untuk membangun dan mempertahankan tata kelola risiko dan manajemen risiko yang efektif dan efisien dalam organisasi. Peran tersebut akan di identifikasi dengan memberikan deskripsi atau definisi spesifik dari setiap peran dan struktur. Ini membantu organisasi untuk membangun lini pertahanan mereka untuk manajemen risiko.

Manajemen risiko harus disematkan dalam proses normal dan merupakan bagian dari praktik manajemen sehari-hari. Budaya sadar risiko juga harus diterapkan dengan baik di antara semua tingkat karyawan. Selain itu juga perlu dilakukan identifiksi dan pengembangan metrik untuk dijadikan indikator risiko utama (KICS) yang digunakan untuk menggambarkan dan melacak indikator risiko [3].

# PERSPEKTIF RESIKO



**Gambar 2.3** Perspektif Risiko

Pada Gambar 2.3 dapat dilihat juga risiko memiliki dua persepektif, yaitu persepektif dari *risk fuunction* dan yang kedua adalah persepektif dari *risk*

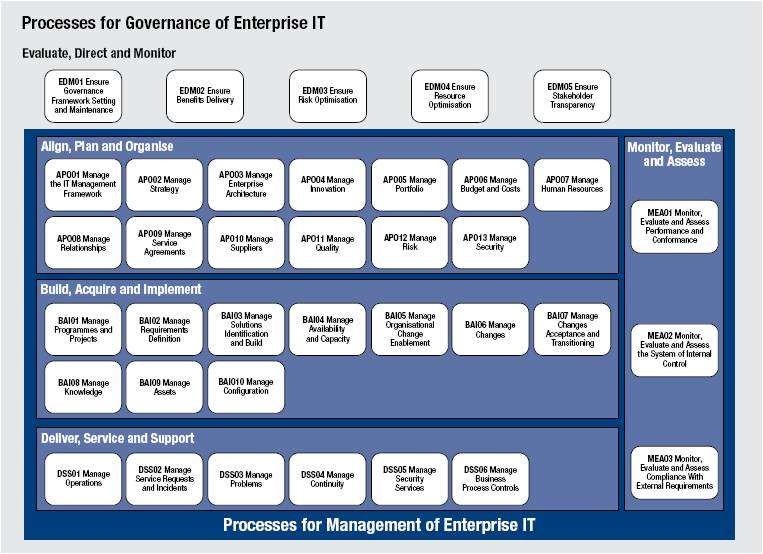
*management.* Dimana kedua persepektif ini berakar dari COBIT 5 Enablers. Dan berikut adalah penjabaran dari kedua persepektif ini :

# 2. 2. 1 Perspektif Fungsi Resiko

Menggambarkan bagaimana membangun dan mempertahankan fungsi risiko di perusahaan dengan menggunakan COBIT5 *enablers*. Cobit 5 For Risk memberikan panduan dan menggambarkan bagaimana masing-masing enabler berkontribusi terhadap keseluruhan tata kelola dan pengelolaan fungsi risiko. Seperti contohnya sebagai berikut[4]:

* + - Proses diperlukan untuk menentukan dan mempertahankan fungsi risiko, mengatur dan mengelola risiko.
    - Arus informasi apa yang dibutuhkan untuk mengatur dan mengelola risiko. misalnya risiko alam semesta, profil risiko.
    - Struktur organisasi yang diperlukan untuk mengatur dan mengelola risiko secara efektif. misalnya komite risiko perusahaan, fungsi risiko.
    - Orang dan keterampilan seperti apa yang harus dilakukan untuk membangun dan mengoperasikan fungsi risiko yang efektif.

Proses COBIT 5 yang diperlukan untuk mendukung fungsi risiko dapat dilihat pada gambar



**Gambar 2.4** Processes for Management of Enterprise IT

Pada **Gambar 2.4** dapat dilihat bahwa terdapat beberapa domain yang telah dikategorikan. Berikut kategori domain pada COBIT 5:

## *COBIT 5 – Governance Domains (Evaluate, Direct and Monitor (EDM))*

* Ensure governance framework setting & maintenance
* Ensure benefits delivery
* Ensure risk optimization
* Ensure resource optimization
* Ensure stakeholders transparency

## *COBIT 5 – Management Domains (Align, Plan and Organise (APO)*

* Manage the IT management framework
* Manage strategy
* Manage enterprise architecture
* Manage innovation
* Manage porfolio
* Manage budget and costs
* Manage human resources
* Manage relationships
* Manage service agreements
* Manage suppliers
* Manage quality
* Manage risk
* Manage security

## *COBIT 5 – Management Domains (Build, Acquire and Implement (BAI))*

* Manage programmes and projects
* Manage requirements definition
* Manage solutions identification and build
* Manage availability and capacity
* Manage organisational change enablement
* Manage changes
* Manage change acceptance and transitioning
* Manage knowledge
* Manage assets
* Manage configurations

## *COBIT 5 – Management Domains (Delivery, Service and Support (DSS))*

* Manage operations
* Manage service requests and incidents
* Manage problems
* Manage continuity
* Manage security services
* Manage business process control

## *COBIT 5 – Management Domains (Monitor, Evaluate and Assess (MEA))*

* Performance and conformance
* The system of internal control
* Compliance with external requirements

# 2.2.1.1 Manage security services (DSS05)

Pada proses ini membahas tentang perlindungan alat-alat komputer dan personal membutuhkan fasilitas fisik yang dirancang baik dan dikelola dengan baik. Proses pengelolaan fisik meliputi dengan memilih fasilitas yang tepat dan merancang proses yang efektif untuk memonitor faktor-faktor keamanan dan mengelola hak akses. Pengelolaan perlindungan fisik yang efektif dapat mengurangi gangguan

bisnis dari kerusakan peralatan komputer dan personal. Control objective yang digunakan adalah[5]:

1. DSS05.01 Protect against malware
2. DSS05.02 Manage network and connectivity security
3. DSS05.03 Manage endpoint security
4. DSS05.04 Manage user identity and logical access
5. DSS05.05 Manage physical access to IT assets
6. DSS05.06 Manage sensitive documents and output devices
7. DSS05.07 Monitor the infrastructure for security-related events

# 2. 2. 2 Perspektif Manajemen Resiko

# 2. 2. 2. 1 Memastikan Optimalisasi Risiko (EDM03)

Proses ini mencakup pemahaman artikulasi dan komunikasi tentang risk appetite perusahaan dan toleransi dan memastikan identifikasi dan pengelolaan risiko terhadap nilai perusahaan yang terkait dengan penggunaan TI dan dampaknya. Tujuan dari proses ini adalah untuk[2]:

1. Menentukan dan mengkomunikasikan ambang batas risiko dan memastikan bahwa kunci risiko terkait TI diketahui
2. Mengelola risiko perusahaan terkait TI secara efektif dan efisien
3. Memastikan risiko perusahaan yang terkait dengan TI tidak melebihi *risk appetite*

# 2. 2. 2. 2 Memanage Risiko (APO12)

Proses ini mencakup identifikasi, penilaian dan pengurangan risiko terkait TI secara terus menerus dalam tingkat toleransi yang ditetapkan oleh manajemen eksekutif perusahaan. pengelolaan risiko perusahaan terkait TI harus diintegrasikan dengan keseluruhan ERM. Biaya dan manfaat pengelolaan risiko perusahaan terkait TI harus diimbangi dengan :

1. Mengumpulkan data yang tepat dan menganalisa risiko.
2. Mempertahankan profil risiko perusahaan dan mengartikulasikan risiko.
3. Mendefinisikan portofolio pengelolaan risiko dan merespons risiko[4].

Proses APO12 terbagi menjadi enam subdomain, yaitu antara lain [6]:

1. APO12.01 : Collect Data
2. APO12.02 : Analyse Risk
3. APO12.03 : Maintain A Risk Profile
4. APO12.04 : Articulate Risk
5. APO12.05: Define a Risk Management Action Portofolio
6. APO12.06 : Respond to Risk

# 2. 3 Risk Scenario

# 2. 3. 1 Risk Scenarios

Risk scenario adalah kejadian-kejadian yang mungkin saja terjadi dan memberikan dampak yang tidak pasti pada pencapaian tujuan perusahaan atau organisasi. Dampak yang tidak pasti ini bisa saja positif atau negatif[4].

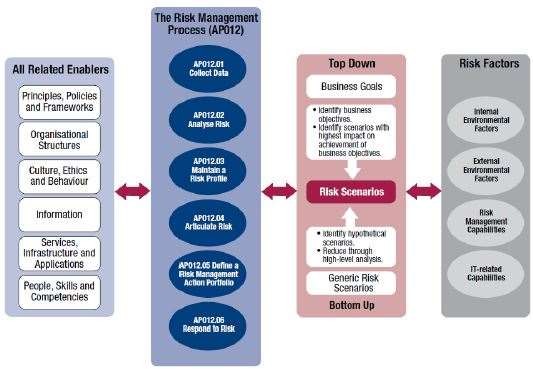
Risk Scenario adalah *key element* pada *Risk Management Process* APO12. Terdapat dua pendekatan :

1. Top-down Approach

Menggunakan tujuan perusahaan atau organisasi secara keseluruhan dan mempertimbangkan IT Risk Scenario mana yang paling relevan dan mungkin berdampak pada tujuan perusahaan.

1. Bottom-up Approach

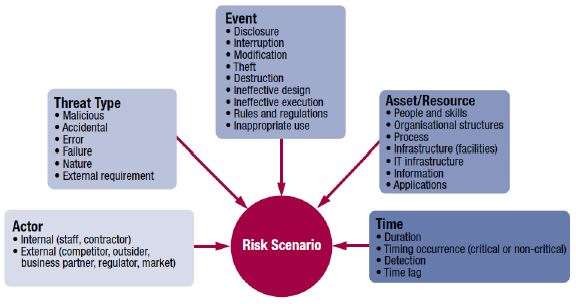
Menggunakan *list* dari *generic scenario* untuk menentukan sebuah *set scenario* yang paling relevan dan bisa disesuaikan untuk digunakan atau di-*apply* pada perusahaan/organisasi.



**Gambar 2.5** Skenario dari Risiko

Kedua pendekatan tersebut saling melengkapi dan harus dilakukan secara serentak atau bersamaan atau sekaligus. Risk Scenario itu sendiri harus relevan dan berkaitan dengan resiko bisnis yang nyata yang ada di perusahaan seperti yang digambarkan dalam Gambar 2.5. Risiko-risiko yang spesifik pada perusahaan dan *critical business requirements* harus benar-benar dipertimbangkan dalam Risk Scenario perusahaan. COBIT 5 for Risk (resiko) memberikan sekumpulan *generic risk scenario* yang luas, menyeluruh dan lengkap yang dapat digunakan sebagai referensi untuk mengurangi kemungkinan perusahaan menghadapi resiko utama atau umum[4]. Selain itu ada banyak hal yang mempengaruhi risiko seperti yang dapat dilihat pada Gambar 2.6.

