**COURSE INTRODUCTION**

\*This course is just a basic introduction to cyber security, so what we want to understand here is the basic terminology that is used in cyber security, and the basic concepts that we have to understand in order to get started with cyber security.

\*This is an introductory course that will be broken down into 5 domains / areas of study

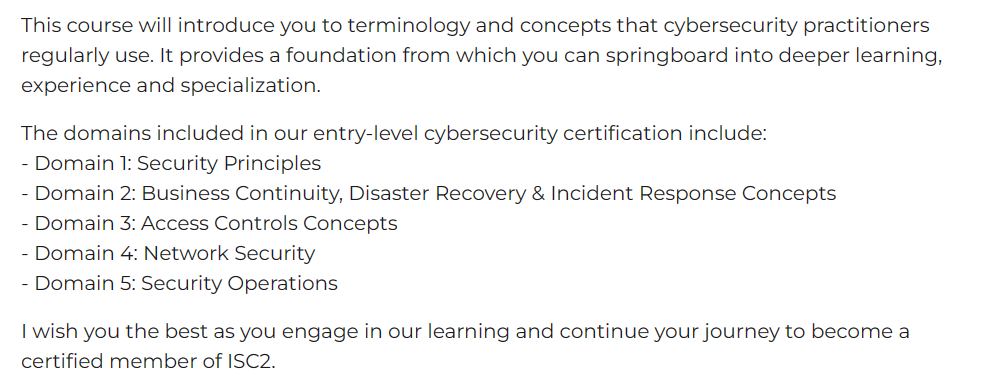
***Domain 1: Security Principles***

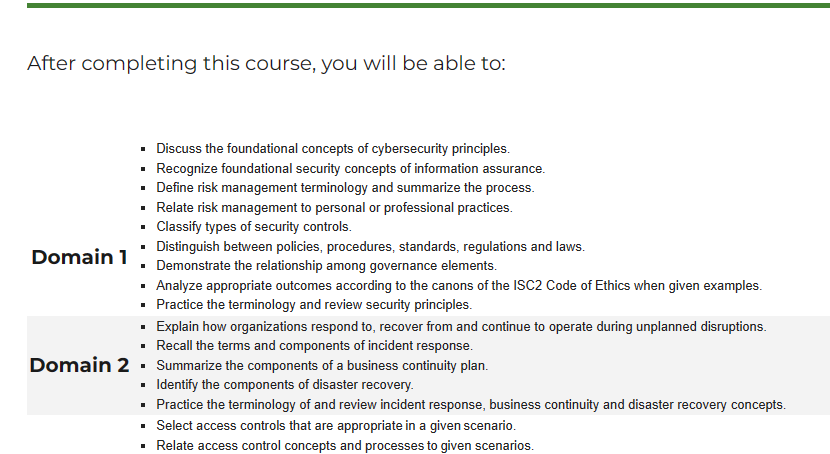
***Domain 2: Business Continuity, Disaster Recovery & Incident Response concepts***

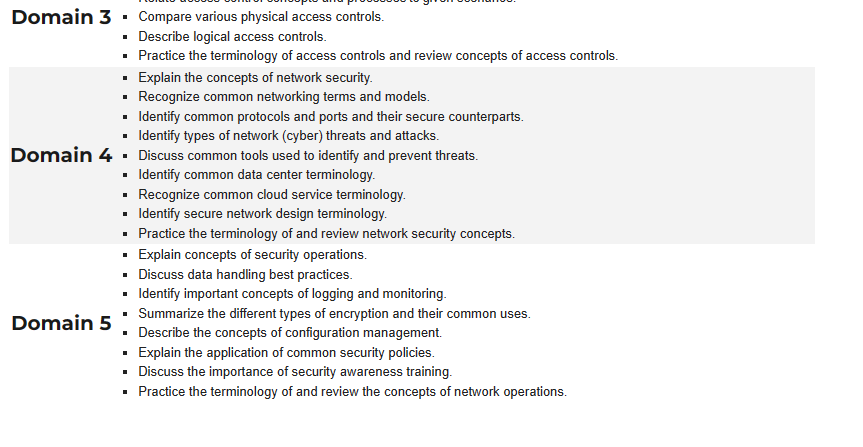
***Domain 3: Access Control Concepts***

***Domain 4: Network Security***

***Domain 5: Security Operations***

******





Pre-Assessment:

A screenshot of a computer

Description automatically generated

**Question 1:**

A screenshot of a computer

Description automatically generated

Correct answer: Physical Control

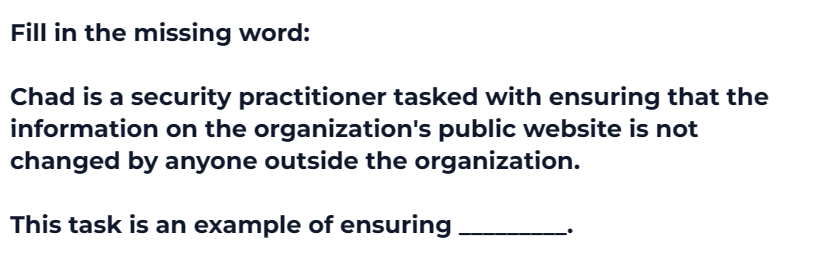
\*To ensure that cars don’t collide with pedestrians, we have to put up physical control measures, so when we talk about physical control measures, we are talking about physical objects that can serve as barriers between a car and a pedestrian, so we talking about physical Objects such as walls, fences, rails on the side of the road.

