

# **MINIBOOK AUDIT SISTEM INFORMASI**

## **Dosen Pengampu:**

Hasdi Putra, M.T	198904212019032024
Adi Arga Arifnur, M.Kom	199208202019031005



## **KELOMPOK 1**

1. Muhammad Irsyadul Fikri	2111521015
2. Thomas Nobel Asfar	2111521019
3. Rafiqatul Ulya	2111522003
4. Syakina Triyana	2111522017
5. Khairunnisa Salsabila	2111522031
6. Ghina Fitri Hidayah	2111523015
7. Sukma Anggarmadi	2111527001

**DEPARTEMEN SISTEM INFORMASI  
FAKULTAS TEKNOLOGI INFORMASI  
UNIVERSITAS ANDALAS  
2024**

## **DAFTAR ISI**

<b>1. Definisi Audit Sistem Informasi.....</b>	<b>1</b>
<b>2. Tujuan Audit Sistem Informasi.....</b>	<b>1</b>
<b>3. Proses Audit Sistem Informasi.....</b>	<b>2</b>
<b>4. Macam macam Framework yang digunakan dalam Audit Sistem Informasi.....</b>	<b>4</b>
<b>5. Aspek Audit Sistem Informasi.....</b>	<b>6</b>
<b>6. Definisi Sertifikasi CISA.....</b>	<b>7</b>
<b>7. Ringkasan 5 Domain yang ada di CISA.....</b>	<b>9</b>

## **1. Definisi Audit Sistem Informasi**

Menurut Ron Weber Audit sistem informasi adalah proses pengumpulan dan penilaian bukti – bukti untuk menentukan apakah sistem komputer dapat mengamankan aset, memelihara integritas data, dapat mendorong pencapaian tujuan organisasi secara efektif dan menggunakan sumberdaya secara efisien.

Audit sistem informasi adalah proses dikumpulkan data dan dievaluasinya bukti untuk menentukan apakah suatu sistem aplikasi komputerisasi sudah diterapkan dan menerapkan sistem pengendalian internal yang sudah sepadan, seluruh aktiva dilindungi dengan baik atau disalahgunakan dan juga terjamin integritas data, keandalan dan juga efektifitas dan efisiensi penyelenggaraan informasi berbasis komputer

## **2. Tujuan Audit Sistem Informasi**

Audit sistem informasi memiliki empat tujuan utama yang harus diperhatikan dalam proses pengumpulan dan penilaian bukti-bukti untuk menentukan apakah suatu sistem informasi dapat memenuhi kebutuhan pengguna dengan sumber daya informasi yang rendah. Berikut adalah empat tujuan audit sistem informasi:

### **1. Mengamankan Aset:**

Mengamankan aset yang berhubungan dengan instalasi sistem informasi mencakup perangkat keras, perangkat lunak, fasilitas, manusia, file data, dokumentasi sistem, dan peralatan pendukung lainnya. Pengamanan aset ini sangat penting untuk mencegah penyalahgunaan aset perusahaan, seperti kerusakan perangkat keras, pencurian perangkat lunak, atau penggunaan peralatan pendukung untuk tujuan yang tidak diotorisasi.

### **2. Menjaga Integritas Data:**

Integritas data berarti data memiliki atribut-atribut tertentu seperti kelengkapan, kebenaran, dan keakuratan. Data yang tidak memiliki integritas dapat menyebabkan keputusan yang tidak sesuai dan kerugian organisasi. Audit sistem informasi harus memastikan bahwa data yang digunakan dalam pengambilan keputusan memiliki atribut-atribut tersebut.

### **3. Menjaga Efektivitas Sistem:**

Efektivitas sistem informasi perusahaan memiliki peranan penting dalam proses pengambilan keputusan. Sistem informasi yang efektif harus sesuai dengan kebutuhan pengguna dan dapat membantu organisasi mencapai

tujuan strategis. Audit sistem informasi harus memastikan bahwa sistem informasi yang digunakan efektif dan efisien dalam mendukung operasional organisasi.

