

## **Tugas Tata Kelola - Narasi Wawancara Design Factor**

### **Anggota kelompok:**

**Iqbal Firmansyah (2111521014)**

**Nurul Insan (2111522013)**

**Putra Ilham (2111522018)**

**Najla Humaira Desni (2211521002)**

**Rizka Kurnia Illahi (2211521012)**

## **OBJEK: SUBDIT KEAMANAN DAN PUSAT DATA LPTIK UNIVERSITAS ANDALAS**

### **Design Factor 1 : Enterprise Strategy**

#### *Value 1: Growth/Acquisition*

##### **Narasi Pertanyaan Value 1:**

- Bagaimana strategi pertumbuhan dan pengembangan layanan keamanan data serta pengelolaan pusat data yang diterapkan oleh Subdit Keamanan dan Pusat Data di LPTIK Unand saat ini?
- Apakah Subdit Keamanan dan Pusat Data memiliki rencana untuk mengadopsi atau mengakuisisi teknologi keamanan atau sistem baru dalam waktu dekat?

#### *Value 2: Innovation/Differentiation*

##### **Narasi Pertanyaan Value 2:**

- Apa inovasi yang sudah dilakukan atau saat ini sedang dilakukan oleh Subdit Keamanan dan Pusat Data untuk membedakan layanan keamanan datanya dari universitas lain?
- Apa saja tantangan yang dihadapi dalam menerapkan inovasi keamanan baru, dan bagaimana cara Subdit Keamanan dan Pusat Data mengatasinya?

#### *Value 3: Cost Leadership*

##### **Narasi Pertanyaan Value 3:**

- Bagaimana Subdit Keamanan dan Pusat Data mengoptimalkan biaya operasional terkait keamanan data tanpa mengorbankan kualitas perlindungan yang diberikan?

Value 4: *Client Service/Stability*

Narasi Pertanyaan Value 4:

- Bagaimana Subdit Keamanan dan Pusat Data menangani keluhan atau masukan dari pengguna terkait masalah keamanan informasi atau gangguan yang mempengaruhi pusat data?

## **Design Factor 2 : Enterprise Goals**

Value 1: *Portfolio of competitive products and services*

Narasi Pertanyaan Value 1:

- Apa saja layanan keamanan data dan pengelolaan pusat data yang menjadi unggulan di LPTIK?
- Bagaimana layanan tersebut berkontribusi terhadap perlindungan dan keamanan data universitas?

Value 2: *Managed business risk*

Narasi Pertanyaan Value 2:

- Bagaimana Subdit Keamanan dan Pusat Data mengidentifikasi dan mengelola risiko keamanan informasi di universitas?
- Apa langkah-langkah utama yang diambil untuk mengurangi risiko terkait keamanan data?

Value 3: *Compliance with external laws and regulations*

Narasi Pertanyaan Value 3:

- Bagaimana memastikan bahwa pengelolaan data dan keamanan informasi mematuhi peraturan dan undang-undang eksternal yang berlaku?
- Apa tantangan utama dalam menjaga kepatuhan terhadap standar keamanan data eksternal?

Value 4: *Quality of financial information*

Narasi Pertanyaan Value 4:

- Bagaimana sistem keamanan informasi mendukung penyediaan data keuangan yang aman dan terlindungi?
- Bagaimana memastikan data keuangan tetap aman dari ancaman keamanan?

Value 5: *Customer-oriented service culture*

Narasi Pertanyaan Value 5:

- Bagaimana Subdit Keamanan dan Pusat Data memastikan bahwa layanan keamanan informasi sesuai dengan kebutuhan pengguna?
- Bagaimana mengukur kepuasan pengguna terhadap keamanan dan keandalan data?

Value 6: *Business-service continuity and availability*

Narasi Pertanyaan Value 6:

- Apa strategi untuk memastikan kontinuitas dan ketersediaan layanan pusat data di universitas?
- Bagaimana Subdit Keamanan dan Pusat Data menangani gangguan layanan yang mempengaruhi keamanan dan aksesibilitas data?

