Okay, so welcome back and for this next session. We're talking about security policies and standards and this is part one.
There are a lot of questions in this topic area and so we're going to go ahead and jump in here and get started. Okay, so the first question involves CSP access.

The question reads: You have been asked to enable corporate role-based security and client antivirus validation
for access to your cloud systems provider. Which security service should you use to accomplish this? Okay, who wants to go first?
This is a guess but would it be the second one? Client encryption?
So I would then ask you what do you think that has to do with corporate role-based security and anti-virus validation? Whatever you're thinking.

I was just thinking it was encryption so it would protect the stuff but the client's stuff but, um, I'm not sure if that answer now; I don't know. That's okay; that's why we're here. So the second thing I would ask you to consider is as you look at the answer choices - DDoS mitigation, client encryption, Cloud access security broker and TPM - there are a couple of things to consider with these choices: The first one is the usual acronyms - acronyms everywhere - so, first thing then is what is TPM does anyone know what that is or what it stands for? TPM is a Trusted Platform Module. It's basically a piece of hardware embedded in a host computer, so it does enable encryption and security to a point.

But we are being asked about a security service, okay, now you can kind of look at TPM and go, "Yeah that provides a service, kind of, but not in the context of this question."

So, I would say TPM is the answer that is most incorrect or at least one of them, to me.
What are these other answers, which of these other answers is a security service or is not a security service?
Of the first three that are left which one do you think is not a security service?
Would it be number two, client encryption? I mean, I'm going to say that client encryption, to my thinking here, is the misdirector because it kind of could be a service.
But DDoS? First of all, what is DDoS? Anybody know what that is?
Okay so DDoS - again more acronyms, gotta love it - Distributed Denial of Service. Okay, one of the classic examples of this is and this really just doesn't happen much any more because everybody's you know gotten t0 the point where they just don't allow you know ICMP PING requests to hit their servers or allow their servers to respond to them; they're typically just dropped or reflected back. But back in the old days, it was one of the first where you could just keep throwing these PING requests at a server. I mean the thing would get really busy trying to respond to something that we really just use nowadays to, you know, test for connectivity.

And that was a very early type of Denial of Service kind of attack. Distributed Denial of Service typically uses botnets. So that is really - DDoS is an attack now mitigating this attack yeah it kind of could be a security service but to me it's still more incorrect than client

encryption and so when I look at this question and, if I'm trying to narrow down the solutions, the answer it's going to be either, in my mind,client encryption or Cloud access security broker. So, when I see a situation like this and maybe I'm struggling between two answers and again, you know, you're trying to pick the best answer. So, I go back to the question and I read it again and - this is an excellent test-taking tip - whenever I take certification exams to, for example, renew a certification even though, you know, I've been doing this a while and, you know, I'm always preparing for the exam and I always use the technique of reading the question twice.
But what I like to do is I read the first time look through the answers of choices,
see if anything stands out is obviously wrong or out of context with the question and, as I said in this case, the first and last answers would be more incorrect or out of context.
So I go back through again and I look at enable corporate role-based security, role-based security, and client anti-virus validation and then Cloud systems provide and when I put those pieces together one of the two remaining answers sort of stands out as a little more pertinent a little more to the point in the context of this question. Which one do you think that would be? Client encryption or Cloud access security broker? Cloud access security broker. Yeah, the service that you're going to get is enforcement of proper security measures okay and, you know, sort of the broker - the organization that functions as a cloud access security broker - is definitely going to ensure that security measures are implemented between Cloud solution and the customer organization. That is what their job is, okay?
And so you can consider them as enforcement points enabling enterprise security policies to be applied when the organization is trying to access the cloud resources and, you know; it's kind of like anything else it's a service if you're paying for it and whoever's selling it wants to stay in business, they're going to do a good job, okay. So in context this stands out as the correct answer and in fact it is. Let's move on to the next one.
So this question involves data concepts.
Which of the following describes a message for website visitors detailing how
their data will be processed and used?

Your choices are: privacy notice, public disclosure,
terms of agreement or information life cycle document. What do you think? Terms
of agreement?

Anybody else? Any other suggestions?