#### **4. Mencapai Efisiensi Sumber Daya:**

Efisiensi sumber daya sangat penting dalam penggunaan sistem informasi. Audit sistem informasi harus memastikan bahwa sistem informasi digunakan secara efisien dan tidak ada lagi kapasitas sistem yang menganggur. Efisiensi sistem pengolahan data menjadi penting untuk memastikan bahwa organisasi dapat beroperasi secara efektif dan efisien

### **3. Proses Audit Sistem Informasi**

Audit sistem informasi adalah bagian penting dari tata kelola teknologi informasi (TI) dan berfungsi untuk memastikan bahwa sistem TI yang ada di suatu organisasi berfungsi secara efektif, efisien, dan sesuai dengan kebijakan dan regulasi yang berlaku. CISA (Certified Information Systems Auditor) adalah sertifikasi yang diberikan oleh ISACA (Information Systems Audit and Control Association) kepada para profesional yang memiliki pengetahuan dan pengalaman dalam audit sistem informasi. Berikut adalah penjelasan tentang proses audit sistem informasi berdasarkan praktik yang dianjurkan dalam CISA:

#### **A. Perencanaan Audit**

- **Pemahaman Lingkungan TI:** Auditor harus memahami lingkungan TI organisasi, termasuk arsitektur sistem, aplikasi yang digunakan, dan proses bisnis yang didukung oleh TI.
- **Identifikasi Risiko:** Menilai risiko terkait dengan sistem informasi yang akan diaudit, termasuk risiko keamanan, integritas data, dan ketersediaan sistem.
- **Penentuan Ruang Lingkup dan Tujuan Audit:** Mendefinisikan ruang lingkup audit, tujuan spesifik, serta sumber daya yang diperlukan.
- **Pengembangan Rencana Audit:** Membuat rencana audit yang mencakup jadwal, prosedur, dan metodologi yang akan digunakan selama audit.

## **B. Pelaksanaan Audit**

- **Pengumpulan Data:** Mengumpulkan data melalui wawancara, kuesioner, observasi langsung, dan peninjauan dokumentasi.
- **Evaluasi Pengendalian Internal:** Menilai efektivitas pengendalian internal yang ada untuk melindungi aset informasi dan menjamin keandalan data.
- **Pengujian Kepatuhan:** Menguji apakah kebijakan, prosedur, dan kontrol TI dipatuhi sesuai dengan standar dan regulasi yang berlaku.
- **Pengujian Substantif:** Memverifikasi keakuratan dan validitas data dalam sistem informasi.

## **C. Pelaporan Audit**

- **Penyusunan Laporan Audit:** Menyusun laporan yang mencakup temuan audit, analisis, dan rekomendasi perbaikan.
- **Diskusi dengan Manajemen:** Mengkomunikasikan temuan dan rekomendasi kepada manajemen untuk memastikan bahwa mereka memahami risiko yang diidentifikasi dan langkah-langkah yang perlu diambil.
- **Tindak Lanjut:** Memantau implementasi rekomendasi dan perbaikan yang telah disepakati oleh manajemen.

## **D. Peningkatan Berkelanjutan**

- **Evaluasi Proses Audit:** Melakukan evaluasi terhadap proses audit yang telah dilaksanakan untuk mengidentifikasi area yang perlu diperbaiki.
- **Pengembangan Kompetensi Auditor:** Meningkatkan kompetensi auditor melalui pelatihan berkelanjutan dan sertifikasi tambahan.

## **E. Standar dan Kerangka Kerja yang Digunakan**

Dalam proses audit sistem informasi, auditor CISA menggunakan berbagai standar dan kerangka kerja seperti:

- **COBIT (Control Objectives for Information and Related Technologies):** Kerangka kerja untuk tata kelola dan manajemen TI yang membantu memastikan bahwa sistem TI mendukung tujuan bisnis.
- **ISO/IEC 27001:** Standar untuk sistem manajemen keamanan informasi.
- **NIST (National Institute of Standards and Technology) Framework:** Panduan untuk mengelola dan mengurangi risiko keamanan siber.

#### **F. Keterampilan dan Pengetahuan yang Diperlukan Auditor CISA**

- **Pengetahuan teknis:** Pemahaman mendalam tentang infrastruktur TI, jaringan, aplikasi, dan sistem operasi.
- **Kemampuan analisis risiko:** Kemampuan untuk mengidentifikasi dan menilai risiko TI.
- **Kemampuan komunikasi:** Kemampuan untuk berkomunikasi secara efektif dengan berbagai pemangku kepentingan, termasuk manajemen dan tim teknis.
- **Pemahaman tentang regulasi:** Pengetahuan tentang regulasi yang relevan dengan industri yang diaudit.