Value 7: *Quality of management information*

Narasi Pertanyaan Value 7:

- Bagaimana memastikan bahwa informasi manajemen terkait keamanan data akurat dan dapat diandalkan?
- Apa indikator kualitas informasi manajemen keamanan yang diutamakan?

Value 8: *Optimization of internal business process functionality*

Narasi Pertanyaan Value 8:

- Apa inisiatif yang dilakukan untuk mengoptimalkan proses bisnis internal terkait keamanan data dan pengelolaan pusat data?
- Bagaimana inisiatif tersebut meningkatkan efisiensi dan keamanan?

Value 9: *Optimization of business process costs*

Narasi Pertanyaan Value 9:

- Bagaimana mengelola dan mengoptimalkan biaya yang terkait dengan keamanan informasi dan pengelolaan pusat data?
- Apa langkah yang diambil untuk mengurangi biaya tanpa mengorbankan kualitas keamanan?

Value 10: *Staff skills, motivation and productivity*

Narasi Pertanyaan Value 10:

- Bagaimana memastikan bahwa staf yang menangani keamanan data dan pusat data memiliki keterampilan yang sesuai?
- Apa indikator keberhasilan dalam menilai motivasi dan produktivitas staf yang terkait dengan keamanan data?

Value 11: *Compliance with internal policies*

Narasi Pertanyaan Value 11:

- Bagaimana memastikan bahwa proses keamanan informasi sesuai dengan kebijakan internal universitas?
- Bagaimana proses monitoring dilakukan untuk memastikan bahwa kebijakan keamanan data diikuti dengan benar?

Value 12: *Managed digital transformation programs*

Narasi Pertanyaan Value 12:

- Apa saja program transformasi digital yang berfokus pada peningkatan keamanan informasi dan pengelolaan pusat data?
- Apa tantangan utama dalam mengelola program transformasi digital yang berkaitan dengan keamanan?

Value 13: *Product and business innovation*

Narasi Pertanyaan Value 13:

- Bagaimana Subdit Keamanan dan Pusat Data mendorong inovasi dalam teknologi keamanan informasi di universitas?
- Apa tantangan terbesar dalam mengembangkan inovasi yang berfokus pada keamanan data?

### **Design Factor 3 : Risk Profile**

Value 1: IT investment decision making, portfolio definition & maintenance

Narasi Pertanyaan Value 1:

- Bagaimana proses pengambilan keputusan untuk investasi TI dilakukan di organisasi saat ini?
- Seberapa sering portofolio IT dievaluasi ulang untuk menyesuaikan prioritas strategis?
- Apakah ada kendala yang signifikan dalam pengelolaan portofolio IT?

Value 2 : Program & projects life cycle management

Narasi Pertanyaan Value 2:

- Apakah organisasi memiliki kerangka kerja yang pasti untuk IT projects life cycle? Jika ada, bagaimana dampaknya?
- Apakah proyek organisasi sering mengalami keterlambatan atau kegagalan?

Value 3 : IT cost & oversight

Narasi Pertanyaan Value 3:

- Apakah anggaran dalam organisasi IT dipantau secara teratur untuk memastikan kesesuaian biaya dan manfaat?
- Apakah pernah terjadi penyimpangan anggaran dalam proyek IT? jika pernah, seberapa sering?
- Apakah ada mekanisme pengendalian biaya yang efektif?

Value 4 : IT expertise, skills & behavior

Narasi Pertanyaan Value 4:

- Bagaimana tingkat keahlian staf IT dalam mendukung kebutuhan operasional?

- Apakah organisasi memiliki program pelatihan yang memadai untuk meningkatkan keterampilan staf IT?
- Seberapa sering ada pergantian staf IT?