Hal-hal yang mempengaruhi Risk Scenario antara lain :



**Gambar 2. 6** Hal-Hal yang Mempengaruhi Risk Scenario

# Identifikasi Actor

Identifikasi actor diperlukan untuk mengetahui siapa saja yang menghasilkan ancaman yang mengeksploitasi kerentanan pada Dinas Perindustrian dan tenaga Kerja Kabupaten Trenggalek. Aktor dapat bersifat internal maupun eksternal serta bisa berupa manusia maupun bukan manusia. Output yang didapat pada tahapan ini ialah daftar actor yang nantinya akan digunakan dalam pembuatan scenario risiko.

# Identifikasi Tipe Risiko

Identifikasi tipe ancaman diperlukan untuk mengetahui apakah tipe-tipe dari ancaman atau risiko yang mungkin terjadi serta mengedintifikasi apakah jenis ancaman itu berbahaya. Output yang didapat pada tahapan ini ialah daftar tipe dan risiko yang mungkin terjadi yang akan digunakan dalam pembuatan scenario risiko.

# Identifikasi Event

Identifikasi aktivitas mencakup perancangan sistem, proses, yang tidak ekfektif dan penggunaan yang tidak tepat. Output yang didapat pada tahapan ini ialah daftar aktivitas yang akan digunakan dalam pembuatan *scenario* risiko.

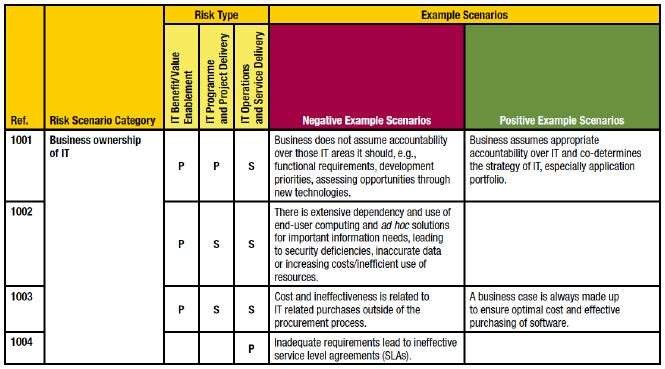
# Identifikasi Resource

Identifikasi aset berharga bagi Dinas Perindustrian dan Tenaga Kerja Kabupaten Trenggalek yang dipengaruhi oleh event dan mengarah pada dampak bisnis. Identifikasi resource dapat membantu untuk mencapai tujuan TI. Output dari tahapan ini adalah daftar resource yang akan digunakan dalam pembuatan scenario risiko.

# Identifikasi Waktu

Identifikasi waktu yang meliputi durasi, kejadian apa yang terjadi pada waktu tertentu, apakah dapat dideteksi dan jeda waktu antara kejadian dan konsekuensi apakah terdapat konsekuensi secara langsung atau tidak. Output dari tahapan ini adalah daftar waktu yang akan digunakan dalam pembuatan scenario risiko.

Ketika *Risk Scenario* terlaksana, telah terjadi *loss event* atau kerugian. *Loss event* atau kerugian telah di-*trigger* oleh *threat event* atau ancaman (*Threat type + Event*). Frekuensi dari ancaman atau *threats* dipengaruhi oleh kerentanan atau vulnerability yang dimiliki perusahaan. Kerentanan ini biasanya dalam bentuk state dimana bisa meningkat dan menurun oleh *vulnerability events*[4]. Dapat dilihat pada Gambar 2.7 dimana skenario risiko yang dibuat akan dibagi dalam dua nilai yaitu primer dan sekunder yang masing-masingnya akan memberikan nilai kepada risiko yang akan dianalisis.



Gambar 2. 7 Contoh Risk Scenario

# 2. 3. 2 Risk Response

Sebuah respon terhadap suatu resiko perlu didefinisikan sedemikian rupa sehingga risiko di masa depan berada dalam batas yang dapat diterima. Ketika analisis risiko menunjukkan bahwa risiko tidak selaras dengan tingkat *risk appetite* dan *tolerance* yang ditentukan, sebuah respon perlu dilakukan. Respon yang mungkin dilakukan adalah *avoid, mitigare, share/transfer* dan *accept*[4]*.*

# 2. 3. 2. 1 Risk Avoidance

Menghindari artinya keluar dari aktifitas atau kondisi yang memungkinkan adanya resiko. Risk avoidance digunakan saat tidak ada respon lain yang cocok[4]. Digunakan saat :

* + Tidak ada respon *cost-effective* yang lain yang mampu mengurangi frekuensi dan dampak dibawah ambang risk appetite
  + Resiko tidak dapat di share atau di transfer
  + Kerugiannya tidak dapat diterima oleh pihak manajemen

# 2. 3. 2. 2 Risk Acceptance

Menerima artinya kerugian disadari tapi tidak ada tindakan yang diambil untk resiko tertentu dan kerugian itu diterima apabila terjadi[4]. Hal ini lain dengan

tidak sadar akan resiko. Menerima resiko diasumsikan bahwa resiko diketahui, misalnya keputusan yang telah dibuat oleh manajamen untuk diterima.

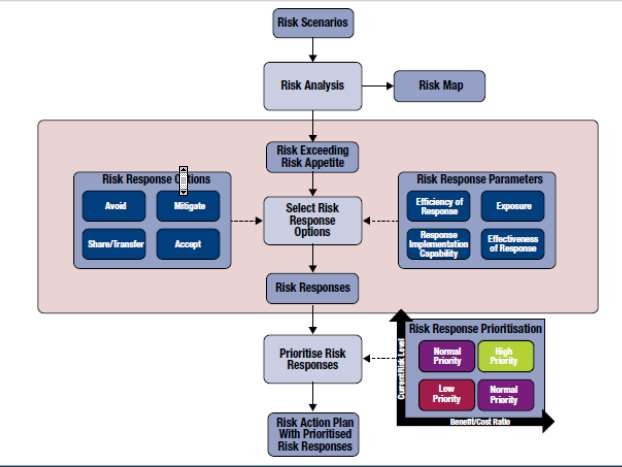
Apabila sebuah perusahaan mengadopsi risk acceptance, harus diperhatikan siapa yang menerima apalagi resiko TI. Resiko hanya boleh diterima oleh manajemen bisnis ( dan bussiness process owner ), sebuah penerimaan harus dikomunikasikan ke manajemen senior.

# 2. 3. 2. 3 Risk Sharing/Transfer

Transfer artinya mengurangi dampak atau frekuensi resiko dengan mentransfer atau membagi porsi dati resiko[4]. Teknik yang biasa digunakan yaitu asuransi dan *outsourcing*. Contohnya mengansuransikan insiden yang terkait TI, *outsourcing* bagian dari aktifitas TI, atau membagi resiko proyek TI dengan penyedia melalui penganggaran harga tetap. Teknik ini tidak meringankan sebuah perusahaan sebagai *risk ownership*, tapi dapat melibatkan ketrampilan dari pihak lain dalam mengelola resiko dan mengurangi konsekuensi finansial apabila resiko terjadi. Dilihat dari sudut pandang reputasi, transfer resiko tidak mentransfer kepemilikan atau tanggung jawab atas resiko tersebut.

# 2. 3. 2. 4 Risk Mitigation

Mitigasi resiko artinya aksi yang dilakukan untuk mengurangi frekuensi atau dampak resiko[4]. Cara ini paling sering dilakukan yaitu penguatan praktisi manajemen resiko IT, misalnya mengimplementasikan proses manajemen resiko IT yang telah didefinisikan di framework COBIT 5. Evaluasi respon risiko bukan merupakan upaya satu kali, namun merupakan bagian dari siklus proses manajemen risiko. Berikut adalah alur kerja respon risiko seperti diilustrasikan pada Gambar 2.8.



**Gambar 2. 8** Alur Kerja Respon Risiko

Dalam proses *risk response selection and prioritisation* menjelaskan bagaimana seleksi dari respon yang cocok, misalkan bagaimana cara merespon dan bagamana untuk memilih diantara opsi-opsi respon yang tersedia. Seperti yang diilustrasikan pada gambar, berikut adalah parameter yang harus diperhitungkan di proses ini :

* + Efisiensi dari sebuah respon, misalnya keuntungan relatif yang mungkin dibandingkan :
    - Investasi lain (menginvestasikan respon resiko selalu diukur dengan investasi lain)
    - Respon lain (suatu respon mungkin menangani beberapa item resiko sedangkan yang lain mungkin tidak)
  + Biaya dari respon
  + Eksposur, misalnya pentingnya resiko ditangani oleh respon, direpresentasikan pada risk map (yang mengkombinasikan antara tingkat frekuensi dan dampak)
  + Kemampuan perusahaan untuk mengimplementasikan respon, misalnya perusahaan tersebut telah matang dalam proses manajemen resikonya akan lebih memungkinkan untuk diimplementasikan daripada yang belum matang
  + Efektifitas respon, misalnya digunakan untuk mengurangi dampak resiko [4].

# 4 Perbandingan COBIT 5 dengan Standar lain

* 1. COBIT5 FOR RISK AND ISO 31000

COBIT 5 *for Risk* menangani semua prinsip yang ada di dalam ISO 31000 melalui COBIT 5 untuk prinsip dan *enabler risk*. Selain itu, proses yang didefinisikan dalam ISO 31000 sepenuhnya tercakup dalam berbagai proses dan praktik yang ada pada COBIT 5 untuk model proses Risiko. COBIT 5 *for Risk*, memberikan panduan yang lebih luas dan mencakup area yang tidak tercakup dalam ISO 31000, seperti tata kelola dan pengelolaan risiko TI.

* 1. COBIT5 FOR RISK AND ISO/IEC 27005

Proses seperti yang didefinisikan di dalam ISO / IEC 27005 sepenuhnya tercakup dalam berbagai proses dan praktik yang ada di dalam COBIT 5 untuk model proses Risiko. Model COBIT 5 for Risk memberikan panduan yang lebih luas dan juga mencakup area yang tidak tercakup oleh ISO / IEC 27005, contoh

: tata kelola risiko dan reaksi terhadap kejadian. Perbedaan yang paling mendasar antara kedua kerangka kerja tersebut adalah bahwa COBIT 5 *for Risk*

menangani sejumlah kategori risiko TI yang komprehensif, sedangkan ISO / IEC 27005 berfokus secara khusus pada risiko keamanan informasi.