Dengan mengikuti proses ini, auditor CISA dapat memastikan bahwa sistem informasi organisasi dikelola dan dikendalikan dengan baik, serta meminimalkan risiko yang dapat berdampak negatif pada operasional dan keberlanjutan bisnis.

#### **4. Macam macam Framework yang digunakan dalam Audit Sistem Informasi**

Dalam audit sistem informasi, berbagai macam kerangka kerja atau *framework* digunakan untuk memastikan bahwa sistem informasi, dapat beroperasi secara efektif, efisien, dan sesuai dengan regulasi yang berlaku. Beberapa *framework* yang umum digunakan sebagai berikut:

- a. **COBIT (Control Objectives for Information and Related Technologies):**
  - **COBIT 5:** Framework yang menyediakan model komprehensif untuk mengelola dan mengatur teknologi informasi dalam organisasi. COBIT 5 membantu memastikan bahwa TI mendukung tujuan bisnis dan mengelola risiko terkait TI.
  - **COBIT 2019:** Pembaruan dari COBIT 5 yang menawarkan panduan yang lebih rinci dan fleksibel untuk pengelolaan dan tata kelola TI.
- b. **ITIL (Information Technology Infrastructure Library):**

Framework yang berfokus pada pengelolaan layanan TI, ITIL menyediakan panduan praktik terbaik untuk manajemen layanan TI guna meningkatkan efisiensi dan efektivitas layanan TI dalam organisasi.

c. **ISO/IEC 27001:**

Standar internasional yang menetapkan persyaratan untuk Sistem Manajemen Keamanan Informasi (ISMS). ISO/IEC 27001 membantu organisasi melindungi informasi dengan pendekatan manajemen risiko yang sistematis.

d. **NIST (National Institute of Standards and Technology) Cybersecurity Framework:**

Framework yang dikembangkan oleh NIST untuk membantu organisasi mengelola dan mengurangi risiko cybersecurity. Framework ini terdiri dari lima fungsi utama: Identify, Protect, Detect, Respond, dan Recover.

e. **COSO (Committee of Sponsoring Organizations of the Treadway Commission):**

Kerangka kerja yang berfokus pada pengendalian internal dan manajemen risiko perusahaan. COSO sering digunakan dalam konteks audit keuangan, tetapi juga relevan untuk audit TI.

f. **TOGAF (The Open Group Architecture Framework):**

Framework untuk pengembangan dan pengelolaan arsitektur perusahaan. TOGAF membantu memastikan bahwa arsitektur TI sesuai dengan tujuan bisnis dan kebutuhan organisasi.

g. **PCI DSS (Payment Card Industry Data Security Standard):**

Standar keamanan informasi yang ditetapkan oleh industri pembayaran untuk melindungi data kartu pembayaran. PCI DSS sangat relevan untuk organisasi yang menangani transaksi kartu kredit.

h. **CMMI (Capability Maturity Model Integration):**

Model untuk meningkatkan proses yang mengukur kematangan proses dalam organisasi. CMMI digunakan untuk memastikan bahwa proses pengembangan dan pemeliharaan perangkat lunak efektif dan efisien.

i. **SABSA (Sherwood Applied Business Security Architecture):**

Framework untuk pengembangan arsitektur keamanan TI yang selaras dengan tujuan bisnis. SABSA membantu memastikan bahwa strategi keamanan mendukung kebutuhan bisnis dan operasional.

j. **O-ISM3 (The Open Information Security Management Maturity Model):**

Framework yang menyediakan model untuk pengelolaan keamanan informasi yang terukur dan berkelanjutan, dengan fokus pada peningkatan berkelanjutan dalam manajemen keamanan informasi.

## **5. Aspek Audit Sistem Informasi**

Jika dilihat dari tujuannya, audit Sistem Informasi dapat dikelompokkan ke dalam dua aspek utama dari ketatakelolaan IT, yaitu :

a. **Conformance (Kesesuaian)**

Kesesuaian merujuk pada penilaian terhadap sejauh mana sistem tersebut memenuhi standar dan persyaratan yang telah ditetapkan. Fokus utama dari kelompok tujuan ini adalah untuk mengevaluasi dan memverifikasi apakah sistem informasi telah mematuhi prinsip-prinsip dasar. Aspek kesesuaian yang dinilai meliputi:

1. Confidentiality (Kerahasiaan): Keamanan informasi yang menjamin bahwa hanya pihak yang berwenang yang dapat mengakses informasi tersebut.
2. Integrity (Integritas): Konsistensi, keutuhan, dan kebenaran informasi serta prosesnya.
3. Availability (Ketersediaan): Ketersediaan informasi dan sistem dalam jangka waktu yang dibutuhkan oleh organisasi.
4. Compliance (Kepatuhan): Kepatuhan terhadap peraturan, kebijakan, standar, dan regulasi yang berlaku.