#### Value 5 : Enterprise/IT architecture

##### Narasi Pertanyaan Value 5:

- Apakah organisasi memiliki arsitektur IT yang terdokumentasi dengan baik?
- Seberapa sering arsitektur IT ditinjau dan diperbarui?
- Apakah ada masalah dalam integrasi sistem yang mempengaruhi operasional?

#### Value 6 : IT operational infrastructure incidents

##### Narasi Pertanyaan Value 6:

- Apakah sering terjadi insiden infrastruktur IT terjadi dalam organisasi? Jika iya, apakah ada mekanisme respons yang memadai untuk menangani insiden tersebut?
- Apa dampak insiden terhadap operasi harian?

#### Value 7 : Unauthorized Actions

##### Narasi Pertanyaan Value 7:

- Seberapa sering terjadi tindakan yang tidak sah pada sistem IT organisasi?
- Apakah kontrol akses yang ada cukup untuk mencegah akses yang tidak sah?
- Bagaimana dampak dari tindakan tersebut terhadap operasi?

#### Value 8 : Software Adoption/Usage Problems

##### Narasi Pertanyaan Value 8:

- Apakah sering terjadi kendala dalam mengadopsi atau menggunakan software baru?
- Apakah pengguna akhir memiliki pelatihan yang memadai untuk memahami dan menggunakan software?
- Bagaimana dampak dari ketidaksesuaian software terhadap produktivitas?

#### Value 9 : Hardware Incidents

##### Narasi Pertanyaan Value 9:

- Apakah sering terjadi kegagalan hardware dalam organisasi?
- Apakah ada prosedur pemeliharaan hardware yang memadai?

- Seberapa besar dampak kegagalan hardware terhadap layanan?

#### Value 10 : Software Failures

##### Narasi Pertanyaan Value 10:

- Seberapa sering software mengalami kegagalan dalam organisasi?
- Apakah ada standar proses pengujian dan pemeliharaan untuk software yang organisasi?
- Bagaimana dampak kegagalan software terhadap proses bisnis organisasi?

#### Value 11 : Logical Attacks (Hacking, Malware, etc.)

##### Narasi Pertanyaan Value 11:

- Seberapa sering organisasi menjadi target serangan siber?
- Apakah ada tindakan keamanan siber yang memadai untuk mencegah serangan seperti hacking dan malware?
- Bagaimana dampak serangan siber terhadap data atau sistem organisasi?

#### Value 12 : Third-Party/Supplier Incidents

##### Narasi Pertanyaan Value 12:

- Seberapa besar ketergantungan organisasi pada pihak ketiga atau pemasok?
- Apakah ada perjanjian SLA (Service Level Agreement) yang jelas dengan pihak ketiga?
- Seberapa sering terjadi kegagalan atau insiden terkait pihak ketiga?

#### Value 13 : Noncompliance

##### Narasi Pertanyaan Value 13:

- Apakah organisasi rutin mengevaluasi kepatuhan terhadap regulasi atau kebijakan yang berlaku?
- Apakah ada audit reguler untuk memastikan kepatuhan?
- Apa konsekuensi dari ketidakpatuhan terhadap aturan atau kebijakan?

#### Value 14 : Geopolitical Issues

##### Narasi Pertanyaan Value 14:

- Apakah operasi organisasi terpengaruh oleh ketidakstabilan politik di wilayah tertentu?
- Apakah ada mitigasi risiko untuk isu geopolitik seperti sanksi atau konflik internasional?
- Seberapa besar dampaknya terhadap rantai pasok atau operasi?

#### Value 15 : Industrial Action

##### Narasi Pertanyaan Value 15:

- Apakah organisasi pernah terdampak aksi industri seperti pemogokan?
- Apakah ada strategi untuk mengatasi dampak aksi industri pada operasional?
- Bagaimana dampak dari aksi tersebut terhadap kinerja organisasi?