* 1. COBIT5 FOR RISK AND COSO ERM

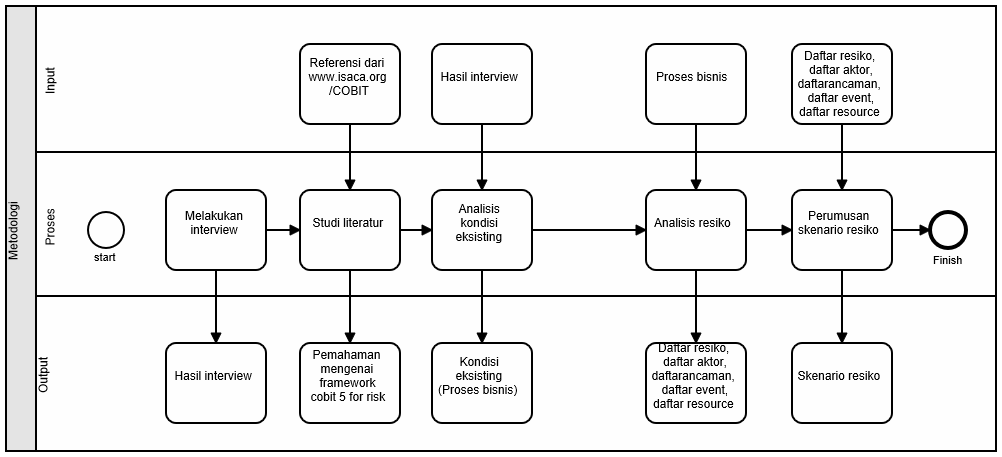
COBIT 5 *for Risk* menangani 8 komponen yang didefinisikan di dalam COSO ERM dan beberapa komponen, memperluas jangkauan COSO ERM secara spesifik dari penggunaan TI di perusahaan. Meskipun COBIT 5 *for Risk* lebih berfokus pada kontrol, namun juga memberikan keterkaitan dengan praktik pengelolaan dalam kerangka COBIT 5. Hal yang paling penting untuk kontrol dan manajemen risiko umum, seperti yang didefinisikan dalam COSO ERM, hadir dalam COBIT 5 *for Risk*, baik melalui asas itu sendiri, rancangan konseptual kerangka kerja, model proses atau panduan tambahan yang diberikan dalam kerangka kerja [3].

# BAB III METODOLOGI

Metodologi penelitian yang digunakan dalam melakukan analisis resiko menggunakan *framework* COBIT 5 dengan menggunakan proses APO12 (Manage Risk) di Dinas Perindustrian dan Tenaga Kerja.

APO12 bertujuan untuk mengidentifikasi dan menilai risiko yang ada dalam organisasi. Dengan APO12, organisasi juga dapat melakukan integrasi manajemen risiko TI dengan manajemen risiko yang ada pada perusahaan. Dan untuk pengerjaan tugas ini, kami hannya melakukan kegiatan yang ada dalam APO12 sebatas analisa dan skenario risiko saja.

Bagian ini menjelaskan metodologi yang digunakan dalam pengerjaan tugas ini. Metodologi ini diperlukan sebagai panduan secara sistematis dalam pengerjaan tugas. Metodologi penelitian dari laporan ini disajikan dalam flowchart sebagai berikut :



Daftar resiko

Daftar resiko

**Gambar 3. 1** Metodologi APO12

# Melakukan Interview

Pada tahapan ini kelompok kami melakukan wawancara kepada Bapak Suparman sebagai Kepala Bidang Penempatan Tenaga Kerja dan Transmigrasi untuk melakukan penggalian data serta kondisi terkini Dinas Perindustrian dan Tenaga Kerja Kabupaten Trenggalek. Output dari interview itu sendiri adalah data hasil wawancara yang akan menjadi inputan pada proses selanjutnya yaitu analisis kondisi eksisting sehingga kelompok kami dapat menganalisa resiko yang ada di Dinas Perindustrian dan tenaga Kerja Kabupaten Trenggalek.

# Studi Literature

Pada tahapan ini kelompok kami melakukan pencarian studi literature yang terkait dengan APO 12, COBIT 5 dan COBIT 5 for Risk. Selain itu juga menelusuri sumber- sumber tulisan yang pernah dibuat sebelumnya terkait dengan manajemen resiko. Pencarian sumber-sumber studi literature ini dilakukan agar kelompok kami memiliki pemahaman yang luas serta dapat dengan mudah melakukan penerapan manajemen risiko berdasarkan COBIT 5 dan APO 12 pada Dinas Perindustrian dan Tenaga Kerja Kabupaten Trenggalek.

# Analisis Kondisi Eksisting

Tahapan ini dilakukan berdasarkan data hasil wawancara yang telah dilakukan pada tahapan Interview. Pada tahapan ini akan dilakukan analisan pada kondisi kenyataan saat ini pada Dinas Perindustrian dan tenaga Kerja Kabupaten Trenggalek. Analisa yang dilakukan meliputi proses bisnis, struktur organisasi serta sistem keamanan yang ada di Dinas Perindustrian dan tenaga Kerja Kabupaten Trenggalek. Output pada tahapan ini adalah proses bisnis atau kondisi eksisting itu sendiri yang akan digunakan sebagai input pada tahapan analisis risiko yang mungkin terjadi.

# Analisis Risiko

Analisis risiko perusahaan diperlukan untuk mengetahui kemungkinan risiko yang akan terjadi pada Dinas Perindustrian dan tenaga Kerja Kabupaten Trenggalek. Risiko yang didapat akan diidentifikasi berdasarkan aktivitas, kategori dan tipe, penyebab, serta faktor dari risiko tersebut yang kemudian nantinya akan digunakan dalam menentukan skenario risiko.

# Identifikasi Risiko Setiap Aktivitas DSS05

Tahapan ini ialah pengidentifikasian aktivtas berdasarkan DSS05. DSS05 itu sendiri berbicara mengenai keamanan. Output dari proses ini ialah daftar aktivtas yang teridentifikasi berdasarkan DSS05.

# Mengidentifikasi Kategori dan Tipe Risiko

Pada tahapan ini risiko yang telah teridentifikasi sebelumnya dikategorikan berdasarkan beberapa kategori dan tipe. Output pada tahapan ini ialah daftar risiko yang telah terkategorikan.

# Analisis Penyebab Risiko

Pada tahapan ini risiko yang telah teridentifikasi dianalisis penyebabnya. Output pada tahapan ini ialah daftar risiko dan penyebab terjadi risiko tersebut.

# Perumusan Skenario Resiko

Tahapan perumusan scenario risiko ini dilakukan untuk setiap risiko. Scenario risiko merupakan dampak bila terjadi risiko tersebut yang dibedakan menjadi dampak positif dan negative. Untuk melakukan perumusan scenario risiko menggunakan hasil dari tahapan analisis risiko.

# BAB IV HASIL DAN PEMBAHASAN

# Melakukan Studi Literatur

Studi literatur merupakan metode pengumpulan data yang didapat dari hasil penelitian yang telah dilakukan sebelumnya. Kami melakukan studi literatur dari berbagai macam referensi COBIT 5 For Risk dalam bentuk *pdf* maupun *file power point* yang membahas mengenai COBIT 5.

Adapun faktor yang harus diperhatikan dalam melakukan studi literatur yaitu : Diperlukannya sumber dari literatur yang relevan yang meliputi buku, presentasi, makalah ilmiah, hasil penelitian, tesis dan sumber-sumber lainnya yang sesuai dan memperhatikan keselarasan dengan tujuan penilitian.

# Analisis Kondisi Eksisting

Hasil wawancara menghasilkan kondisi eksisting pada Dinas Perindustrian dan Tenaga Kerja Kabupaten Trenggalek. Berikut merupakan kondisi eksisting pada dinas perindustrian dan tenaga kerja kabupaten trenggalek.

# Struktur Organisasi Dinas Perindustrian dan Tenaga Kerja Kabupaten Trenggalek

Pada gambar 4.1 merupakan struktur organisasi dari dinas perindustrian dan Tenaga Kerja Kabupaten Trenggalek. Dinas ini memiliki tiga bidang yaitu bidang perindustrian, bidang penempatan tenaga kerja dan transmigrasi, dan bidang hubungan industrial. Tidak terlihat bidang yang menangani khusus IT dalam struktur organisasi tersebut. Di antara ketiga bidang tersebut hanya bidang penempatan tenaga kerja dan transmigrasi yang memakai aplikasi IT dalam proses bisnisnya.

Bidang penempatan kerja dan transmigrasi membawahi tiga seksi yakni seksi pelatihan dan produktifitas tenaga kerja, seksi penempatan dan perluasan kesempatan kerja, dan seksi transmigrasi. Pada bidang penempatan tenaga kerja dan transmigrasi memiliki layanan publik yang bernama SISKOTKLN (Sistem

Komputerisasi Tenaga Kerja Luar Negeri) yang memanfaatkan aplikasi untuk mengintegrasikan proses layanan publiknya. Untuk proses manajemen resiko kami berfokus pada layanan publik SISKOTKLN pada bidang penempatan tenaga kerja dan transmigrasi.

BIDANG HUBUNGAN INDUSTRIAL

BIDANG PENEMPATAN TENAGA KERJA DAN TRANSMIGRASI

BIDANG PERINDUSTRIAN

KELOMPOK JAB. FUNGSIONAL

SEKRETARIS DINAS

KEPALA DINAS

SEKSI PENYELESAIAN PERSELISIHAN HUBUNGAN INDUSTRIAL

SEKSI TRANSMIGRASI

SEKSI STANDARISASI DAN DESAIN PRODUK

SEKSI KESEJAHTERAAN DAN JAMSOSTEK

SEKSI SYARAT KERJA

SEKSI PENEMPATAN DAN PERLUASAN KESEMPATAN KERJA

SEKSI INDUSTRI NON ARGO

SEKSI ELATIHAN DAN PRODUKTIFITAS TENAGA KERJA

SEKSI INDUSTRI ARGO

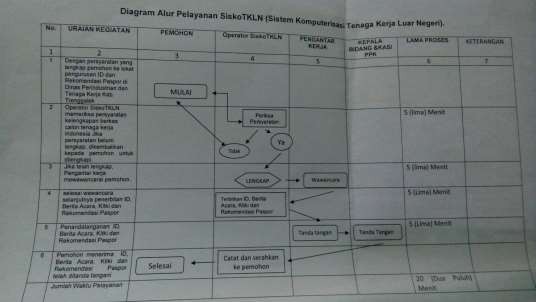
SUB BAGIAN KEUANGAN, PELAPORAN DAN PERENCANAAN

SUB BAGIAN UMUM DAN KEPEGAWAIAN

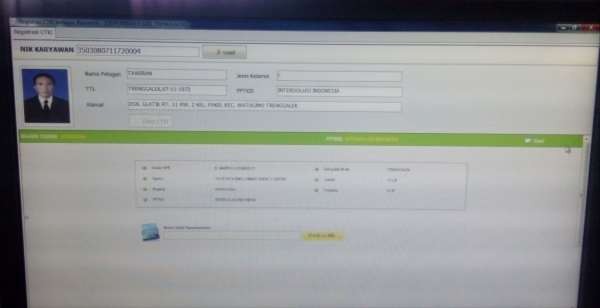
**Gambar 4. 1** Struktur Organisasi Dinas Perindustrian dan Tenaga Kerja

# Proses Bisnis Layanan publik SISKOTKLN

SISKOTKLN merupakan singkatan dari Sistem Komputerisasi Tenaga Kerja Luar Negeri. SISKOTKLN adalah salah satu layanan publik pada dinas Perindustrian dan Tenaga Kerja tepatnya pada bidang Tenaga Kerja dan Transmigrasi. Sistem ini berfungsi sebagai pendataan bagi Calon Tenaga Kerja Indonesia yang akan berangkat keluar negeri. Dapat dilihat pada Gambar 4.2 dan Gambar 4.3 dimana setiap Calon TKI Kabupaten Trenggalek akan menyerahkan persyaratan ke loket pengurusan ID dan Rekomendasi Paspor di Dinas Perindustrian dan Tenaga Kerja Kabupaten Trenggalek. Kemudian Operator SiskoTKLN memeriksa persyaratan kelengkapan berkas calon tenaga kerja Indonesia. Jika persyaratan belum lengkap akan dikembalikan kepada pemohon untuk dilengkapi. Apabila persyaratan telah lengkap, Pengantar Kerja mewawancarai pemohon. Selesai wawancara dilanjutkan dengan penerbitan ID, Kitki, Berita Acara dan Rekomendasi Paspor dan penandatanganan oleh Pengantar Kerja dan Kepala Bidang dan Aksi PPK. Kemudian pemohon menerima ID, Kitki, Berita Acara dan Rekomendasi Paspor.