A screenshot of a computer

Description automatically generated

------------------------------------------------------------------------------------------------

**Question 2:**





Correct Answer: Integrity

\*What we basically want to do here is that we want to prevent unauthorized people, from modifying data that they don’t have the authority to modify.

\*Apart from having data that sits in a companies website, that cannot be modified outside the company, we can also look at a database, a database is used to store data. And only authorized people are supposed to be able to modify data that sits in a database.

\*So according to our security principles, the ability to design a system that prevents the unauthorized modification of data, speaks to the Integrity of the data.

\*So when we say that a database has Integrity, what we really mean is that the data in the database cannot be modified by someone who doesn’t have the authority to modify it.

\*so to ensure that the data that sites in the database cannot be modified by someone who doesn’t have the authority to modify it, we set up what’s called a root password for the database, where only an administrator knows the root password and only they can access the database directly.

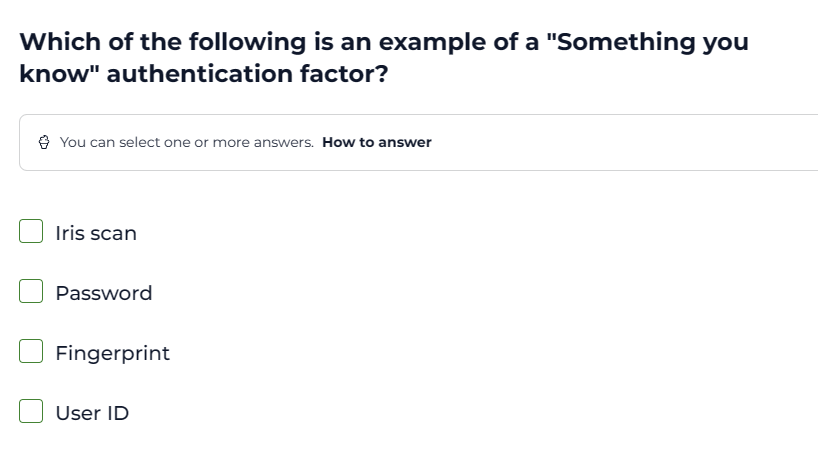
\*The second example would involve setting up levels of administrative privileges, this means that only an administrator has the ability to DROP and TRUNCATE tables in a database, a normal user has only what we call read and write privileges, so they can only view the data in the database and write new data to the database via an input form but they cannot delete data from the database.

A screenshot of a computer

Description automatically generated

------------------------------------------------------------------------------------------------

**Question 3:**



Correct Answer: Password

A white background with black text

Description automatically generated

A green rectangular sign with white text

Description automatically generated

------------------------------------------------------------------------------------------------

**Question 4:**

A screenshot of a questionnaire

Description automatically generated

Correct Answer:

\*So the basic idea here is that we want something that we can be able to authenticate who you are with, something that we can use to verify your identity, to verify that you are the person you are claiming to be.

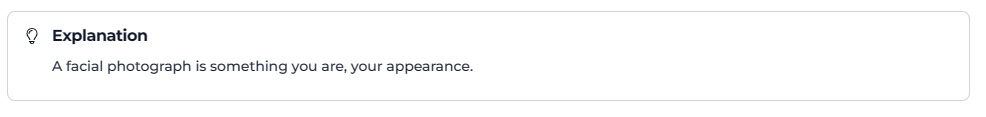
\*In this case the type of authentication is “something that you are”, this means that we want to use something that is physical, something that you are naturally born with, its not something that is assigned or given to you, or that you make up, its something that you are naturally and physically born with. And in this case that is a facial photograph.

\*This means that you would use your face as a form of authentication, this is the case with most modern Mobile devices, where you have the option to use facial recognition in order to verify your identity.

\*Facial recognition is an example of using “something that you are” as a form of authentication.

A green and white sign

Description automatically generated



------------------------------------------------------------------------------------------------

**Question 5:**

A screenshot of a missing word

Description automatically generated

Correct Answer: Non-repudiation

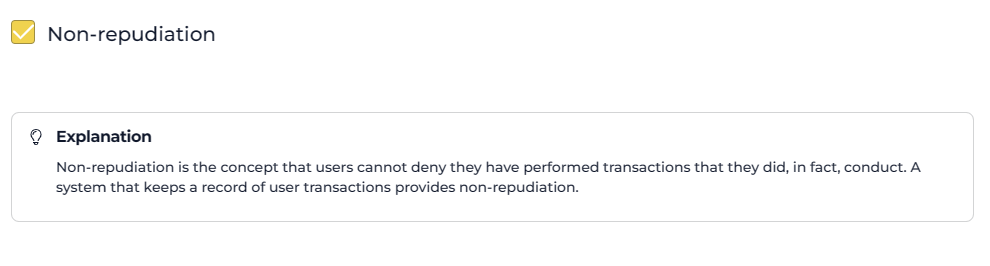
\*Non-repudiation is this basic concept that a user cannot deny the fact that they have performed a given transaction, so what we have to do is that we have to build systems that are able to prove that a user has performed a given transaction , so we need to build systems that are able to keep records of user transactions.