#### Value 16 : Acts of Nature

##### Narasi Pertanyaan Value 16:

- Seberapa sering lokasi organisasi terpengaruh oleh bencana alam seperti banjir, gempa bumi, atau badai?
- Apakah ada rencana pemulihan bencana yang memadai?
- Bagaimana dampak bencana alam terhadap infrastruktur atau layanan?

#### Value 17 : Technology-Based Innovation

##### Narasi Pertanyaan Value 17:

- Apakah organisasi secara aktif mengeksplorasi dan mengadopsi teknologi inovatif?
- Apakah ada risiko yang teridentifikasi terkait dengan penerapan teknologi baru?
- Bagaimana pengaruh inovasi teknologi terhadap model bisnis organisasi?

#### Value 18 : Environmental

##### Narasi Pertanyaan Value 18:

- Apakah organisasi memiliki kebijakan yang mendukung keberlanjutan lingkungan?
- Apakah ada risiko terkait dengan dampak lingkungan dari operasi organisasi?
- Bagaimana dampak pelanggaran lingkungan terhadap reputasi atau operasional?

#### Value 19 : Data & Information Management

##### Narasi Pertanyaan Value 19:



- Apakah organisasi memiliki kebijakan yang memadai untuk pengelolaan data?
- Apakah sering terjadi insiden seperti kehilangan atau pelanggaran data?
- Bagaimana dampak insiden data terhadap operasional dan kepercayaan pelanggan?

#### **Design Factor 4 : importance of each generic IT**

Value 1: Frustration between different IT entities across the organization because of a perception of low contribution to business value

Narasi Pertanyaan Value 1:

- Apakah Anda pernah merasa frustrasi karena kontribusi TI di organisasi ini dirasa kurang mendukung pencapaian nilai bisnis? Jika iya, apa penyebab utamanya?

Value 2: Frustration between business departments (i.e., the IT customer) and the IT department because of failed initiatives or a perception of low contribution to business value

Narasi Pertanyaan Value 2:

- Bagaimana Anda menilai kontribusi TI terhadap inisiatif-inisiatif bisnis? Apakah ada kasus di mana inisiatif tersebut gagal atau kontribusi TI dirasa kurang maksimal?

Value 3: Significant IT-related incidents, such as data loss, security breaches, project failure and application errors, linked to IT

Narasi Pertanyaan Value 3:

- Pernahkah terjadi insiden besar seperti kehilangan data, pelanggaran keamanan, atau kegagalan proyek yang berdampak signifikan? Jika iya, bagaimana insiden tersebut ditangani?

Value 4: Service delivery problems by the IT outsourcer(s)

Narasi Pertanyaan Value 4:

- Apakah ada masalah yang signifikan dengan layanan yang diberikan oleh penyedia TI eksternal? Jika iya, bagaimana dampaknya terhadap operasi organisasi?

Value 5: Failures to meet IT-related regulatory or contractual requirements

Narasi Pertanyaan Value 5:

- Apakah ada kasus di mana departemen TI gagal memenuhi persyaratan regulasi atau kontrak? Apa yang menjadi tantangan utama untuk mematuhi persyaratan tersebut?

Value 6: Regular audit findings or other assessment reports about poor IT performance or reported IT quality or service problems

Narasi Pertanyaan Value 6:

- Apakah hasil audit atau laporan penilaian lainnya pernah menunjukkan masalah kinerja TI atau kualitas layanan? Bagaimana hal tersebut direspon?

Value 7: Substantial hidden and rogue IT spending, that is, IT spending by user departments outside the control of the normal IT investment decision mechanisms and approved budgets

Narasi Pertanyaan Value 7:

- Apakah ada indikasi pengeluaran TI yang dilakukan oleh departemen bisnis tanpa melalui mekanisme pengambilan keputusan TI yang normal? Bagaimana ini memengaruhi anggaran TI?

Value 8: Duplications or overlaps between various initiatives, or other forms of wasted resources

Narasi Pertanyaan Value 8:

- Apakah organisasi pernah mengalami duplikasi inisiatif TI atau pemborosan sumber daya? Bagaimana hal tersebut diidentifikasi dan diatasi?