**Gambar 4. 2** Alur Pelayanan SISKOTKLN



Gambar 4. 3 Aplikasi SISKOTKLN

|  |  |  |
| --- | --- | --- |
| **No** | **Proses bisnis** | **Sub Process** |
| 1 | Pelatihan dan produktivitas tenaga kerja | Menyiapkan informasi regulasi bidang pelatihan kerja yang akan disebarluaskan kepada lembaga  pelatihan kerja swasta |
| Menyiapkan rancangan kesiapan materi pelatihan, kurikulum dan  silabus pelatihan |
| Menyiapkan bahan koordinasi penyelenggaraan pelatihan berbasis  kompetensi |
| Menyiapkan program pelatihan, tenaga instruktur dan tenaga pelatihan serta sarana dan prasarana  pelatihan kerja |

|  |  |  |
| --- | --- | --- |
|  |  | Menyiapkan data dan metode pengukuran produktivitas serta merencanakan pemantauan tingkat  produktivitas |
| Menyiapkan sumber daya manusia  bidang konsultasi produktivitas dan pengukuran produktivitas |
| Melaksanakan kegiatan pelatihan  dan produktivitas tenaga kerja |
| 2 | Layanan publik SISKOTKLN dengan aplikasi siskotkln | Input data calon TKI |
| Pemasangan antivirus terhadap  aplikasi |
| Melakukan aktivasi *firewall* |
| Mengelola network untuk  menjalankan aplikasi |
| Mengelola hak akses terhadap  aplikasi |
| 3 | Transmigrasi | Menyiapkan data animo  transmigrasi/calon transmigran; |
| Melaksanakan koordinasi dalam pelaksanaan penjajagan kerjasama penyelenggaraan transmigrasi ke  daerah transmigrasi |
| Menyiapkan bahan koordinasi dengan pihak terkait dalam pembahasan naskah perjanjian kerjasama penyelenggaraan  transmigrasi |
| Melaksanakan koordinasi dalam  rangka pelaksanaan kerjasama |

|  |  |  |
| --- | --- | --- |
|  |  | penyelenggaraan transmigrasi  dengan pemerintah daerah transmigrasi |
| Melaksanakan peninjauan/monitoring ke lokasi  transmigrasi |
| Menyiapkan bahan fasilitasi dan penyuluhan/sosialisasi  ketransmigrasian |
| Menyiapkan bahan seleksi calon  transmigran |
| Menyiapkan bahan pembinaan,  pelatihan dan pemberangkatan transmigran |

**Tabel 4.1** Proses Bisnis dan Sub Proses Bisnis

# Pemilihan dan Pemetaan Proses Bisnis sesuai COBIT 5 Enabling Process

Pada tahap ini akan dilakukan pemilihan proses bisnis dengan kriteria yang mendekati proses yang ada pada COBIT 5 Enabling Process. Setelah kami melakukan analisis akhirnya ditetapkan proses bisnis yang akan diidentifikasi risikonya adalah proses bisnis layanan publik SISKOTKLN dengan aplikasi siskotkln. Hal ini diputuskan karena terdapat proses yang khusus tentang hal tersebut dalam DSS05 (Manage Security). Selain itu detail Key Management Process yang ada pada DSS05 juga memiliki kaitan dengan tiap aktivitas yang ada dalam proses manage security yang dilakukan oleh Dinas Perindustrian dan Tenaga Kerja. Berikut penjabaran aktivitas dari setiap sub proses dari proses bisnis Tenaga Kerja

Kabupaten Trenggalek yang terdapat pada layanan publik SISKOTKLN dengan aplikasi siskotkln :

|  |  |  |
| --- | --- | --- |
| **Sub Proses** | **Detail Aktivitas** | **Aktivitas DSS05** |
| Input data calon TKI | 1. Menerima CTKI | - |
| 2. Petugas mengisikan biodata  CTKI | - |
| 3. Petugas mengisikan nomor  SPR CTKI | DSS05.04 |
| 4. Petugas mengisikan agensi  CTKI | DSS05.04 |
| 5. Petugas mengisikan negara  tujuan CTKI | DSS05.04 |
| 6. Petugas mengisikan status  penempatan CTKI | DSS05.04 |
| Pemasangan antivirus terhadap aplikasi | 1. Petugas melakukan  pengidentifikasian antivirus yang sesuai | DSS05.01 |
| 2. Melakukan pemasangan  antivirus | DSS05.01 |
| 3. Melakukan scan terhadap  aplikasi | DSS05.01 |
| 4. Melakukan update antivirus  secara berkala | DSS05.01 |
| Melakukan aktivasi *firewall*  Mengel | 1. Melakukan aktivasi *firewall*  kepada seluruh perangkat keras yang ada | DSS05.02 |

|  |  |  |
| --- | --- | --- |
|  | 2. Melakukan pemantauan  terhdap aktivitas keluar masuknya data | DSS05.02 DSS05.07 |
| Mengelola network untuk menjalankan aplikasi | 1.Melakukan *maintenance*  terhadap jaringan *(network)* yang ada | DSS05.02 |
| 2. Melakukan pengecekan dan pemantauan pada jaringan  komputer | DSS05.02 DSS05.07 |
| Mengelola hak akses terhadap aplikasi | 1.Akses untuk komputer milik  dinas hanya dapat dilakukan oleh staf operasional yang bertugas | DSS05.04 DSS05.05 |
| 2.Jika terdapat staf baru yang bertindak sebagai operasional maka akan dilakukan pemberian hak akses kepada staf baru  tersebut | DSS05.04 DSS05.05 |

**Tabel 4.2** Pemetaan Proses Bisnis Sesuai COBIT 5

Dari data yang baru saja dijabarkan didapat kesimpulan *activity gap* kegiatan yang dikerjakan oleh Dinas Perindustrian dan Tenaga Kerja Kabupaten Trenggalek dengan detail aktivitas dalam DSS05 yang adalah sebagai berikut :

|  |  |  |
| --- | --- | --- |
| **Key Management**  **Practice** | **Aktivitas** | **Activity Gap** |
| DSS05.01  Praktik khusus yang | 1.Mengkomunikasikan  kesadaran terhadap | Sudah |

|  |  |  |
| --- | --- | --- |
| membentuk proses  mengelola layanan  keamanan, seperti perlindungan terhadap malware yang harus diimplementasikan melalui sistem deteksi ancaman. | malware dan menerapkan  prosedur pencegahan |  |
| 2.Menginstal dan aktivasi tools proteksi terhadap *malware* untuk semua  fasilitas pemrosesan | Sudah |
| 3.Mengkonfigurasi semua proteksi terhadap *software* berbahaya secara  terpusat | Belum |
| 4.Melakukan *review* secara teratur dan evaluasi informasi terhadap  potensi ancaman baru | Belum |
| 5.Menerapkan filter terhadap *traffic* yang masuk seperti *email* dan  *download* | Belum |
| 6.Mengadakan pelatihan pada staf-staf tentang *malware* pada *email* dan  penggunaan internet | Belum |
| DSS05.02  Melakukan *manage* terhadap jaringan dan konektivitas dari keamanan sistem. | 1.Membuat kebijakan  untuk keamanan konektivitas berdasarkan  penilaian risiko. | Belum |
| 2.Menentukan otorisasi  terhadap devices yang boleh mengakses | Sudah |

|  |  |  |
| --- | --- | --- |
|  | informasi institusi dan  jaringan insitusi. |  |
| 3.Membuat mekanisme filtering untuk jaringan seperti firewalls dan intrusion detection  software. | Belum |
| 4.Menerapkan enkripsi  informasi saat pengiriman berdasarkan klasifikasinya. | Sudah |
| 5.Menerapkan protokol keamanan yang telah disetujui untuk  konektivitas jaringan. | Sudah |
| 6.Melakukan konfigurasi peralatan jaringan dengan  aman. | Sudah |
| 7.Membangun mekanisme yang terpercaya untuk mendukung transmisi yang  aman. | Belum |
| 8.Mengadakan penetration test atau simulasi untuk melihat  kehandalan jaringan. | Belum |
| 9.Menguji sistem keamanan secara berkala untuk menentukan kecukupan sistem  perlindungan. | Belum |

|  |  |  |
| --- | --- | --- |
| DSS05.03  Melakukan *manage* terhadap *end-point* dari keamanan sistem | Mengkonfigurasi sistem  operasi dengan cara yang aman | Sudah |
| Membuat mekanisme  *lockdown* untuk perangkat-perangkat TI | Belum |
| Mengenkripsi informasi pada penyimpanan/*storage* sesuai dengan  klasifikasinya | Belum |
| Mengatur *remote access*  *and control* | Belum |
| Mengkonfigurasi jaringan  dengan cara aman | Sudah |
| Mengimplementasi *traffic filtering* pada jaringan di  perangkat *endpoints* | Belum |
| Melindungi dan menjaga  integritas sistem | Belum |
| Apakah dilakukan proteksi secara fisik untuk  perangkat *endpoint* | Sudah |
| Membuang *devices* yang tidak terpakai lagi dengan  cara yang benar dan aman | Sudah |
| DSS05.04  Melakukan *manage*  terhadap identitas dari | 1.Menjaga hak-hak akses user sesuai dengan fungsi bisnis dan kebutuhan  prosesnya. | Sudah |