Tujuan dari audit kesesuaian adalah untuk menentukan sejauh mana sistem informasi dan prosesnya mematuhi standar keselamatan, keamanan, dan regulasi yang berlaku.



## **b. Performance (Kinerja)**

Kinerja mengacu pada kemampuan sistem informasi untuk berfungsi secara optimal dalam mencapai tujuan bisnisnya. Audit kinerja bertujuan untuk mengevaluasi dan memastikan bahwa sistem informasi tidak hanya beroperasi, tetapi juga memberikan manfaat yang diharapkan secara efektif dan efisien. Aspek kinerja yang dinilai meliputi:

1. Effectiveness (Efektivitas): Sejauh mana sistem informasi mencapai tujuan dan menghasilkan output yang diharapkan.
2. Efficiency (Efisiensi): Seberapa baik sistem informasi memanfaatkan sumber daya (seperti waktu, tenaga kerja, dan biaya) untuk mencapai tujuan yang telah ditetapkan.
3. Reliability (Kehandalan): Kemampuan sistem informasi untuk memberikan layanan dan hasil yang konsisten dan dapat diandalkan.

Tujuan dari audit kinerja adalah untuk mengevaluasi seberapa baik sistem informasi dalam mencapai tujuan bisnisnya secara efisien, efektif, dan dapat diandalkan.

## **6. Definisi Sertifikasi CISA**

Sertifikasi Certified Information Systems Auditor (CISA) merupakan pengakuan global yang diberikan kepada para profesional di bidang audit, pengendalian, dan keamanan sistem informasi. Sertifikasi ini dikeluarkan oleh ISACA (Information Systems Audit and Control Association), sebuah organisasi profesional yang mengkhususkan diri dalam manajemen risiko dan keamanan sistem informasi.

CISA dirancang untuk menguji pengetahuan dan keterampilan individu dalam mengaudit, mengendalikan, dan memberikan jaminan atas sistem informasi organisasi. Fokus utamanya meliputi pengendalian internal, manajemen risiko, dan keamanan informasi, dengan menekankan pada audit sistem informasi, pengelolaan risiko, kebijakan keamanan, dan praktik terbaik dalam industri.

Persyaratan untuk mendapatkan sertifikasi CISA meliputi pendidikan dan pengalaman kerja yang ditentukan oleh ISACA, serta lulus ujian CISA yang mencakup berbagai topik terkait audit dan keamanan sistem informasi. Memegang

sertifikasi CISA memungkinkan para profesional untuk menunjukkan kompetensi mereka dalam mengaudit dan mengendalikan sistem informasi, yang dapat meningkatkan peluang karir dan memberikan pengakuan internasional di industri.