Value 9: Insufficient IT resources, staff with inadequate skills or staff burnout/dissatisfaction

Narasi Pertanyaan Value 9:

- Apakah organisasi pernah menghadapi kekurangan staf TI yang kompeten atau masalah kepuasan kerja di kalangan staf TI? Bagaimana dampaknya pada operasional TI?

Value 10: IT-enabled changes or projects frequently failing to meet business needs and delivered late or over budget

Narasi Pertanyaan Value 10:

- Seberapa sering proyek atau perubahan yang didukung TI gagal memenuhi kebutuhan bisnis, terlambat, atau melebihi anggaran? Apa penyebab utamanya?

Value 11: Reluctance by board members, executives or senior management to engage with IT, or a lack of committed business sponsorship for IT

Narasi Pertanyaan Value 11:

- Seberapa besar keterlibatan anggota dewan, eksekutif, atau manajemen senior dalam inisiatif TI? Apakah pernah ada kendala karena kurangnya dukungan atau komitmen?

Value 12: Complex IT operating model and/or unclear decision mechanisms for IT-related decisions

Narasi Pertanyaan Value 12:

- Apakah mekanisme pengambilan keputusan terkait TI di organisasi ini sudah jelas? Jika tidak, bagaimana kompleksitas ini memengaruhi efisiensi operasional TI?

Value 13: Excessively high cost of IT

Narasi Pertanyaan Value 13:

- Bagaimana Anda menilai biaya TI di organisasi ini? Apakah biaya tersebut dianggap terlalu tinggi dibandingkan dengan manfaat yang diperoleh?

Value 14: Obstructed or failed implementation of new initiatives or innovations caused by the current IT architecture and systems

Narasi Pertanyaan Value 14:

- Apakah arsitektur atau sistem TI saat ini pernah menjadi penghalang dalam implementasi inisiatif atau inovasi baru? Bagaimana Anda menyelesaikan masalah tersebut?

Value 15: Gap between business and technical knowledge, which leads to business users and information and/or technology specialists speaking different languages

Narasi Pertanyaan Value 15:

- Apakah Anda melihat adanya kesenjangan komunikasi antara pengguna bisnis dan spesialis teknologi? Bagaimana hal ini memengaruhi kolaborasi dalam proyek TI?

Value 16: Regular issues with data quality and integration of data across various sources

Narasi Pertanyaan Value 16:

- Seberapa sering organisasi mengalami masalah dengan kualitas data atau integrasi data dari berbagai sumber? Bagaimana Anda menangani tantangan ini?

Value 17: High level of end-user computing, creating (among other problems) a lack of oversight and quality control over the applications that are being developed and put in operation

Narasi Pertanyaan Value 17:

- Apakah programmer atau setingkat High level of end-user computing sering mengembangkan aplikasi mereka sendiri tanpa pengawasan departemen TI? Bagaimana hal ini memengaruhi kualitas dan kontrol sistem?

Value 18: Business departments implementing their own information solutions with little or no involvement of the enterprise IT department (related to end-user computing, which often stems from dissatisfaction with IT solutions and services)

Narasi Pertanyaan Value 18:

- Apakah ada kasus di mana departemen bisnis mengembangkan solusi informasi mereka sendiri tanpa melibatkan TI? Apa dampaknya terhadap keselarasan sistem organisasi?

Value 19: Ignorance of and/or noncompliance with privacy regulations

Narasi Pertanyaan Value 19:

- Seberapa baik organisasi mematuhi regulasi terkait privasi data? Apakah ada kasus ketidaktahuan atau ketidakpatuhan yang pernah terjadi?

Value 20: Inability to exploit new technologies or innovate using I&T

Narasi Pertanyaan Value 20:

- Bagaimana kemampuan organisasi dalam mengadopsi teknologi baru atau berinovasi menggunakan TI? Apakah ada kendala tertentu yang menghambat proses ini?