\*The moment we have systems that are able to keep track of user transactions, so that the systems can be used as proof that the user has performed the transaction, it means that we have a system that is able to provide us with non-repudiation.

\*Non-repudiation systems help us to detect fraudulent transactions that have not been committed by a user. So one of the easiest ways to create non-repudiation systems is to focus on anomalies, for example you can take location, what we can do is to train a model that can easily discover patterns in location, so if a user performs 90% of their transactions in Johannesburg (they withdraw cash at an ATM in Johannesburg 90% of the time) , they moment they try to perform a transaction in Durban which is a different city, then the system has to pick that up an amorality, as a deviation , as an outlier.

\*The moment the system picks up this anomality, it has to notify the client, and then request further authentication, this is when the system can use 2 factor authentication and ask the user to verify the transaction using a biometric method such as a fingerprint scan.

\*so a non-repudiation system is what we call a positive identifier, its used to positively identify that a user has indeed performed a given transaction.



------------------------------------------------------------------------------------------------

**Question 6:**

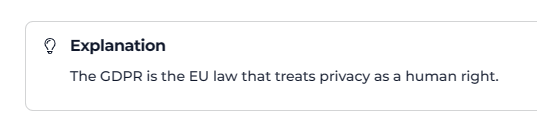


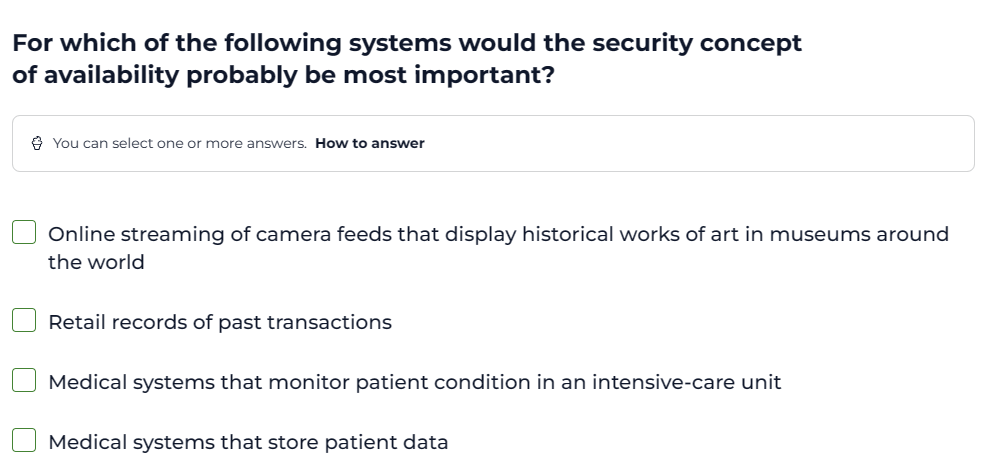


\*So we need to make sure that we are very clued up about different international laws that protect data privacy. This is important because we know that data is raw unprocessed facts, and we derive information that helps organisations and individuals in key decision making, from data.

\*The other key reason is that a lot of social media websites collect a lot of user data, when you sign up to a website, or even a recruitment website, when you send your cv to a recruiter via their website, you are sending sensitive data, that needs to be protected.

\*So there is international laws, that we have to know that go about protecting consumer data, and this is an example of how the European Union is protecting consumer data, via this “General Data Protection Regulation” GDPR





A green rectangular sign with white text

Description automatically generated

Okay the next thing that we need to understand is the CIA triad when it comes to data Availability, so what we mean by data Availability is that data should be readily and easily available in real time. The emphasise here is on real time, data should be available in real time.

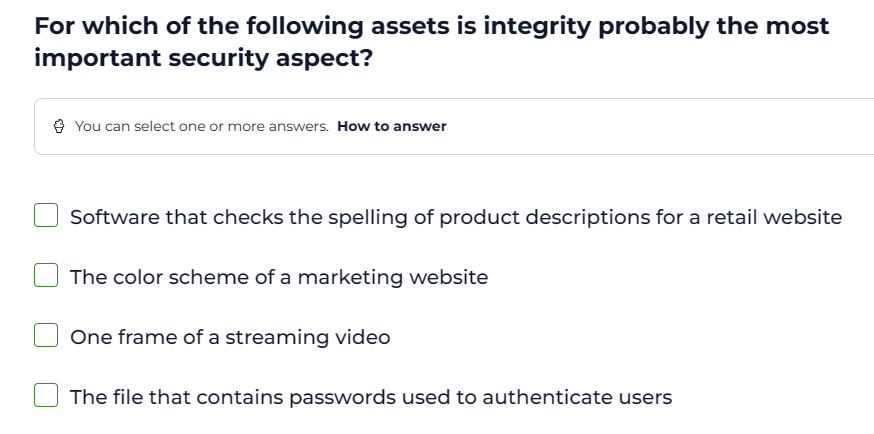
\*So here we are asked to describe a scenario, where the availability of data in real time, is important and applicable. And we can see from the example that has been given to us that the moment we have a system that is able to monitor patients in ICU, then it becomes very important that we are able to have a system that is able to deliver data in real time.