|  |  |  |
| --- | --- | --- |
| *user* dan juga gak akses yang *logical.* | 2.Memastikan bahwa semua peran-peran telah terdefinisi dengan baik dan  unique untuk tiap peran. | Sudah |
| 3.Melakukan authentication semua akses terhadap aset informasi berdasarkan  klasifikasi keamanannya. | Sudah |
| 4.Mengatur siapa yang dapat melakukan perubahan terhadap hak- hak akses (create,  modification, delete). | Sudah |
| 5.Memisahkan dan mengelola *privileged user*  *account.* | Sudah |
| 6.Melakukan review  manajemen secara teratur/rutin mengenai semua akun dan hak-hak terkait. | Belum |
| 7.Memastikan bahwa semua user dan aktivitasnya secara *unique*  telah teridentifikasi. | Belum |
| 8.Melakukan audit terhadap akses informasi- informasi yang bersifat  sangat sensitif. | Belum |

|  |  |  |
| --- | --- | --- |
| DSS05.05  Melakukan *manage* terhadap akses fisik ke aset Teknologi Informasi (akses ke komputer) | Mengelola permintaan  dan pemberian akses ke fasilitas TI | Sudah |
| Memastikan bahwa profil  akses tidak berubah-ubah | Sudah |
| Menginstruksi kepada semua staf untuk memakai tanda pengenal yang  terlihat | Sudah |
| Menemani pengunjung  yang masuk ke IT sites dan tidak ditinggal sendirian | Sudah |
| Membangun pembatasan akses ke bagian lingkungan TI yang sensitive (pagar,  dinding) | Belum |
| Mengadakan pelatihan  atau training tentang kesadaran keamanan fisik. | Belum |
| DSS05.06  Melakukan *manage* terhadap dokumen atau data yang sensitive dengan melakukan perlindungan oleh kontrol yang bagus. | 1.Pengaturan penggunaan dan pembuangan form sensitif dan output devices baik di dalam/luar  institusi. | Belum |
| 2.Pengaturan hak untuk mengakses dokumen sensitif dan perangkat  output. | Sudah |

|  |  |  |
| --- | --- | --- |
|  | 3.Pembuatan inventarisasi |  |
| dokumen yang sensitif dan | Belum |
| perangkat output. |  |
| 4.Pemberian perlindungan |  |
| fisik secara tepat terhadap  dokumen yang sensitif dan | Belum |
| perangkat output. |  |
| 5.Penghancuran informasi |  |
| sensitif dan perangkat  output dengan cara yang | Belum |
| tepat. |  |
|  | 1.Mencatat events yang |  |
|  | berkaitan dengan |  |
|  | keamanan yang diperoleh | Sudah |
|  | dari alat-alat pemantau |  |
|  | keamanan. |  |
|  | 2.Menetapkan sifat dan |  |
| DSS05.07  Memantau infrastruktur dari seluruh kegiatan yang berhubungan dengan keamaanan. | karakteristik inisiden potensial yang berhubungan dengan  keamanan. | Sudah |
| 3.Melakukan review  secara rutin terhadap event logs untuk insiden- | Belum |
|  | insiden yang potensial. |  |
|  | 4.Memelihara prosedur |  |
|  | dalam mengumpulkan  bukti-bukti security | Belum |
|  | events. |  |

|  |  |  |
| --- | --- | --- |
|  | 5.Memastikan *incident*  *tickets* dibuat dengan tepat waktu. | Belum |

**Tabel 4.3** Activity GAP

# Analisis Risiko Perusahaan

Pada tahapan ini akan dilakukan identifikasi dari risiko yang berdasarkan pada data yang telah didapat dari metodologi sebelumnya, yang nantinya pada akhir kegiatan akan didapatkan nilai analisis yang dapat digunakan untuk merumuskan *risk profile*.

# Identifikasi Risiko Setiap Aktivitas DSS05

Dalam tahapan ini akan dilakukan identifikasi risiko berdasarkan pada setiap detail aktivitas pada KMP DSS05. Adapun detail aktivitas sekaligus identifikasi risiko yang adalah sebagai berikut :

|  |  |  |  |
| --- | --- | --- | --- |
| **Key Management**  **Practice** | **Aktivitas** | **Activity**  **Gap** | **Risiko** |
| DSS05.01 | Mengkomunikasikan | Sudah | D1001 - Adanya ketidak |
| Praktik khusus yang | kesadaran terhadap |  | tahuan mengenai |
| membentuk proses | malware dan menerapkan |  | pentingnya prosedur |
| mengelola layanan | prosedur pencegahan |  | pencegahan. |
| keamanan, seperti |  |  | D1002 - Tidak adanya |
| perlindungan |  |  | pengetahuan untuk |
| terhadap malware |  |  | mengatasi masalah |
| yang harus |  |  | keamanan |

|  |  |  |  |
| --- | --- | --- | --- |
| diimplementasikan melalui sistem deteksi ancaman. | Menginstal dan aktivasi tools proteksi terhadap malware untuk semua fasilitas  pemrosesan. | Sudah | D1003 - Tools yang digunakan masih rentan terhadap malware |
| Mengkonfigurasi semua proteksi terhadap software berbahaya secara terpusat. | Belum | D1004 - Tidak adanya pengawasan secara terpusat sehingga memudahkan acaman untuk masuk dari  berbagai celah |
| Melakukan review secara teratur dan evaluasi informasi terhadap potensi  ancaman baru. | Belum | D1005 - Tidak siap dalam menghadapi ancaman D1008 - Tidak adanya  mitigasi ancaman |
| Menerapkan filter terhadap traffic yang masuk seperti email dan download. | Belum | D1006 - Bebasnya data yang masuk sehingga lebih rentan akan  penyebaran malware |
| Mengadakan pelatihan pada staf-staf tentang malware pada email dan penggunaan  internet. | Belum | D1007 – Penanganan terhadap ancaman keamanan tidak dapat  dilakukan dengan tepat |
| DSS05.02  Melakukan *manage* terhadap jaringan dan konektivitas dari keamanan sistem. | Membuat kebijakan untuk keamanan konektivitas berdasarkan penilaian risiko. | Belum | D2001 - Tidak adanya tindakan yang jelas apabila keamanan  konektivitas terancam. |
| Menentukan otorisasi terhadap  *devices* yang boleh | Sudah | D2002 - Perlu adanya tindakan intensif dan berkala untuk  melakukan otorasi |

|  |  |  |  |
| --- | --- | --- | --- |
|  | mengakses informasi institusi dan jaringan insitusi. |  | sehingga diperlukan resource yang berfokus melakukan pengecekkan  berkala. |
| Membuat mekanisme *filtering* untuk jaringan seperti *firewalls* dan intrusion detection *software* | Belum | D2003 - Tidak adanya *filtering* jaringan dapat membahayakan keselamatan komputer  dari kejahatan malware. |
| Menerapkan enkripsi informasi saat pengiriman berdasarkan klasifikasinya. | Sudah | D2004 - Butuh tenaga IT untuk melakukan *maintenance* dan hal ini akan menyebabkan penambahan biaya  untuk *resource* baru ini. |
| Menerapkan protokol keamanan yang telah disetujui untuk konektivitas jaringan | Sudah | D2005 - Butuh tenaga IT untuk melakukan *maintenance* dan hal ini akan menyebabkan penambahan biaya  untuk *resource* baru ini. |
| Melakukan konfigurasi peralatan jaringan dengan aman | Sudah | D2006 - Butuh tenaga IT untuk melakukan *maintenance* dan hal ini akan menyebabkan penambahan biaya untuk *resource* baru ini. Selain itu, teknologi terus berkembang,  penjahat akan berusaha |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | mencari celah sehingga |
| organisasi perlu |
| melakukan *upgrading* |
| terhadap peralatan |
| jaringan agar lebih |
| aman. |
| Membangun mekanisme | Belum | D2007 - Celah keamanan |
| yang terpercaya untuk |  | masih besar sehinga |
| mendukung transmisi yang |  | peluang untuk |
| aman. |  | melakukan kejahatan |
|  |  | juga besar. |
| Mengadakan *penetration* | Belum | D2008 - Tingkat |
| *test* atau simulasi untuk |  | performa dari aplikasi |
| melihat kehandalan |  | yang ada pada organisasi |
| jaringan. |  | tidak maksimal sehingga |
|  |  | saat digunakan dapat |
|  |  | terjadi kerusakan. |
| Menguji sistem keamanan | Belum | D2009 - Data-data yang |
| secara berkala untuk |  | ada dalam komputer |
| menentukan kecukupan |  | organisasi dapat tercuri |
| sistem perlindungan. |  | dan komputer dapat |
|  |  | terserang malware. |
|  | Mengkonfigurasi sistem | Sudah | D3001 - Kemungkinan |
| DSS05.03  Melakukan *manage* terhadap *end-point* dari keamanan sistem. | operasi dengan cara yang  aman. |  | untuk terjangkit  malware lebih kecil |
| Membuat mekanisme lockdown untuk perangkat- perangkat TI. | Belum | D3002 -  Pencurian perangkat TI  beserta media atau file penting lain yang |
|  |  |  | melekat pada perangkat |

|  |  |  |  |
| --- | --- | --- | --- |
|  | Mengenkripsi informasi pada penyimpanan/storage sesuai dengan klasifikasinya. | Belum | D3003 -  Terjadi modifikasi informasi hasil  pembobolan dari  penyimpanan |
| Mengatur remote access and control. | Belum | D3004 – Terdapat peluang me-remote  sistem secara tidak legal |
| Mengkonfigurasi jaringan dengan cara aman. | Sudah | D3005 – Kemungkinan  celah keamanan untuk dibobol lebih kecil |
| Mengimplementasi traffic filtering pada jaringan di perangkat endpoints. | Belum | D3006 – Tereksposnya data-data yang bersifat rahasia dengan memanfaatkan celah pada jaringan dan  komputer |
| Melindungi dan menjaga integritas sistem. | Belum | D3007 – Terdapat celah keamanan dalam perlindungan terhadap manipulasi dan  modifikasi sistem |
| Apakah dilakukan proteksi secara fisik untuk perangkat endpoint. | Sudah | D3008 –Masih terdapat peluang celah keamanan secara logical melalui  jaringan |
| Membuang devices yang  tidak terpakai lagi dengan cara yang benar dan aman. | Sudah | D3009 – Meminimalisir  eksploitasi devices yang tidak terpakai untuk |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | mendapat informasi  tertentu |
| DSS05.04  Melakukan *manage* terhadap identitas dari *user* dan juga gak akses yang *logical.* | Menjaga hak-hak akses user sesuai dengan fungsi bisnis dan kebutuhan prosesnya | Sudah | D4001 - Pembobolan terhadap sistem aplikasi |
| Memastikan bahwa semua peran-peran telah terdefinisi dengan baik dan *unique*  untuk tiap peran. | Sudah | D4002 - Munculnya peran fungsi yang redudansi |
| Melakukan *authentication* semua akses terhadap aset informasi berdasarkan  klasifikasi keamanannya. | Sudah | D4003 - Sistem aplikasi akan dirusak oleh hacker/cracker/malware |
| Mengatur siapa yang dapat melakukan perubahan terhadap hak-hak akses *(create,*  *modification, delete).* | Sudah | D4004 - Terjadi modifikasi data secara liar |
| Memisahkan dan mengelola  *privileged user account* | Sudah | D4005 - Masih ada  session dari account lain |
| Melakukan *review*  manajemen secara  teratur/rutin mengenai semua akun dan hak-hak  terkait. | Belum | D4006 - Tidak dapat memantau aktivitas akun |
| Memastikan bahwa semua user dan aktivitasnya secara  *unique* telah teridentifikasi. | Belum | D4007 - User dapat  mengakses tanpa batasan tertentu |