Information life cycle document?

Information life cycle document, okay.

So both that answer and terms of agreement are not correct in this context.

Terms of agreement basically is a document that outlines the rules and conditions of a relationship between two parties in the most general sense. Information life cycle document - so information has a life cycle within the business basically from the time it's created, distributed, used, maintained, and then disposed of.

So that's that's a lot of stuff for a message for website visitors detailing how their data will be processed and used. Okay, so if we rule out those last two suggestions that leaves us with privacy notice and public disclosure.
Which of those two do you think is correct, is the best answer? Public disclosure.
******Garbled*******
It's there well maybe all right public disclosure
Okay, so the the correct answer here Privacy notice.
Public disclosure - If you're uncertain of the context of public disclosure or the meaning of it as well, okay, can be a misdirector so, you know, public disclosure typically involves regulations and laws that govern the organization.
Okay, so for example, if you have a security breach and you're a large organization maybe your retailer you know something else banking you may be required to make a public statement about a serious security incident and you may have to disclose the details of the type of information that has been breached. Okay, so that's really at the heart of what public disclosure is and that just leaves us with privacy notice and again if you look at the context of the question.
We're told a message for website visitors detailing how their data will be used and in that context privacy notice makes the most sense.
of course now you know it means that you have to understand something about the sort of formal meanings of the other terms like public disclosure, terms of agreement - which is a little too general - and then information life cycle document, which is this big thing that is way beyond the scope or way out of context for what's being described in this question. This make sense?
So, do you hear me? Yes, I can hear you. So at this point I was confusing this sometimes you know you know certain websites they'll have yoU do like a terms of agreement and I feel like it kind of…Does it encompass everything or like when you're just signing and checking does it also are the privacy notices in the terms of agreement?
See, the difference is that you're really not agreeing to anything if you're just visiting a website, right, and you're … maybe you have to enter some information. I mean, who knows, maybe, you know, they want an email address or something because you're gonna - I don't know - you're gonna download something that's beneficial to you somehow. Okay, so you really being told that you, know, we're going to provide this to you but this is how we're going to use your data. okay in an agreement it's going to be a little more formalized than that because they're going to be rules and conditions of the relationship it's it's kind of like entering into a more formalized business relationship with this entity or this organization.
You're just a website visitor and this is just a message that tells you how your data, if any, will be processed and used and that really does fall under the heading of a privacy notice, okay?

That makes more sense, thank you. All right, let’s move on to the next question.

Okay, so this involves data security and the scenario is:

Paul's son is turning 10 years old in a month and he's been asking for a trampoline for his birthday. Paul decides to buy the trampoline online and have it delivered to their house. I think that they meant to say Paul's dad or somebody so once - oh no it's Paul's son who's turning 10 years old. Well, my mistake. So Paul decides to buy the trampoline online and have it delivered to their house once he purchases the trampoline and looks at his emailed confirmation receipt he notices that there are a bunch of x's in front of the last four digits of his credit card number. What method is this an example of? Your choices are: Data Hashing, Data Aggregation, Data Tokenization, or Data Masking.
Okay,
So let's see what are you thinking on this one?
Data hashing. Okay,
Is there a reason that that sticks out to you?
I kind of was doing something like this so it
might be I remember before this but I might
have I might have gotten the term incorrect
but I do remember covering this and that kind
of sticks out to me. Maybe it's masking.
Well it's not data hashing. Okay. So a hash and data hashing or the creation of a hash value ensures data integrity and basically what what happens is there's a mathematical algorithm that’s it's often just called a hashing algorithm and it takes in data and generates a hash value. What it's typically used for is that the hash is sent with the data and the reason
it's sent is so that when it gets to the receiving end the destination system can run the same data through a hashing algorithm, the same hashing algorithm, and generate a hash value.
I think the most common place that I've seen is personally is downloading some software and especially stuff that's - well not especially it could be open source it could be something you pay for and it's often doneso that you the customer have a way to verify the integrity of the download that you just made because if it you know the integrity was suspect then you probably wouldn't you know decompress the file or run the program right because it could be it could be it could have been messed with.
Okay, so it's definitely not Data Hashing and now that leaves Aggregation and
Tokenization…