\*It becomes important that we have a system that is able to convert data into information in real-time.

\*So when it comes to data, not only is it important that we are able to store data in real time, it also becomes important that we are able to convert data into information in real time. The process of converting data into information can be automated, or it can be done manually by a data analyst using data analytics

A white background with black text

Description automatically generated



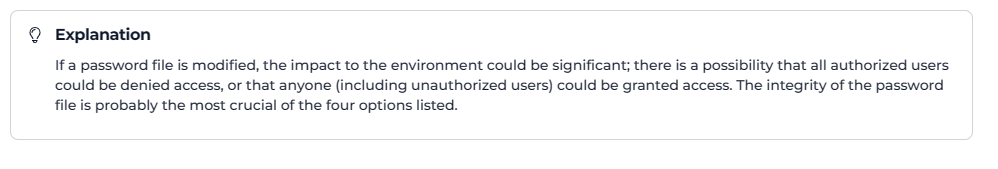
A green rectangular sign with white text

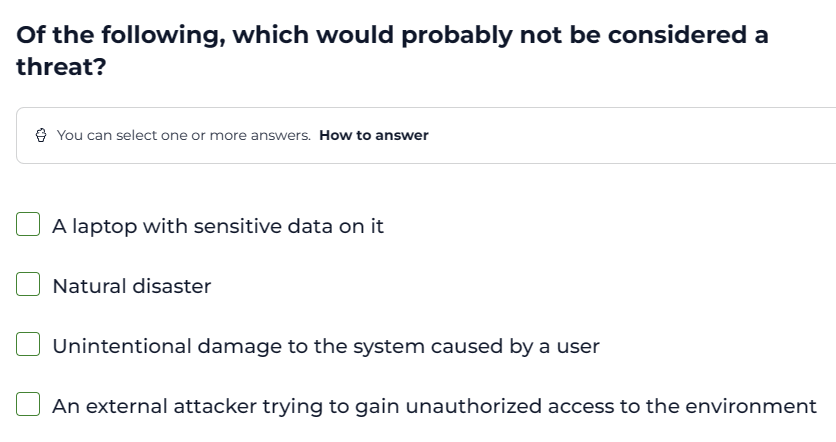
Description automatically generated

\*Data Integrity is simply the concept that data cannot be modified by people who don’t have the authority to modify it.

\*So which scenario would be most applicable to ensure that data cannot be modified by people who don’t have the authority to modify it. And such a case is a file that contains passwords that are used to authenticate users.

\*So if a file that contains passwords that are used to authenticate users is modified by someone who doesn’t have the authority to modify the file, then it means that our system cannot authenticate the users. So it means that for this system which uses passwords to authenticate users, data integrity is very important.





A green and white sign

Description automatically generated

\*So we are still looking at the domain of Security principles, and we ned to make sure that we understand the jargon that is used in cyber security, simply put we need to make sure that we understand the basic terminology that is used in cyber security. This means that we need to make sure that we understand the difference between an Asset and a Threat.

**Asset**: An asset in cyber security is something that has value and must be protected.

\*A computer that contains sensitive data is an Asset, because data is valuable, we know that we convert data into information, so the data is an asset, it is a raw unprocessed asset, and this means that we have to protect the laptop, because it is an asset, we have to protect the data in the laptop, because the data is an asset

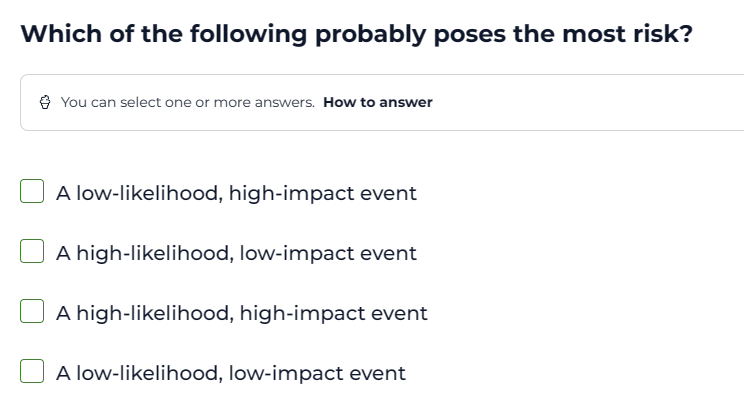
**Threat**: A threat is anything that poses a risk to an asset, anything that has the ability to damage an asset, anything that has the ability to corrupt the asset. So in cyber security we need to mitigate against the impact of a threat.

