TOP 10 TIPS
for the CISSP exam

Luis Alejandro Sosa , MSc - CISSP

Disclaimer

This document is completely free and is intended for anyone who is in the process of preparing for the CISSP exam (or another if apply). This is a contribution aligned with canon # 4 of the ISC² code of ethics:

"Promote and protect the profession"

This is an original creation of the author, however some terms, tips and language are the result of analysis from multiple sources and authors, the intention has never been to violate copyright, so if you find something against copyright , contact the author to the address h4r2s33@gmail.com to proceed to eliminate what does not comply.

I hope this small document is useful to you and if you have any questions do not hesitate to contact me:

Luis Sosa MSc , CISSP

TOP 10 - TIPS **for the CISSP exam**

TIP

Identify **keywords** that will help you **eliminate** responses (read **word** by **word**)

Note: it is very likely that you can eliminate 2 options and you will have a 50% chance of having the correct answer.

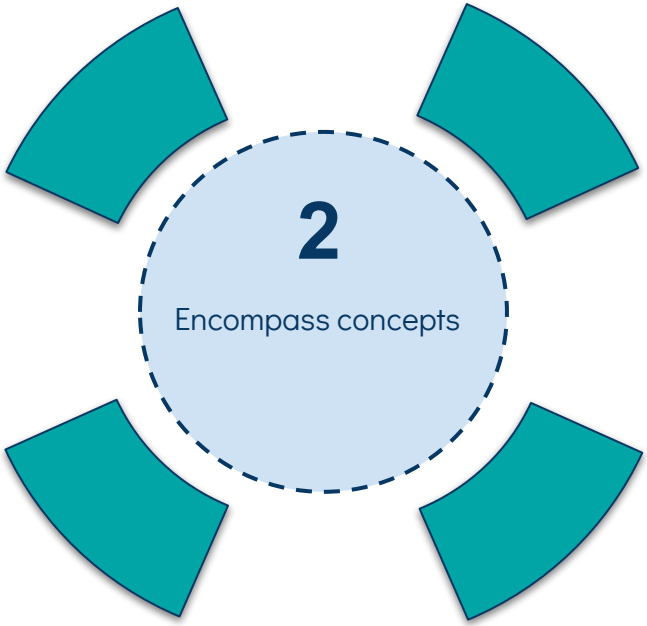
EXAMPLE

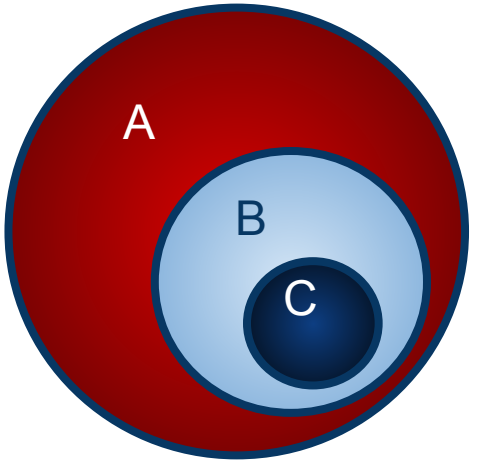
¿Which of the following **standards** is an organization **most** likely to rely on, in order to establish an information security management system? :

A. COBIT (it's a Framework not a standard) ✘ -- Eliminate
B. ITIL (set of best practices) ✘ -- Eliminate
C. ISO27001
D. ISO 31000

50% chances

TOP 10 - TIPS **for the CISSP exam**





TIP

"If you **identify** an option that **contains** the others, it is likely that this is the **correct** answer."

Note: You will find questions where all the options are correct, this TIP will help you to choose the most correct one.

EXAMPLE

¿what would you implement to ensure the **authentication** and **authorization** flows so that you can use a **third-party** application in the cloud?

A. SAML
B. OAUTH
C. **Federated Identity** (Correct)
D. OpenID Connect

It **contains** the others

TOP 10 - TIPS **for the CISSP exam**

3

Think strategically

"Think like a manager"

TIP

If you are asked about a **concept**/recommendation towards senior **management**, process improvement or **decision** making, use the "**Think like a manager**" concept, which means, choose the **high** level answer.

Note: Before making a decision, first of all think about the risk to the organization.

EXAMPLE

¿What is the **FIRST** thing you would do if your organization is thinking of **merging** or **acquiring** another company?

A. Infrastructure Vulnerability Analysis
B. Perform a pentesting on all organizations systems
C. Align controls between both companies
D. Perform a Risk Analysis (Correct)

Every decision starts with a **risk analysis**

TOP 10 - TIPS **for the CISSP exam**

4

Time Management
"Beta Questions"

TIP

In the exam you will find **questions** you have **no idea** of the answer or the topic they are asking for, I advise you not to **waste** time on these questions, **choose** an option and continue, **saving** time will give you **peace** of mind in the exam.

Note: It is likely that some of these questions are what is generally called **Beta questions**, these do **not score** in the exam, in addition this time could be used to take small breaks in the exam.

TOP 10 - TIPS **for the CISSP exam**

5

Interpret the hidden meaning

TIP

Most questions on the exam will not be **direct question**, for example they will not ask you which of the following is a symmetric encryption algorithm? ...