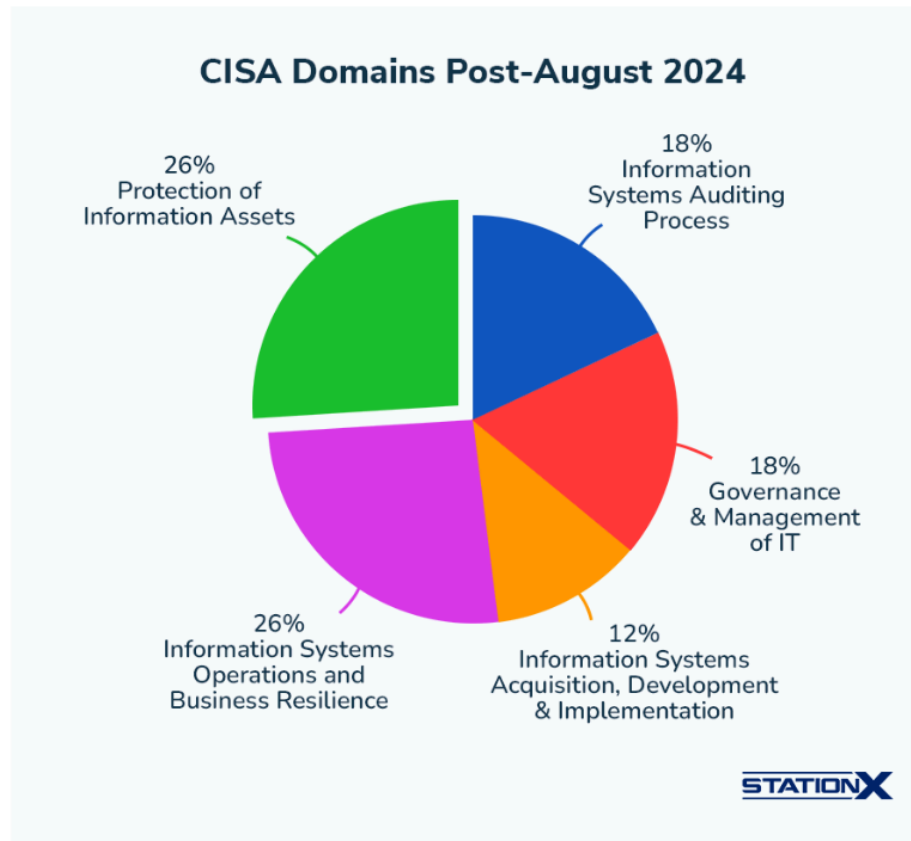
**Manfaat Sertifikasi CISA:**

1. Pengakuan Global: Sertifikasi CISA dikenal secara internasional dan diakui oleh organisasi di seluruh dunia. Ini membuka pintu untuk peluang karir yang lebih luas dan memberikan daya saing yang kuat dalam industri keamanan informasi.
2. Kompetensi dalam Audit: Sertifikasi ini menunjukkan bahwa pemegangnya memiliki kemampuan untuk melakukan audit keamanan informasi yang mendalam dan efektif. Ini sangat berharga dalam mengidentifikasi risiko dan mengelola keamanan sistem.
3. Kemampuan Mengendalikan Risiko: CISA mengajarkan cara mengidentifikasi, menilai, dan mengendalikan risiko yang terkait dengan keamanan informasi. Ini membantu organisasi dalam melindungi aset dan data yang sensitif.
4. Kesesuaian dengan Standar: Sertifikasi ini mencakup pemahaman mendalam tentang berbagai standar keamanan informasi, seperti ISO 27001, COBIT, dan lainnya. Ini penting untuk memastikan bahwa organisasi mematuhi regulasi dan standar yang berlaku.
5. Kemampuan Manajerial: CISA juga menguji kemampuan manajemen pemegangnya dalam mengelola proyek, tim, dan sumber daya yang terkait dengan keamanan informasi.

Sertifikasi ini dianggap sangat bernilai dalam dunia bisnis dan teknologi informasi, dengan banyak organisasi mencari profesional yang memiliki sertifikasi CISA untuk memastikan keamanan dan keandalan sistem informasi mereka. Selain itu, pemegang sertifikasi CISA juga dapat mengambil peran konsultan, auditor, atau manajer keamanan informasi di berbagai organisasi.

Dengan demikian, sertifikasi CISA bukan hanya menegaskan kualifikasi profesional, tetapi juga menawarkan jalur karir yang mapan dalam bidang audit dan keamanan sistem informasi.

## 7. Ringkasan 5 Domain yang ada di CISA



Berikut ini terkait domain pada CISA (*Certified Information Systems Auditor*)

### Domain 1: Information System Auditing Process

Domain pertama mencakup dasar-dasar audit TI, mulai dari proses audit hingga standar dan praktik terbaik jaminan. Domain ini bertujuan untuk menguji kemampuan Auditor dalam menilai keamanan informasi, kontrol, serta praktik dan prosedur risiko di suatu organisasi sesuai dengan pedoman dan metode audit yang sudah standar.

Pada domain 1, kita akan belajar cara merencanakan audit yang sesuai berdasarkan standar dan prosedur audit yang umum, serta kebutuhan organisasi yang Anda audit. Dalam ujian CISA, pertanyaan Domain 1 mencakup topik seperti jenis-jenis audit, teknik pengumpulan bukti, standar audit, dan laporan audit. Domain ini mencakup 18% dari konten ujian CISA dan terbagi menjadi dua bagian besar:

- (A) Perencanaan
- (B) Pelaksanaan.