A green line on a white background

Description automatically generated

A screenshot of a computer

Description automatically generated

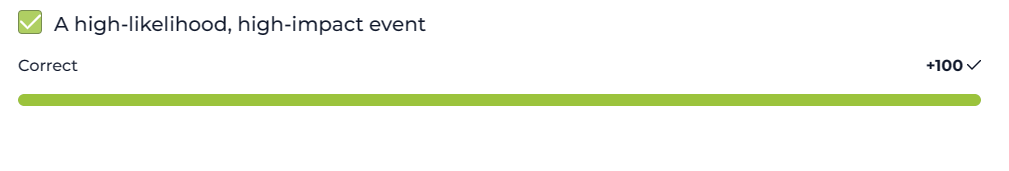


\*The question here is very simple: Once I have identified something as a threat, meaning that I have identified this thing as posing a potential risk to an asset. The question is how do I assess the risk that the threat poses. What metric do I use.

\*In order to measure a threat we use 2 metrics: The likelihood of the threat occurring( this means the probability of the threat occurring) and the impact of the threat when it has occurred.

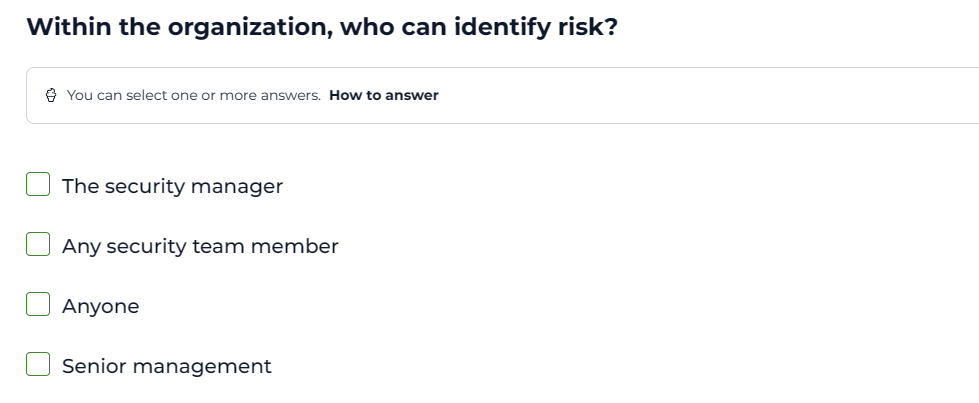
\*So if the threat has a high probability of occurring and a high impact when it has occurred then the threat is what we call a high priority threat.

\*So what you need to take of here is that cyber security is not a stand alone profession, it integrates Statistics, Mathematics, Data analytics and Data Science.



A green rectangular sign with white text

Description automatically generated



A green and white sign

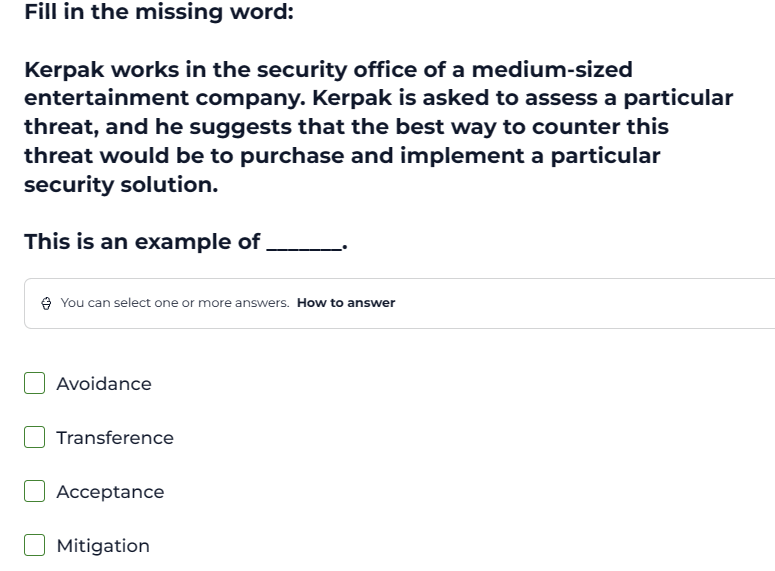
Description automatically generated

A white background with black and white clouds

Description automatically generated

A white rectangular with black text

Description automatically generated



A green rectangular sign with white text

Description automatically generated

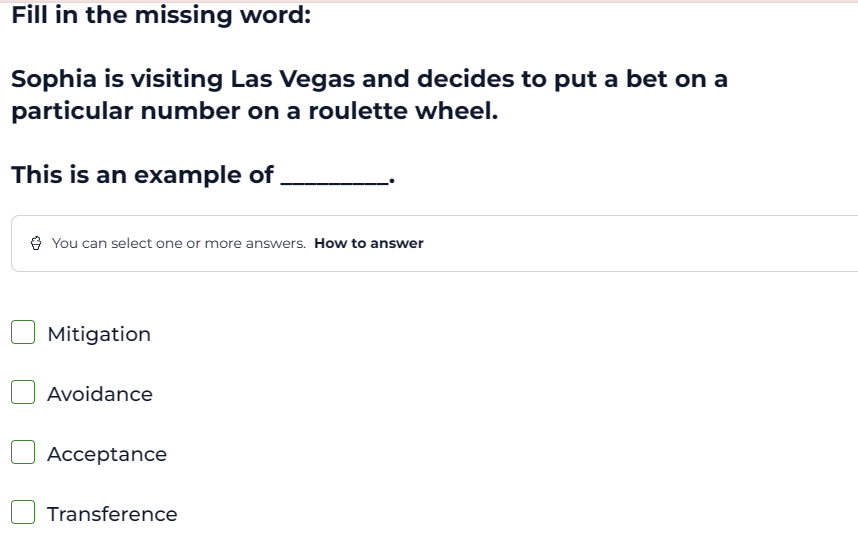
\*Okay so we have this person that works for an entertainment company, and they have identified a threat, to put it in simple terms they have identified something that poses a potential risk to a given asset in the company.