Rather, you will be asked.....

EXAMPLE

¿Which algorithm is **MOST** likely to be used to encrypt the **hard drive** of a workstation?

A. RSA
B. AES (Correct)
C. DH (Diffie Hellman)
D. ElGamal

1 Data at **rest** → **Symetric**

2 All are **Asymmetric** algorithms

Note: You must understand how to relate concepts and interpret the hidden meaning

TOP 10 - TIPS **for the CISSP exam**

6

Structure and **understand** the order of processes

TIP

It is **important understanding** the **order** in which the tasks or **phases** of a **process** are carried out. Rather than learning it by **heart**, it is **making sense** of what do I need to do in this **step** to use it in the **next one.**

EXAMPLE

1. In a **BCP** (Business Continuity Plan) I cannot start a **BIA** (Business Impact Analysis) analysis if I do not have **resources** to work with, that is, if I have not defined the **BCP Team** or if I have not defined the scope, then we can say BCP team selection goes first than BIA .

2. I cannot define an **MTD** (Maximum Tolerable Downtime) metric if I have not yet **prioritized** the business activities and the **resources/systems** that support them. Then MTD definition goes after business activities prioritization

TOP 10 - TIPS **for the CISSP exam**

7

"Elimination or filtering"

¿How does it work?

TIP

The **elimination** process **works** like this:

1. **Eliminate** 2 of the **wrong** answers using an **objective** process that is, with strong **justification** why it is not the answer**.**

2. For the **remaining** options, use a **subjective** process, that is, according to your **experience** or what you **intuit/sense** to choose the **correct** one between the 2 options.

TOP 10 - TIPS **for the CISSP exam**

8

Choose the "**most correct**" answer

TIP

In the exam you will **find** questions where **all** the **answers** are **correct**. Use step 2 (encompasses concepts) and / or step 3 ("Think like a manager") when you come across them so that you can **choose** the **most** correct option

TOP 10 - TIPS **for the CISSP exam**

9

Human life is the most important factor to protect

TIP

In the **exam** (and I hope in all you do) you **must** consider that **human life** is the most important factor. If you are **asked** about the **ultimate** goal of a security component / process and in the options some are related to the **safety** of people , it is very likely that this is the correct answer.

Note: **Physical security** generally has the **highest** priority and is tied to the concept of **protecting** human life and controlling access to physical locations.

EXAMPLE

Immediately after an earthquake occurs at one of ACME LTDA's main facilities and after a **Disaster** is declared, which is the **FIRST** thing the organization **must** ensure:

A. Minimal impact to critical data
B. Restoring of critical business processes
C. **Employees are safe** (Correct)
D. La protección de los sistemas físicos

Priority
1. People
2. Data
3. Business

TOP 10 - TIPS **for the CISSP exam**

10

Apply the ISC² code of ETHICS

4 Canons

TIP

The **ISC²** code of **ethics** is **evaluable** in the exam, so it is important to know the **4 canons** and their order of **priority**.

When you come across **questions** that include the **behavior** that the security professional should have, **apply** the code of **ethics** taking into account the **priority** of each canon

Remember: People have priority

EXAMPLE

1. Protect **society**, the common good, necessary public trust and confidence, and the infrastructure.
2. Act **honorably**, honestly, justly, responsibly, and legally.
3. Provide diligent and **competent** service to principals.
4. **Advance** and **protect** the profession.

TOP 10 - TIPS **para el CISSP**

BONUS

TOP 10 - TIPS for the **CISSP exam**

In the exam you must take the role of an **advisor**, security **consultant** or **manager** (Avoid a technical role)

Do not **assume** information that is not explicit in the questions, you can be sure that most of the exam questions are very well designed and do not give for **interpretations** or ambiguities, they are **tricky** (misleading) yes, but clear in what they are looking for the answer.

Before choosing an answer, you **must** balance the **cost-benefit**, remember that the priority for management is to generate **efficiency** for the business.
EXAMPLE: Compare the costs of implementing recovery sites: Cold Site Vs Warm Site Vs Hot Site

Every **decision** begins with a prior **risk analysis**

The **ultimate** responsible for security is not the security professional (CISO or CSO), it is **SENIOR MANAGEMENT**

Security must be present from the **initial** phases of the software or systems development process

Risk management does not seek to **eliminate** risk, but to **reduce** it to the **acceptable** levels that the organization is willing to **assume**

In the **CISSP** you don't fix **problems**, you fix **processes** ===> Choose the **long-term** solution and not the short-term one

always **think** about and **apply** the concept of **security in depth** (Security for each layer) ===> Perimeter - Network - System - Data

TOP 10 - TIPS **for the CISSP exam**

SOURCES - CREDITS

[1] https://www.studynotesandtheory.com/ - Luke Ahmed

[2] The Memory Palace - Prashant Mohan

[3] CISSP Practice Question with Spock & Kirk - Larry Greenblatt

[4] Why you will pass the CISSP - Kelly Handerhan

[5] https://www.isc2.org/ - ISC2 WebSite

[6] freepik.es - FREEPIK

Luis Sosa MSc , CISSP