And also data masking, so it leaves us with three
choices and of the three choices - Aggregating, Tokenizing or Masking - which of those three do you think would be the least correct? We're trying to whittle this down here, trying to narrow the results down to the correct one.
So what is Aggregation?
Okay, if you think about it and if you’ve ever seen, for example, Local Area Network segment - and and we're talking wired here not wireless just to keep it simple. You would often see what we would call a layer two switch and the layer 2 switch acts as an aggregation point. In other

words, it aggregates or collects signals from end users or hosts. Okay, so a common example of this could be you know you're you're having your friends over for LAN party. Okay, so you have a small switch and you invite all your friends over and you're like okay everybody plug in we're gonna you know play Call of Duty and you know crash each other's planes and so on and so forth. So what's happening is the switch is the aggregation point so aggregation and specifically data aggregation is taking and summarizing say a large pool of data for some other purpose, usually high-level analysis. Okay, so you can take lots of data from different databases and organize it into a simpler, easier-to-use medium or usually doing something like uh utilizing sums, averages, or means as references for this big pool of data that you're trying to summarize. So that doesn't sound like what Paul is seeing on his receipt so that really leaves us with tokenization or masking. Of those two choices, what do you think it is when instead of printing out the whole 16 digits of a credit card number, X's are printed out and only the last four digits are preserved as numbers?
Does that sound like tokenizing or masking? What do you think?
Masking? Yeah, that's correct the answer is masking. When we talk about data tokenization so this is when you have sensitive information and it is substituted with a non-relevant data string and we would call that a token, okay. And so the string is then stored in a data map and you know can be looked up to convert the token back to the sensitive data as you need to and in fact it's a common technique for storing credit card information so that credit card data is not stored with the customer data. So we kind of replace the sensitive stuff with tokens. What this scenario describes is definitely called Data Masking and that is that we are absolutely masking the other 12 digits of the credit card number with X's. Let's go on to the next one.

So this question involves data types and the question is: Which of the following is not an example of PII? Your choices are: A static IP address when someone browses the web; An IP address that is dynamically assigned by the ISP; A social security number or; Biometric data.

So the name of the game here again is acronyms. Let's start with PII.

What does that mean? What does that stand for? Is it Personally Identifiable Information? Absolutely is, yes, very good Morgan; wonderful. Okay, so we're looking for the choice that is not an example of PII so let's start at the bottom with Biometric Data. Do you think that's PII? Yes. Yeah. so something like a fingerprint -

that's personally identifiable information. What about a social security number?
Well, okay, so they're all supposed to be unique and unique to us so that would be PII. We're still looking for an example or one of the choices that's not PII, so now that leaves us with IP addresses: one that is dynamically assigned and one that is statically assigned.

So what do you think? Would it be the dynamic one? Okay and why do you think that?
Because static is staying in one place and dynamic it's just like it's multiple and changes. So an IP address that is dynamically assigned by the ISP is if you release your IP address and you need to renew it or your system does it on your behalf which happens okay?
An IP address is grabbed out of the pool of free addresses and assigned to your host so it's not predictable it's not identifiable. A static IP address on the other hand is chosen and statically assigned and it sticks and so if it sticks it's referenceable and can be PII. So in this question and in this context, an IP address that is dynamically assigned by the ISP is not an example of PII. Okay, all right, moving on Data Types (2):

Can you explain what PII stands for again? Yes, PII stands for Personally Identifiable Information.
and so the examples are things like your Social Security Number, your fingerprint, could be a retina scan: anything that can be used to identify you personally.
All right. Thank you. You're welcome.

Data Types (2): Which of the following examples is the least appropriate use of PII; least appropriate. Your choices are: A law enforcement agent using a person's driver's license to look up their criminal history;
Using a facial scanner to log into a smartphone;

Storing PII data on unencrypted laptops; or
Using PII to help users reset a password?
The third one. The third one, storing PII data on unencrypted laptops. Yeah, absolutely, in other words if they're unencrypted and that's kind of an interesting phrase on encrypted laptops.
but clearly we mean you know a lack of say hold disk or full disk encryption or file system encryption So if I'm storing credit card numbers Social Security Numbers other information that is personally identifiable to anyone then

that is absolutely the least appropriate because it's in an unencrypted or plain text format and that means anybody who has access to the machine or who gets into it is going to be able to see that and use that information.