\*In order to counter this threat, the person suggests that the company implement a particular security solution.

\*so what the company is doing here is that they are mitigating against the security threat. By implementing a security solution to counter the threat they are mitigating against the threat.

A screenshot of a computer

Description automatically generated



\*So whats basically happening here is that we have this person that goes to a Casino, in order to gamble. We know that in order to gamble, there are certain risks that are associated with gambling but at the same time, there is also rewards associated with gambling.

\*But the issue with gambling is that you have to accept the risk that comes with gambling in order to potentially reap the rewards that come with gambling.

\*That’s why in this scenario that we are given, we talk about risk acceptance, you have to accept the risk associated with gambling in order to potentially reap the rewards associated with the risk.

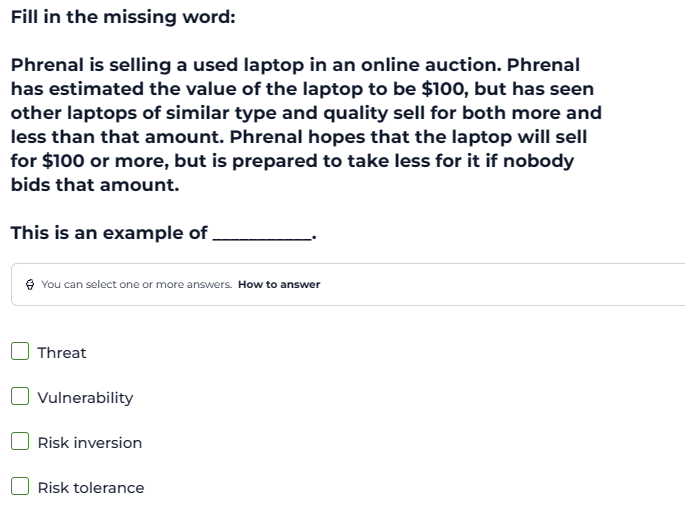
\*So when we think about risk in cyber security, we have to break down risk into 2 simple factors, benefits and losses. Because with every risk there is 2 possible outcomes either you win or you lose. So to understand why this risk is acceptance, we have to think about this scenario very well, when you gamble, you cannot control the range of profits and loses that you can make. You either win or you lose you cannot control the inbetween hence you have to accept the risk

A green and white rectangular sign

Description automatically generated

A close up of a text

Description automatically generated



\*We are still dealing with understanding risk in cyber security, so similar to the person that was gambling, they are taking a risk and with that risk they will either win or lose. This person has a min and a max in terms of the profits that they are willing to take and the loss that they are willing to take, and the amount of profit and loss that they are going to take is out of their control, because they don’t know if someone will buy the laptop or not.