|  |  |  |  |
| --- | --- | --- | --- |
|  | Melakukan audit terhadap akses informasi-informasi yang bersifat sangat sensitif. | Belum | D4008 - Tidak dapat mengetahui cara penanganan informasi  sensitif |
| DSS05.05  Melakukan *manage* terhadap akses fisik ke aset Teknologi Informasi (akses ke komputer). | Mengelola permintaan dan pemberian akses ke fasilitas TI. | Sudah | D5001 - Terdapat penyalahgunaan hak akses melalui social engineering dan teknik  lainnya |
| Memastikan bahwa profil akses tidak berubah-ubah. | Sudah | D5002 - Adanya penyalahgunaan hak  akses |
| Menginstruksi kepada semua staf untuk memakai tanda pengenal yang terlihat. | Sudah | D5003 - Adanya  pemalsuan tanda pengenal dan informasi dari tanda pengenal yang dapat menjadi  celah |
| Menemani pengunjung yang masuk ke IT sites dan tidak ditinggal sendirian. | Sudah | D5004 – Pengunjung harus selalu ditemani oleh staff yang memiliki tanggung jawab atas  pengunjung tersebut. |
| Membangun pembatasan akses ke bagian lingkungan TI yang sensitif (pagar, dinding). | Belum | D5005 - Mudahnya pembobolan pada akses lingkungan TI yang sensitive sehingga dapat menimbulkan pencurian  asset |

|  |  |  |  |
| --- | --- | --- | --- |
|  | Mengadakan pelatihan / training tentang kesadaran keamanan fisik. | Belum | D5006 - Tidak adanya aware mengenai  masalah keamanan sehingga kurangnya ilmu untuk melakukan pencegahan sehingga pencegahan tidak dapat  dilakukan dengan tepat |
| DSS05.06  Melakukan *manage* terhadap dokumen atau data yang sensitive dengan melakukan perlindungan oleh kontrol yang bagus. | Pengaturan penggunaan dan pembuangan form sensitif dan  *output devices* baik di  dalam/luar institusi. | Belum | D6001 – Human error dalam melakukan kesalahan pengelolaan form sensitif |
| Pengaturan hak untuk mengakses dokumen sensitif dan perangkat  *output.* | Sudah | D6002 – Pembobolan hakses dari pihak yang tidak berwenang |
| Pembuatan inventarisasi dokumen yang sensitif dan  perangkat *output.* | Belum | D6003 – Terbobolnya inventaris sehingga data  tersebar |
| Pemberian perlindungan fisik secara tepat terhadap dokumen yang sensitif dan perangkat  *output.* | Belum | D6004 – Perusakan terhadap perlindungan fisik sehingga data sensitive dapat dicuri |
| Penghancuran informasi sensitif dan perangkat *output* dengan cara yang  tepat. | Belum | D6005 – Informasi dihancurkan secara tidak tepat karena human  error |

|  |  |  |  |
| --- | --- | --- | --- |
| DSS05.07  Memantau infrastruktur dari seluruh kegiatan yang berhubungan dengan keamaanan. | Mencatat events yang berkaitan dengan keamanan yang diperoleh dari alat-alat pemantau keamanan. | Sudah | D7001 - Masih terdapat celah yang dapat kecolongan meskipun ada alat pemantau  keamanan |
| Menetapkan sifat dan karakteristik inisiden potensial yang berhubungan dengan keamanan. | Sudah | D7002 - Masih terdapat insiden yang terjadi yang belum teridentifikasi sifat dan  karakteristiknya |
| Melakukan review secara rutin terhadap event logs untuk insiden-insiden yang  potensial. | Belum | D7003 - Tidak  mengetahui insiden  potensial dan cara penanganannya |
| Memelihara prosedur dalam mengumpulkan bukti-bukti security events. | Belum | D7004 - Tidak tahu bagaimana menentukkan penanganan terhadap  keamanan |
| Memastikan incident tickets dibuat dengan tepat waktu. | Belum | D7005 - Tidak dapat melakukan proses  eskalasi |

**Tabel 4.4** Risiko pada Aktivitas DSS05

# Mengidentifikasi Kategori dan Tipe Risiko

Pada tahapan ini akan dilakukan identifikasi kategori risiko berdasarkan 20 kategori risiko yang telah distandardisasi dalam COBIT 5 for Risk. 20 Kategori risiko tersebut adalah:

1. Portofolio establishment and maintenance
2. Programmer/ projects life cycle management
3. IT investment decision making
4. IT expertise and skills
5. Staff operations
6. Information
7. Architectural
8. Infrastructure
9. Software
10. Business ownership of IT
11. Supplier selection/performance, contractual compliance, termination of service and transfer
12. Regulatory compliance
13. Geopolitical
14. Insfrastructure theft or destruction
15. Malware
16. Logical Attacks
17. Industrial Action
18. Environmental
19. Acts of Nature
20. Innovation

Selain itu dalam tahapan ini akan dibuat daftar risiko yang nantinya akan didokumentasikan dan dilakukan penentuan tipe risiko , dimana tipe risiko dibagi menjadi tiga, yaitu :

* 1. IT Benefit / Value Enablement Risk akan diisi dengan ‘P’ (Primer) apabila risiko terkait TI sebagai enabler untuk meningkatkan solusi bisnis, jika tidak terkait maka akan diisi dengan ‘S’ (Sekunder)
  2. IT Programme and Project Delivery Risk akan diisi dengan ‘P’ (Primer) apabila risiko terkait dengan program dan proyek TI, jika tidak terkait maka akan diisi dengan ‘S’ (Sekunder)
  3. IT Operations and Service Delivery Risk akan diisi dengan ‘P’ (Primer) apabila risiko terkait dengan ketersediaan layanan, stabilitas operasional dan gangguan layanan, jika tidak terkait maka akan diisi dengan ‘S’ (Sekunder)

Berikut merupakan hasil kategorisasi dan identifikasi tipe risiko:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk Category** | **Risk** | **Risk Type** | | |
| **IT Benefit/ Value Enablement Risk** | **Risk IT**  **Programme & Project Delivery**  **Risk** | **IT**  **Operations & Service Delivery Risk** |
| Staff Operations | D1001 | S | P | P |
| D1008 | P | P | P |
| D1007 | P | P | P |
| D1005 | S | P | P |
| D1002 | S | S | P |
| D2001 | S | P | S |
| D2002 | P | P | P |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | D2004 | P | S | P |
| D2005 | P | S | P |
| D2006 | P | S | P |
| D4002 | P | S | S |
| D4005 | S | S | P |
| D4007 | S | P | P |
| D4006 | S | S | P |
| D5003 | P | S | S |
| D5006 | S | P | P |
| D6001 | P | S | P |
| D7003 | P | S | P |
| D7004 | P | S | P |
| D7005 | S | S | P |
| Information | D2009 | P | P | S |
| D3003 | P | S | P |
| D3006 | S | P | P |
| D3007 | S | P | P |
| D3009 | S | P | S |
| D4004 | P | S | S |
| D4008 | P | S | S |
| D5001 | P | S | P |
| D5002 | P | S | P |
| D6002 | P | P | P |
| D6003 | P | S | P |
| D6005 | P | S | P |
| Infrastructure | D3008 | P | S | P |
| D5004 | P | S | S |
| D6004 | P | P | P |
| Software | D1004 | P | P | P |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | D3005 | S | S | S |
| D4001 | P | P | P |
| D4003 | S | P | P |
| Malware | D1003 | S | P | P |
| D1006 | S | P | P |
| D2003 | S | P | P |
| D3001 | S | P | S |
| Environment | D2007 | P | P | S |
| D3002 | S | S | P |
| D3004 | S | P | S |
| D5005 | P | P | P |
| D7001 | S | S | P |
| D7002 | S | S | S |

**Tabel 4.5** Identifikasi Tipe Risiko

# Analisis Penyebab Risiko

Tahapan ini akan dilakukan analisis penyebab dari skenario yang telah diidentifikasi sebelumnya. Adapun tabel pemetaan penyebab risiko adalah sebagai berikut :

|  |  |
| --- | --- |
| **Resiko** | **Penyebab** |
| D1001 | Kurangnya sosialisasi mengenai pentingnya  pencegahan terhadap celah keamanan |
| D1002 | Kurangnya pengetahuan dalam mengatasi masalah  keamanan |
| D1003 | Tidak melakukan update tools secara berkala serta  kurangnya identifikasi terhadap tools yang sesuai |
| D1004 | Kurangnya resource atau tenaga ahli |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| D1005 | Kurangnya pengetahuan  masalah keamanan | dan | aware | terhadap |
| D1006 | Tidak adanya filter traffic pada jaringan | | | |
| D1007 | Tidak adanya training atau transfer ilmu kepada staf  atau tenaga kerja | | | |
| D1008 | Kurangnya identifikasi risiko yang mungkin terjadi  serta cara menanggulangi risiko tersebut | | | |
| D2001 | Tidak ada kebijakan yang dibuat untuk permasalahan  keamanan konektivitas | | | |
| D2002 | Adanya otorasi yang dilakukan terhadap *devices* yang  boleh mengakses informasi dan jaringan | | | |
| D2003 | Karena tidak adanya tenaga ahli IT yang ada pada  Dinas Perindustrian dan Tenaga Kerja Kabupaten Trenggalek | | | |
| D2004 | Tidak adanya tenaga IT khusus dalam dinas yang  dapat melakukan proses enkripsi | | | |
| D2005 | Tidak adanya tenaga IT khusus dalam dinas yang  dapat menerapkan protokol keamanan | | | |
| D2006 | Tidak adanya tenaga IT khusus dalam dinas yang  dapat melakukan konfigurasi jaringan | | | |
| D2007 | Belum adanya mekanisme yang terpecaya untuk  mendukung transmisi yang aman | | | |
| D2008 | Belum dilakukannya penetration test untuk peingkatan performa dari aplikasi yang ada pada  organisasi | | | |
| D2009 | Tidak dilakukannya pengujian sistem keamanan  secara berkala | | | |
| D3001 | Tidak adanya standar operasional prosedur terkait  konfigurasi system operasi dengan cara aman | | | |