**Berikut ini adalah beberapa istilah yang terdapat pada Domain 1 CISA :**

- IAR: Information Asset Register
- RACE Matrix: Risk Assessment and Control Evaluation Matrix
- COBIT: Control Objectives for Information and Related Technologies
- DRP: Disaster Recovery Plan
- GDPR: General Data Protection Regulation

**Contoh Soal dan Jawaban :**



PREVIOUS NEXT

The first phase of a risk analysis is:

- ☐ Identifying business risks
- ☐ Mitigating risk
- ☐ Evaluating business processes
- ☐ Monitoring

STATIONX

**Answers:**

**C. Evaluating business processes.**

The other answers are steps in the risk analysis process but are accomplished only after business processes are evaluated, and the purpose and importance of business activities are determined

## **Domain 2: Governance and Management of IT**

Domain kedua memvalidasi kemampuan kandidat untuk mengenali struktur dan praktik tata kelola serta manajemen TI yang baik dan menilai seberapa baik organisasi tersebut terstruktur. Ini mencakup prosedur tata kelola, kebijakan, dan kepemimpinan. Dalam

domain ini, Kita akan belajar tentang apa yang membuat struktur organisasi efisien dan efektif serta apa yang membuat tata kelola yang baik dari para manajer dan tim manajerial.

Pertanyaan Domain 2 akan mencakup topik seperti struktur organisasi, manajemen sumber daya, kematangan organisasi, dan jaminan kualitas TI. Domain ini menyumbang 18% dari konten ujian CISA, dan terbagi menjadi dua bagian besar:

(A) Tata Kelola TI

(B) Manajemen TI

**Berikut ini adalah beberapa istilah yang terdapat pada Domain 2 CISA :**

- BSC: Balanced Scorecard
- MEI: Management Effectiveness Inspection
- COSO: Committee of Sponsoring Organizations
- ITG: IT Governance
- ITIL: Information Technology Infrastructure Library
- CMMI: Capability Maturity Model Integration

**Contoh Soal dan Jawaban :**

PREVIOUS NEXT

Which model can be used to determine the maturity level of an organization's processes and focuses on whether an organization's processes have a level of maturity associated with measurement and continuous improvement?

☐ Capability Maturity Model Integration (CMMI)

☐ COBIT

☐ IT Infrastructure Library (ITIL)

☐ ISO 9000

STATIONX

**Answers:**

**Capability Maturity Model Integration (CMMI).**

CMMI is an integrated capability maturity model that measures the maturity level of an organization's process. The other frameworks are not used to measure maturity.

### **Domain 3: Information System Acquisition, Development, and Implementation**

Domain ketiga memvalidasi kemampuan kandidat untuk menilai seberapa baik pilihan sistem informasi suatu organisasi selaras dengan tujuan organisasi tersebut. Ini mencakup keputusan manajerial seperti kerangka kerja manajemen proyek yang harus diikuti dan jenis langganan perangkat lunak yang digunakan untuk mendukung tujuan bisnis.

Dalam domain ini, Kita akan mempelajari peran, implementasi, dan praktik manajemen proyek, serta sistem aplikasi bisnis dan metode terbaik yang digunakan untuk mendorong perusahaan mencapai tujuannya. Dalam ujian CISA, dapat mengharapkan pertanyaan Domain 3 mencakup topik seperti metodologi manajemen proyek, praktik penerapan infrastruktur, dan desain kontrol. Domain ini mencakup 12% dari konten ujian CISA dan terbagi menjadi dua bagian:

- (A) Akuisisi dan Pengembangan Sistem Informasi
- (B) Implementasi Sistem Informasi.

#### **Berikut ini adalah beberapa istilah yang terdapat pada Domain 3 CISA :**

- Agile: A kind of continuous development framework
- PMI: Project Management Institute
- SDLC: Software Development Lifecycle
- SaaS: Software as a Service
- WBS: Work Breakdown Structure

#### **Contoh Soal dan Jawaban :**

PREVIOUS

NEXT

Which of the following is NOT one of the alternatives considered when making a decision to purchase or develop a software application?