A green and white sign

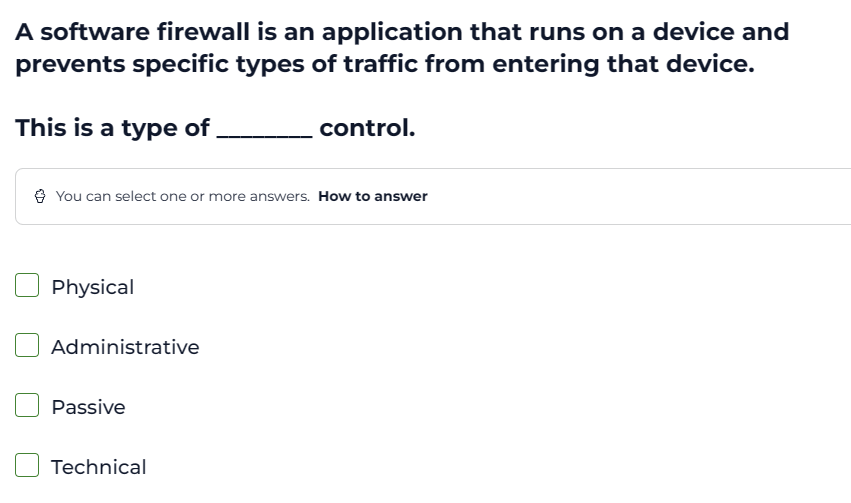
Description automatically generated

A green line with black text

Description automatically generated

A white rectangular box with black text

Description automatically generated

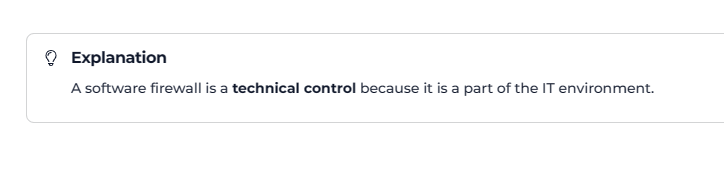


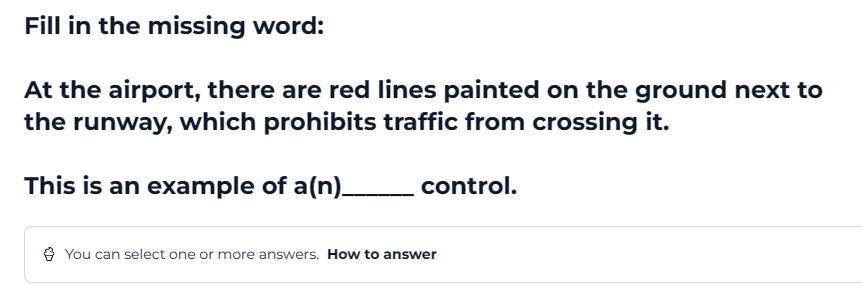
\*A firewall by definition is a software that is able to filter and control the type of traffic that is able to enter and leave a device.

\*So by the very definition of what a firewall is, a firewall is able to perform control operations.

\*A fire-wall performs what we call technical control, its software, that is administered in the IT side of things, hence it helps us perform technical control.







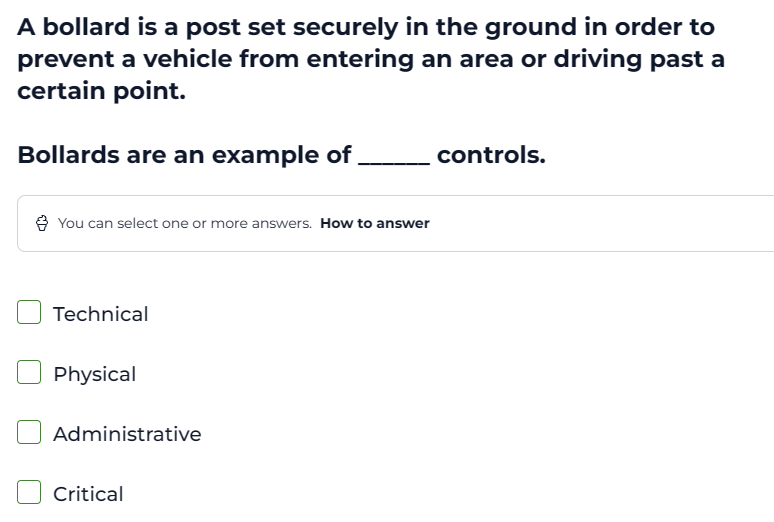
\*You have paintings that have been physically painted on the ground, in order to restrict traffic from crossing, this is an example of physical control.

\*so what we need to understand here is that physical control not only refers to things that are physical such as physical barriers in the form of walls and fences, but they also refer to things that that we can physically see that are there to introduce a form of physical barriers.



A close-up of a message

Description automatically generated



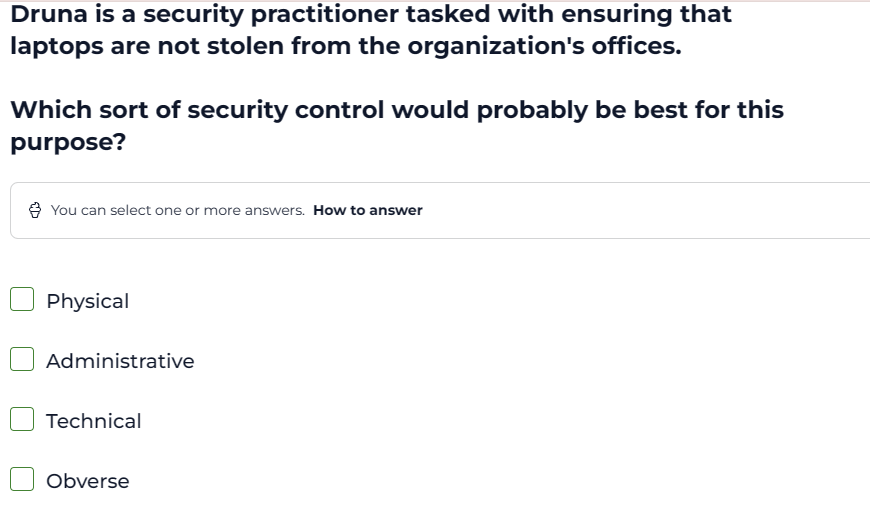
A green line on a white background

Description automatically generated

\*Physical control is something that we erect, such a wall or a fence that physically represents a barrier, or physical control can be something that is painted on the ground in order to represent physical control, and in this case we have a classic example of physical control, where we see that we have something that has been physically built or erected in order to represent physical control.