|  |  |
| --- | --- |
| D3002 | Tidak ada penerapan lockdown untuk perangkat-  perangkat TI |
| D3003 | Tidak ada penerapan enkripsi informasi pada  penyimpanan/storage sesuai dengan klasifikasinya |
| D3004 | Tidak ada kebijakan terkait pengaturan remote  access and control |
| D3005 | Tidak ada kebijakan terkait pengaturan konfigurasi  jaringan secara aman |
| D3006 | Tidak adanya kebijakan terkait pengaturan traffic  filtering pada jaringan di perangkat endpoints |
| D3007 | Tidak ada perllndungan dan penjagaan integritas  system secara keseluruhan |
| D3008 | Tidak ada peninjauan secara menyeluruh terkait  penerapan proteksi secara logical melalui jaringan |
| D3009 | Tidak menerapkan kebijakan atau standar operasional prosedur terkait pembuangan devices yang tidak terpakai lagi dengan cara yang benar dan  aman |
| D4001 | Tidak ada pembatasan hak akses dan kurangnya  penangkal keamanan dalam pembobolan |
| D4002 | Tidak ada batasan peran secara jelas antar satu staff  dengan yang lain |
| D4003 | Kurangnya pembatasan hak akses serta kurangnya  penangkal keamanan dan testing |
| D4004 | Kurangnya pembatasan hak akses serta kurangnya  penangkal keamanan |
| D4005 | Tidak adanya pengelolaan dan pembatasan waktu  session |
| D4006 | Tidak adanya review secara rutin |
| D4007 | Tidak adanya pembatasan hak akses |

|  |  |
| --- | --- |
| D4008 | Kurangnya pengetahuan dalam hal audit informasi  sensitif |
| D5001 | Human error dan kurangnya penangkal keamanan |
| D5002 | Human error dan kurangnya penangkal keamanan |
| D5003 | Human error serta tidak ada identifikasi khusus  seperti bardcode dalam tanda pengenal sehingga mudah di manipulasi |
| D5004 | Kurangnya pantauan keamanan seperti cctv |
| D5005 | Kurangnya pembangunan infrastruktur keamanan  yang lebih kompleks |
| D5006 | Kurangnya pengetahuan, sosialisasi, dan training  dalam hal pencegahan keamanan informasi |
| D6001 | Kurangnya prosedur teknis mengenai pembuangan  form sensitif |
| D6002 | Tidak adanya pengaturan hak akses yang spesifik dan  kurangnya penangkalan keamanan |
| D6003 | Kurangnya infrastruktur keamanan pada inventaris |
| D6004 | Tidak adanya penjagaan dan masih rentannya  infrastruktur keamanan |
| D6005 | Tidak adanya prosedur teknis dan kurangnya  pengetahuan mengenai prosedur penghancuran |
| D7001 | Karena teknologi terus berkembang, penjahat akan  selalu berusaha mencari celah untuk melakukan kejahatan |
| D7002 | Belum adanya penetepan sifat dan karakteristik  insiden yang berpotensial |
| D7003 | Tidak dilakukannya review secara rutin terhadap  event logs |
| D7004 | Tidak adanya prosedur dalam mengumpulkan bukti  security events |

|  |  |
| --- | --- |
| D7005 | Tidak adanya aktivitas incident tickets |

**Tabel 4.6** Penyebab Risiko

# Perumusan Skenario Risiko

Tahapan ini akan diidentifikasi skenario risiko berdasarkan analisa risiko yang dilakukan. Berikut hasil dari skenario risiko :

|  |  |  |  |
| --- | --- | --- | --- |
| **Risiko** | **Skenario** | | |
| **Positif** | | **Negatif** |
|  | Melakukan | sosialisasi | Tidak adanya sosialisasi |
|  | mengena | pentingnya | dan pencerdasan |
|  | prosedur | pencegahan | mengenai pentingnya |
|  | terhadap | keamanan | pencegahan terhadap |
| D1001 | informasi |  | keamanan informasi |
|  |  |  | sehingga kurangnya |
|  |  |  | pengetahuan dan aware |
|  |  |  | terhadap keaamanan |
|  |  |  | sistem itu sendiri |
|  | Melakukan | training | Tidak adanya training |
|  | mengenai | langkah | dan pencerdasan |
|  | mengatasi | masalah | mengenai langkah |
|  | keamanan |  | melakukan mitigasi |
| D1002 |  |  | dalam ancaman |
|  |  |  | keamanan sehingga |
|  |  |  | kurangnya pengetahuan |
|  |  |  | dalam melakukan |
|  |  |  | mitigasi keamanan |

|  |  |  |
| --- | --- | --- |
|  | Melakukan update | Tidak melakukan update |
|  | secara berkala dan | rutin dan tidak |
| D1003 | menggunakan tools yang  sesuai | melakukan identifikasi  tools sehingga tools |
|  |  | masih rentan terhadap |
|  |  | malware |
|  | Melakukan konfigurasi | Konfigurasi tidak |
|  | semua proteksi terhadap | dilakukan secara |
|  | software berbaya secara | terpusat karena |
| D1004 | terpusat | kurangnya tenaga ahli  sehingga ancaman dapat |
|  |  | masuk dari berbagai |
|  |  | celah dan susah untuk |
|  |  | melakukan maintenance |
|  | Melakukan review dan | Tidak adanya aware |
|  | analisis secara teratur | untuk melakukan review |
|  | mengenai risiko yang | dan evaluasi informasi |
| D1005 | mungkin akan terjadi | terhadap potensi |
|  |  | ancaman baru sehingga |
|  |  | dalam menghadapi |
|  |  | ancaman kurang siap |
|  | Menerapkan filter pada | Bebasnya file dan |
|  | traffic pada jaringan dan | informasi yang melintas |
|  | meningkatkan keamanan | karena tidak adanya |
| D1006 | jaringan dengan tools | keamanan dan filter pada |
|  | dan metode metode | jaringan sehingga |
|  | terpercaya | malware dapat dengan |
|  |  | mudah masuk |

|  |  |  |
| --- | --- | --- |
| D1007 | Adanya pelatihan terhadap pencegahan ancaman keamanan | Kurangnya kemauan  untuk melakukan pelatihan untuk menangani ancaman  keamanan |
| D1008 | Dilakukan list dan review terhadap ancaman yang mungkin akan muncul | Tidak adanya mitigasi terhadap ancaman baru karena tidak dilakukan analisa risiko yang  berpotensi |
| D2001 | Menyusun kebijakan agar adanya tindakan yang jelas apabila keamanan  konektivitas terancam | Tidak menyusun  kebijakan sehingga  dibiarkan tidak adanya kebijakan ini |
| D2002 | Adanya jadwal untuk melakukan otorasi  sehingga resource  berfokus pada pengecekkan berkala | Tidak memperhatikan jadwal sehingga resource yang ada tidak dapat memanfaatkan waktu yang ada secara  maksimal |
| D2003 | Melakukan *filtering* pada jaringan untuk menjaga keamanan komputer dari kejahatan malware | Membiarkan jaringan tidak terfilter dan menambah besar kemungkinan perangkat terkena virus atau  malware |
| D2004 | Membuat divisi IT yang bertugas secara khusus untuk melakukan  maintenance | Tidak perlu membuat divisi baru, bisa melakukan hiring tenaga  ahli dari luar namun |

|  |  |  |
| --- | --- | --- |
|  |  | biaya bisa jadi  membengkak |
| D2005 | Membuat divisi IT yang bertugas secara khusus untuk melakukan maintenance | Tidak perlu membuat divisi baru, bisa melakukan hiring tenaga ahli dari luar namun biaya bisa jadi  membengkak |
| D2006 | Membuat divisi IT yang bertugas secara khusus untuk melakukan maintenance | Tidak perlu membuat divisi baru, bisa melakukan hiring tenaga ahli dari luar namun biaya bisa jadi  membengkak |
| D2007 | Membuat mekanisme yang dapat membantu sekaligus medukung  transmisi yang aman | Pembuatan mekanisme tidak perlu dilakukan, dibiarkan saja tanpa  adanya tindakan mitigasi |
| D2008 | Melakukan penetration test untuk menguji kehandalan aplikasi sehingga saat digunakan dapat menunjukkan indikator performa yang  baik | Tidak adanya usaha yang dilakukan untuk peningkatan indikator performa (tidak melakukan penetration test) |
| D2009 | Adanya jadwal berkala dimana sistem akan dilakukan pengujian  untuk menentukan | Jadwal tidak dibuat secara berkala, ada, namun tidak terjadwal. |

|  |  |  |
| --- | --- | --- |
|  | kecukupan sistem  perlindungan. |  |
| D3001 | Menyusun standar  operasioal prosedur terkait konfigurasi sistem operasi drngan cara aman dan  menerapkannya | Tidak menyusun dan tidak menerapkan  standar operasional  prosedur terkait  konfigurasi sistem operasi dengan cara  aman |
| D3002 | Menerapkan lockdown untuk perangkat-  perangkat TI | Tidak menerapkan lockdown untuk  perangkat-perangkat TI |
| D3003 | Menerapkan enkripsi informasi pada penyimpanan/storage sesuai dengan  klasifikasinya | Tidak menerapkan enkripsi informasi pada penyimpanan/storage sesuai dengan  klasifikasinya |
| D3004 | Menyusun dan menerapkan kebijakan terkait pengaturan remote access and  control | Tidak menyusun dan menerapkan kebijakan terkait pengaturan remote access and  control |
| D3005 | Menyusun dan menerapkan kebijakan terkait pengaturan konfigurasi jaringan  secara aman | Tidak menyusun dan menerapkan kebijakan terkait pengaturan konfigurasi jaringan  secara aman |
| D3006 | Menyusun dan menerapkan kebijakan  terkait pengaturan traffic | Tidak menyusun dan menerapkan kebijakan  terkait pengaturan traffic |

|  |  |  |
| --- | --- | --- |
|  | filtering pada jaringan di  perangkat endpoints | filtering pada jaringan di  perangkat endpoints |
| D3007 | Melakukan perlindungan dan penjagaan integritas system secara keseluruhan | Tidak melakukan perlindungan dan penjagaan integritas system secara  keseluruhan |
| D3008 | Melakukan peninjauan secara menyeluruh  terkait penerapan proteksi secara logical melalui jaringan | Tidak melakukan peninjauan secara  menyeluruh terkait  penerapan proteksi secara logical melalui  jaringan |
| D3009 | Menyusun dan menerapkan kebijakan atau standar operasional prosedur terkait pembuangan devices yang tidak terpakai lagi dengan cara yang benar  dan aman | Tidak menyusun dan menerapkan kebijakan atau standar operasional prosedur terkait pembuangan devices yang tidak terpakai lagi dengan cara yang benar  dan aman |
| D4001 | Memiliki pembatasan hak akses sesuai dengan proses bisnis yang dilakukan serta memperketat keamanan  dalam autorisasi | Tidak memiliki keamanan yang kuat dalam hal autorisasi sehingga masih mudah dilakukan keancaman |
| D4002 | Pembagian peran dan fungsi diidentifikasi  secara jelas | Peran dan fungsi tidak terdefinisi secara jelas |