### **Design Factor 5 : Thread Landscape**

Value 1: *High*

Narasi Pertanyaan Value 1:

- Apa ancaman keamanan siber paling serius yang dihadapi oleh Subdit Keamanan dan Pusat Data saat ini?

- Langkah-langkah apa saja yang diambil oleh Subdit Keamanan dan Pusat Data untuk memitigasi risiko atau ancaman yang dapat mengganggu operasional keamanan dan stabilitas data?

Value 2: *Normal*

Narasi Pertanyaan Value 2:

- Seberapa sering Subdit Keamanan dan Pusat Data melakukan evaluasi terhadap sistem keamanannya untuk memastikan perlindungan yang memadai?
- Bagaimana proses pembaruan atau peningkatan sistem keamanan yang dilakukan secara rutin?

### **Design Factor 6 : Compliance Requirements**

Value 1: *High*

- Bagaimana SUBDIT Keamanan dan Pusat Data memastikan kepatuhan terhadap regulasi perlindungan data yang bersifat kritis?
- Apa protokol khusus yang diterapkan untuk menangani data-data sensitif mahasiswa dan pegawai?

Value 2: *Normal*

- Bagaimana prosedur operasional standar dalam pengelolaan backup data di LPTIK UNAND?
- Bagaimana mekanisme pemantauan dan pelaporan insiden keamanan yang diterapkan sehari-hari?

Value 3: *Low*

- Apa pertimbangan utama dalam menentukan bahwa suatu kebijakan atau sistem tertentu memiliki prioritas rendah dalam penerapan di LPTIK?
- Apakah ada dokumentasi untuk prosedur-prosedur yang jarang digunakan namun tetap perlu dijaga?

## **Design Factor 7 : Role IT**

### *Value 1: Support*

- Bagaimana Subdit Keamanan dan Pusat Data mendukung aktivitas operasional harian di LPTIK, seperti pengelolaan server, jaringan, atau sistem akademik? Apakah ada standar keamanan tertentu yang diimplementasikan untuk menjaga kelancaran operasional tersebut?
- Apa langkah-langkah yang dilakukan Subdit Keamanan untuk memastikan layanan sistem informasi tetap dapat diakses dengan cepat, aman oleh mahasiswa, dosen, dan tenaga kependidikan tanpa gangguan teknis yang berarti?

### *Value 2: Factory*

- Bagaimana Subdit Keamanan menangani risiko downtime yang dapat memengaruhi kegiatan akademik seperti registrasi mahasiswa atau pengambilan KRS?

### *Value 3: Turnaround*

- Dalam konteks transformasi digital, apa langkah-langkah yang telah dilakukan Subdit Keamanan dan Pusat Data untuk meningkatkan sistem keamanan data atau memperbarui teknologi yang digunakan? Apakah ada tantangan signifikan selama proses transformasi ini?

### *Value 4: Strategic*

- Bagaimana Subdit Keamanan dan Pusat Data mendukung strategi Universitas Andalas dalam meningkatkan reputasi institusi melalui layanan digital yang aman dan andal? Apakah ada inovasi keamanan atau pengelolaan data yang telah diimplementasikan untuk mencapai tujuan tersebut?

## **Design Factor 8 : Sourcing Model for IT**

### *Value 1: Outsourcing*

#### Narasi Pertanyaan Value 1:

- Apakah ada layanan atau proyek keamanan data yang saat ini dialihdayakan (outsourced) ke pihak ketiga oleh Subdit Keamanan dan Pusat Data? Jika iya, mengapa layanan tersebut dipilih untuk di-outsourcing-kan?