A white background with black text

Description automatically generated



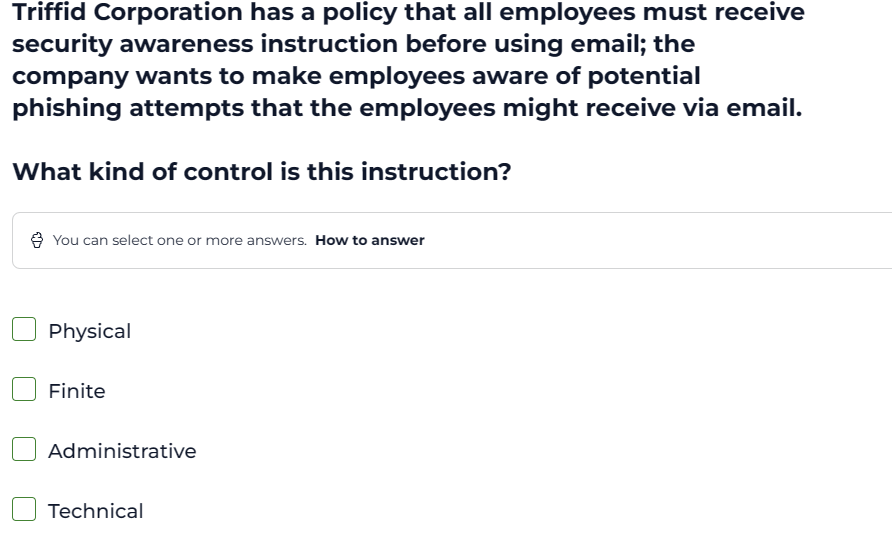
\*The moment we have a tangible Object, such a laptop and we want to secure the laptop, then we have to use physical control in order to secure the physical Object / tangible object.

A green line with white background

Description automatically generated

A white background with black text

Description automatically generated



\*The moment we have to give instructions, or train employees on company policy so that they don’t fall victim to online scams or email phishing then we are enforcing administrative control.

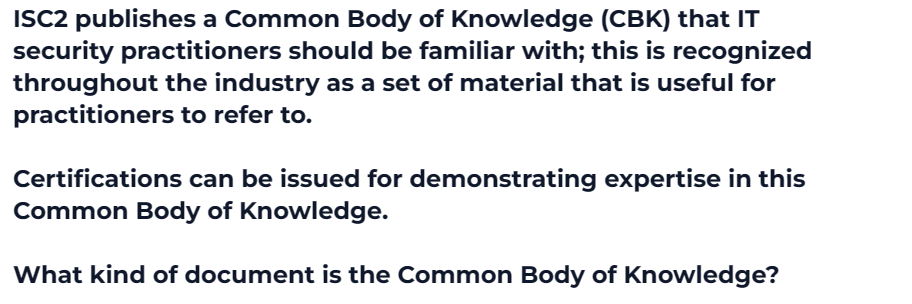
\*So administrative control is all about rules and instructions and company policy.

A black text on a white background

Description automatically generated

A close-up of a white background

Description automatically generated



A white background with blue text

Description automatically generated

\* A policy in cyber security is a set of rules, or instructions that have to be followed by the organisation or a set of people in an organisation or a department in an organisation. A policy is a subset of a standard, and what this means is that we use standards in order to draft policies.

\*A standard is a body of knowledge, that is internationally accepted and widely used, a standard is used as a reference when we draft policies. The key idea here is that a standard is a body of knowledge that is used throughout industry, it is accepted throughout industry, and we use it a reference, when we want to draft tailored policies.

\*A policy is very specific to a given organisation; it is tailored to that specific organisation.

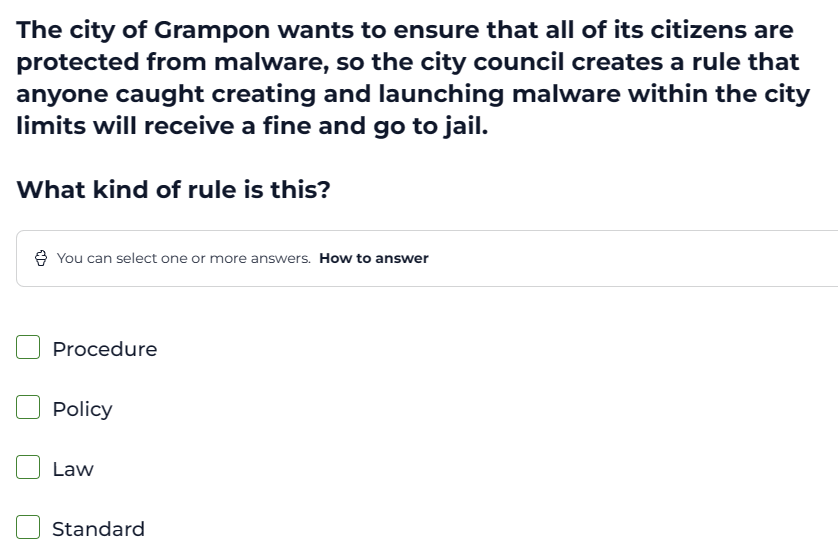
\*In this case we have a standard, we have a body of knowledge that is referenced and internationally accepted and used throughout industry.

\*



A close-up of a white background

Description automatically generated



\*