☐ Delivering the raw information to someone else to process and then purchasing the results

☐ Developing the application in-house

☐ Purchasing the application

☐ Renting the application (Software as a Service, or SaaS)

STATIONX

**Answers:**

**Delivering the raw information to someone else to process and then purchasing the results.**

The others are alternatives when making a “make versus buy” decision on software applications. The first answer is not normally an option, as there may be regulatory and intellectual property issues with delivering raw information to a third party and then purchasing the processed results

**Domain 4: Information Systems Operations and Business Resilience**

Domain keempat memvalidasi kemampuan kandidat untuk menilai efektivitas dan efisiensi struktur operasional dan kebijakan organisasi yang harus memastikan aliran informasi yang aman dan berkelanjutan. Dengan kata lain, domain ini memvalidasi kemampuan kandidat untuk mengaudit seberapa baik organisasi dapat memastikan kelangsungan bisnis dengan menanggapi masalah dan memastikan operasi yang terus-menerus dan efisien.

Pertanyaan Domain 4 mencakup topik seperti tata kelola data, respons dan manajemen insiden, manajemen basis data, dan rencana pemulihan bencana. Pertanyaan Domain 4 adalah yang paling umum dalam ujian CISA, bersama dengan Domain 5, jadi penting untuk mengetahui materi ini dengan baik. Domain ini mencakup 26% dari konten ujian CISA dan terbagi menjadi dua bagian

(A) Operasi Sistem Informasi

(B) Ketahanan Bisnis.

**Berikut ini adalah beberapa istilah yang terdapat pada Domain 4 CISA :**

- ITSM: IT Service Management
- SLA: Service Level Agreement
- KEDB: Known Error Database
- SIP: Service Improvement Plan
- BCP: Business Continuity Plan

### Contoh Soal dan Jawaban

PREVIOUS NEXT

A new CIO needs to gather information about applications. What does the CIO need to create?

☐ Project portfolio

☐ Configuration management database (CMDB)

☐ Data dictionary

☐ Application portfolio

STATIONX

**Answers:**

**Application portfolio.**

The CIO needs to create an application portfolio to catalog, manage, and measure applications in the environment. A project portfolio is used to track projects. A CMDB is a repository for every component in an environment that contains information on every configuration change made on those components. A data dictionary is a set of data in a database management system that describes the structure of databases stored there.

### Domain 5: Protection of Information Assets



Domain kelima memvalidasi kemampuan kandidat untuk menilai kebijakan dan proses perlindungan informasi suatu organisasi. Ini mencakup kemampuan organisasi untuk melindungi dari akses yang tidak sah atau kehilangan atau kerusakan data yang tidak disengaja, serta memastikan praktik sistem informasinya mematuhi undang-undang dan peraturan privasi. Dalam ujian CISA, dapat mengharapkan pertanyaan Domain 5 mencakup topik seperti infrastruktur kunci publik (PKI), keamanan jaringan, keamanan Internet-of-Things (IoT), dan kesadaran keamanan organisasi.

Bersama dengan Domain 4, domain ini mencakup sebagian besar materi dalam ujian, jadi penting untuk memahami domain ini dengan baik. Domain ini mencakup 26% dari konten ujian CISA dan terbagi menjadi dua bagian: (A) Keamanan dan Kontrol Aset Informasi dan (B) Manajemen Kejadian Keamanan.

**Berikut ini adalah beberapa istilah yang terdapat pada Domain 5 CISA :**

- ISP: Information Security Policy
- PKI: Public Key Infrastructure
- IDS: Intrusion Detection System
- IAM: Identity and Access Management
- ITAM: Information Technology Asset Management

**Contoh Soal dan Jawaban :**

PREVIOUS

NEXT

Video surveillance is an example of which type of control?

☐ Preventive only

☐ Preventive and deterrent

☐ Detective only

☐ Detective and deterrent

STATIONX

**Answers:****Detective and deterrent.**

Video surveillance is both a detective control (because it can record unwanted activity) and a deterrent control (because its presence may deter unwanted activity).

**Kesimpulan**

Ujian CISA mencakup lima domain yang menguji pengetahuan Anda tentang audit TI di berbagai area, mulai dari proses dasar audit sistem informasi hingga struktur organisasi dan pencegahan kehilangan data.

Seorang auditor TI sering diharapkan untuk merekomendasikan perbaikan bagi seluruh kebijakan dan praktik operasional, manajerial, dan prosedural sistem informasi suatu organisasi, sehingga ujian CISA mencakup berbagai materi audit TI.