- Bagaimana proses pemilihan vendor atau mitra outsourcing yang dilakukan Subdit Keamanan dan Pusat Data, terutama terkait kriteria keamanan yang harus dipenuhi?
- Apa kendala utama yang dihadapi dalam pengelolaan layanan keamanan data yang di-outsourcing-kan, dan bagaimana Subdit Keamanan dan Pusat Data mengatasinya?
- Bagaimana Subdit Keamanan dan Pusat Data mengawasi dan mengevaluasi kinerja mitra outsourcing untuk memastikan standar keamanan terpenuhi?

#### Value 2: *Cloud*

##### Narasi Pertanyaan Value 2:

- Apakah Subdit Keamanan dan Pusat Data sudah memanfaatkan teknologi cloud dalam mendukung keamanan data di lingkungan universitas? Jika iya, data atau aplikasi apa yang di-hosting di cloud?
- Apakah ada rencana untuk memperluas penggunaan cloud sebagai bagian dari strategi keamanan data di masa depan?

#### Value 3: *Inourced*

##### Narasi Pertanyaan Value 3:

- Apa saja layanan keamanan data yang dikelola sepenuhnya oleh Subdit Keamanan dan Pusat Data secara internal?
- Tantangan apa yang dihadapi dalam pengelolaan layanan keamanan data secara internal, terutama dalam hal SDM dan teknologi?
- Bagaimana strategi Subdit Keamanan dan Pusat Data dalam mengembangkan keterampilan atau kemampuan tim internal untuk mengelola keamanan data secara lebih efektif?

### **Design Factor 9 : IT Implementation Methods**

#### Value 1: *Agile*

##### Narasi Pertanyaan Value 1:

- Apakah Subdit Keamanan dan Pusat Data menerapkan metode Agile dalam proyek peningkatan keamanan informasi? Jika iya, bagaimana metode ini diadaptasi untuk memenuhi kebutuhan keamanan di lingkungan universitas?

- Apa tantangan terbesar yang dihadapi dalam implementasi Agile di Subdit Keamanan dan Pusat Data, terutama dalam hal koordinasi dengan berbagai departemen di universitas?

Value 2: *DevOps*

Narasi Pertanyaan Value 2:

- Apakah Subdit Keamanan dan Pusat Data menggunakan pendekatan DevOps dalam pengelolaan siklus hidup perangkat lunak keamanan dan sistem keamanan lainnya di universitas?
- Apa tantangan utama dalam mengadopsi pendekatan DevOps, terutama dalam konteks keamanan dan kebijakan yang berlaku di universitas?

Value 3: *Traditional*

Narasi Pertanyaan Value 3:

- Apakah Subdit Keamanan dan Pusat Data masih menggunakan metode tradisional (waterfall) dalam beberapa proyek keamanan informasi, dan jika iya, pada jenis proyek atau layanan keamanan apa metode ini lebih efektif?
- Apa tantangan yang dihadapi saat menggunakan metode tradisional dalam pengelolaan proyek keamanan informasi di era perubahan teknologi yang pesat?
- Apakah ada rencana Subdit Keamanan dan Pusat Data untuk tetap mempertahankan penggunaan metode tradisional atau akan beralih ke metode yang lebih modern untuk pengelolaan proyek keamanan?

### **Design Factor 10 : Technology Adoption Strategy**

Value 1: *First Mover*

- Bagaimana SUBDIT Keamanan dan Pusat Data mengidentifikasi teknologi-teknologi baru yang potensial untuk diimplementasikan?
- Apa strategi mitigasi risiko yang diterapkan ketika mengadopsi teknologi yang relatif baru?

Value 2: *Follower*

- Bagaimana SUBDIT Keamanan dan Pusat Data memantau dan menganalisis kesuksesan implementasi teknologi di institusi lain sebelum mengadopsinya?



- Apa kriteria yang digunakan dalam memilih teknologi yang sudah terbukti efektif di tempat lain?

Value 3: *Slow Adopter*

- Apa parameter yang digunakan untuk menentukan waktu yang tepat dalam mengadopsi teknologi yang sudah established?
- Apa pertimbangan utama yang membuat SUBDIT memilih untuk menunda adopsi teknologi baru?