|  |  |  |
| --- | --- | --- |
|  |  | sehingga hak akses masih  tidak spesifik |
| D4003 | Adanya autentikasi yang kuat dalam hak akses sehingga data tidak dapat termodifikasi dan  dihapus | Sistem akan secara mudah di rusak oleh pihak yang tidak memiliki hak akses |
| D4004 | Melakukan pembatasan hak akses terhadap siapa saja yang berhak melakukan perubahan | Tidak adanya hak akses yang membatasi penggunaan aplikasi sehingga dengan mudah dimodifikasi oleh pihak luar yang tidak memiliki  akses |
| D4005 | Melakukan pemisahan terhadap hak akses, melakukan pengaturan pembatasan waktu  session | Session tidak terdapat pembatasan durasi dan tidak ada *privileged user account* |
| D4006 | Melakukan review secara rutin terhadap aktivitas akun untuk menghindari aktivitas yang mencurigakan | Tidak adanya review karena terbatasanya  resource sehingga tampak kurang aware mengenai aktivitas- aktivitas yang dilakukan  oleh akun |
| D4007 | Mengidentifikasi user  dan aktivitasnya secara jelas | User tidak teridentifikasi  secara jelas sehingga tidak ada batasan oleh |

|  |  |  |
| --- | --- | --- |
|  |  | user untuk melakukan  hak akses |
| D4008 | Melakukan audit informasi yang bersifat sensitif | Kurangnya kepemahaman dan pengetahuan mengenai  audit informasi |
| D5001 | Menjaga kerahasiaan hak akses sebaik mungkin dan tidak mudah terpengaruhi | Adanya human error serta kerentanan terhadap sumber daya manusia sehingga dapat mudah terjebak dalam  teknik *social engineering* |
| D5002 | Memastikan hanya  pihak-pihak tertentu yang memiliki hak akses | Tidak adanya  keterbatasan hak akses sehingga siapapun dapat mengakses dan tingkat risiko pembobolan  semakin tinggi |
| D5003 | Menggunakan tanda pengenal yang terlihat dan terintegrasi oleh suatu sistem keamanan sehingga tidak mudah  untuk dimanipulasi | Tanda pengenal masih sangat minim dan tidak ada proteksi keamanan sehingga dengan mudah dimanipulasi tanpa  adanya verifikasi |
| D5004 | Menemani pengunjung yang ingin berkunjung ke lingkungan IT, memasang CCTV | Pengunjung dibiarkan masuk sehingga celah ancaman keamanan dapat terbuka lebar  dengan mudahnya |

|  |  |  |
| --- | --- | --- |
| D5005 | Membangun infrastruktur keamanan yang kuat dan kebal akan ancaman seperti pagar dengan password, sidik  jari, retina, dll | Infrastruktur keamanan masih sangat sederhana dan sangat mudah untuk dibobol karena tidak adanya proteksi yang  kuat |
| D5006 | Mengadakan pelatihan pencegahan ancaman keamanan dan cara  menanggulanginya | Tidak adanya pelatihan sehingga tingkat aware masih sangat minim |
| D6001 | Adanya prosedur pengaturan pembuangan form sensitive agar tidak terbuang secara sembarangan sehingga tidak adanya  pemungutan dari pihak luar yang tidak  bertanggung jawab | Pembuangan form sensitive dilakukan secara bebas tanpa adanya prosedur dan aturan untuk mencegah terambilnya informasi dari pihak yang tidak bertanggung jawab. |
| D6002 | Pembatasan hak akses pada informasi sensitif agar tidak semua orang dapat mengakses dan celah ancaman keamanan berkurang | Informasi sensitive dapat diakses oleh siapapun sehingga semakin lebarnya pintu celah pembobolan dari pihak luar yang tidak  bertanggung jawab |
| D6003 | Melakukan proteksi  terhadap inventaris dokumen atau informasi sensitif | Tidak adanya proteksi yang kuat pada inventaris sehingga dapat terbobol  dengan mudah |

|  |  |  |
| --- | --- | --- |
| D6004 | Pembangunan infrastruktur keamanan yang kuat dan tidak  hanya satu | Lemahnya infrastruktur keamanan sehingga masih mudah dirusak dan  dicuri |
| D6005 | Membuat prosedur penghancuran informasi sensitive yang tepat sehingga tidak adanya informasi yang terbuang secara bebas dan dapat ditemukan oleh pihak yang tidak bertanggung  jawab | Tidak adanya prosedur penghancuran informasi sensitive sehingga  informasi dapat  dihancurkan secara bebas dan ditemukan oleh pihak yang tidak betanggung jawab. |
| D7001 | Aktivitas yang terjadi dicatat untuk memastikan tidak adanya celah keamanan sehingga tidak terjadi  kecolongan | Tidak melakukan pencatatan terhadap aktivitas yang berkaitan dengan keamanan |
| D7002 | Melakukan penetapan sifat dan karakteristik insiden yang  berhubungan dengan  keamanan | Tidak dilakukannya penetapan sifat dan karakteristik sehingga kemungkinan terjadinya  insiden adalah mungkin |
| D7003 | Melakukan review secara rutin agar insiden-insiden dapat diminimalisasi | Tidak dilakukannya review rutin terhadap event logs sehingga kemungkinan insiden  adalah ada |

|  |  |  |
| --- | --- | --- |
| D7004 | Prosedur ditetapkan untuk mengumpulkan bukti-bukti security  events | Tidak dilakukan pengumpulan prosedur sehingga bukti-bukti  security events tidak ada |
| D7005 | Proses eskalasi dilakukan dengan memastikan incident tickets dibuat dengan tepat waktu | Tidak dilakukan proses eskalasi untuk memastikan incident tickets agar dibuat tepat  waktu |

**Tabel 4.7** Skenaro Risiko

# BAB 5 PENUTUP

# Kesimpulan

Kesimpulan yang dapat diambil berdasarkan rumusan masalah yang telah kami jabarkan pada bab sebelumnya dari hasil penelitian yang telah dilakukan adalah :

1. Bagaimana proses bisnis dari Dinas Perindustrian dan Tenaga Kerja Kabupaten Trenggalek?

Dinas Perindustrian dan Tenaga Kerja Kabupaten Trenggalek bergerak di bidang ketenaga kerjaan. Mengelola sumber daya manusia dengan cara menyalurkan antara pencari kerja dan perusahaan/organisasi/pabrik yang membutuhkan pekerjaan. Dinas Perindustrian dan Tenaga Kerja Kabupaten Trenggalek juga mengurusi Tenaga Keja Indonesia (TKI) dimana sebelum keberangkatan para TKI akan tinggal di asrama dan mendapatkan beberapa pelatihan. Dari penjabaran proses bisnis yang telah kami lakukan seperti pelatihan dan produktivitas tenaga kerja, kemudian layanan publik SISKOTKLN dengan aplikasi siskotkln dan transmigrasi yang dipetakan ke dalam COBIT 5 dengan domain DSS05 *Manage Security*.

1. Bagaimanakah proses manajemen risiko IT pada Dinas Perindustrian dan Tenaga Kerja Kabupaten Trenggalek saat ini? Kami mendapat setidaknya 50 risiko yang telah kami identifikasi yang bisa mempengaruhi proses bisnis dari Dinas Perindusrian dan Tenaga Kerja. Risiko tersebut lebih terfokus pada risiko-risiko yang muncul akibat kelemahan keamanan.
2. Bagaimanakah membuat rancangan manajemen risiko IT pada Dinas Perindustrian dan Tenaga Kerja Kabupaten Trenggalek dengan menggunakan *framework* COBIT 5? Yang kami lakukan untuk membuat rancangan manajemen risiko adalah dengan menggolongkan risiko kedalam domain DSS05 dan dibagi kedalam sub domain untuk kemudian di identifikasi

berdasarkan penyebab, tipe risiko maupun kategori risiko yang nantinya akan mengerucut ke skenario risiko.

# Saran

Saran yang dapat kami tawarkan terkait dengan pengerjaan tugas final project ini adalah saran kepada Dinas Perindustrian dan Tenaga Kerja Kabupaten Trenggalek, adalah sebagai berikut :

1. Risiko tidak hanya dapat mempengaruhi dari segi proses bisnis perusahaan, akan tetapi juga bisa mempengaruhi dari segi lain seperti Aset Teknologi Informasi, sehingga dapat dilakukan identifikasi kembali untuk risiko yang berdampak kepada aset TI yang dimiliki oleh perusahaan.
2. Peneliti atau pengembang selanjutnya dapat membuat Dokumen Tata Kelola TI berkaitan dengan pengelolaan risiko untuk Dinas Perindustrian dan Tenaga Kerja Kabupaten Trenggaleh. Sehingga kebijakan dan prosedur dalam menanggapi risiko bisa sesuai dengan best practice yang ada.
3. Peneliti menyarankan untuk memperkuat kebijakan dalam hak akses data dan informasi sensitive sehingga informasi tetap dapat terjaga dengan baik.
4. Perlu adanya tenaga kerja khusus yang menangani dalam bidang IT untuk melakukan maintenance rutin dan sebagai pencegahan celah keamanan data dan informasi sensitive.
5. Perlu adanya analisis dan review rutin untuk mengidentifikasi terjadinya risiko dan ancaman yang kemungkinan akan terjadi. Serta mengidentifikasi mitigasi dari risiko dan ancaman tersebut.
6. Tenaga kerja perlu mendapatkan pemahaman lebih lanjut seperti sosialisasi, pelatihan, dan pencerdasan mengenai pentingnya akan pencegahan terhadap celah keamanan IT serta bagaimana cara menanggulanginya.

# Referensi:

[1] “No Title,” no. Cobit 5, pp. 5–18, 2012.

1. S. Babb, E. Anton, and J. Bleicher, “COBIT 5 for Risk,” *Isaca*, vol. 4, pp. 9–18, 2013.
2. H. S. A. Ahmed, “COBIT 5 for Risk — A Powerful Tool for Risk Management,” pp. 1–5, 2017.
3. “COBIT 5 for Risk – An overview.”
4. L. Belakang, “Bab 1. PENDAHULUAN,” no. Cc, pp. 1–11, 2007.
5. N. Z. Firdaus, “Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan COBIT 5 IT Risk ( Studi Kasus : PT . Petrokimia Gresik ),” vol. 2, no. 1, pp. 91–100, 2018.