Facial scanners? I'm sure many of you use if you're running a Windows operating system you may use Windows Hello or maybe just in your smartphone, you know when you push the button and it scans your face and logs you in that way that's appropriate law enforcement agent using a person's driver's license to look up their criminal history. If they've been stopped and hopefully for reasonable purposes then that's within their purview to look up and see if someone they've pulled over for some violation has a criminal history. Helping users reset a password. Sure. But number three is the correct answer in this question. Okay, let's move on.

Data Types (3) the question is: PHI data is blank. So once again our old friends the acronyms. PHI data is: Not very sensitive because it can be changed; Extremely sensitive but can be changed; Not very sensitive but it cannot be changed; or Extremely sensitive because it cannot be changed.

So this is kind of one of those wordsmithing problems. The way the answer choices are worded but the key to this question of course is knowing what PHI stands for so what does PHI stand for?

Is that personal or protected health information? It absolutely is Protected Health Information. So now we get to read the choices again. Now this question…
remember what I said earlier that when I take certification exams that I always have this habit of reading a question at least twice and there's a lot of good reasons for that especially someone say in my position who's been doing this for so long - believe it or not - you know sometimes I see something and I just want to jump right at it because I know that I've got the correct answer.

And yeah maybe I do maybe. Test makers test creators are very good at making
you think that so my habit of course is to read the question at least twice in this instance this is where you're going to read the possible answers twice because there's not much of a question now once you know that PHI is protected health

information now you have to go through the answers again and see you know is there anything that can be obviously discounted or is there something that sticks out as making good sense to you So we're talking about health information now probably at this point we've all experienced having to go to the doctor okay for something and of course they have your medical records or your protected health information on file.

Keeping that in mind, now read the choices: Is it Not very sensitive because it can be changed?
What do you think about that answer? That's incorrect. Yeah, and what about it really hits you as that is completely wrong?
The not sensitive part? Yeah, absolutely.
Because you know my my health information is very sensitive and there are only certain people or professional or professional organizations that I want to have it. So when I see "not very sensitive," I'm almost I don't even care really what comes after that because I know it's very sensitive, okay
Well in this context now they're saying the only other two choices are extremely sensitive and I'm gonna go with that I don't have heartburn with that at all it's extremely sensitive.

So now we have to read the rest of the phrase: "extremely sensitive but can be changed" or "extremely sensitive because it cannot be changed" which of those two do you think is correct?
Extremely sensitive but it can be changed?
Okay, so when you go to the doctor and they they have to pull up your medical records because you know it gives them a baseline of how you were say a year ago. Let's say it's a yearly checkup or something and they need this reference point.

But you said it can be changed.

What does that mean?

Your health can change, the status of your health can change? Okay, and so let me ask you this then:

And I agree with that yes the status of your health can change hopefully for the better.

So when that happens, where does that go in your medical record?

Does it go in the end of the record that's from a year ago or the end of the record that is today?

I'd say the more recent/ Yes, more recent. So it's appended to your medical record.

Now you can look at that… it can be changed right because we've added new information that's the whole record.

But the past, the pre-existing record,
cannot be changed because if it is changed then your health care provider may get the wrong information or have a wrong picture of your health. Do you see what I'm getting at here? So it really is extremely sensitive because
it cannot be changed; in other words, the Integrity
of your health record needs to stay intact
so that the doctors know exactly where your
health is coming from and then they can better
determine if the changes they're seeing now
are good changes or maybe not-so-good changes,
it definitely makes a difference and that's
why the answer is extremely sensitive because

it cannot be changed. Okay, does this make sense to everyone? Let’s move on right now:

Data Types (4): Which one of the
following is considered proprietary data?

Your choices are: Password; Company statistics;
Brainstorming notes or; Manufacturing processes

262
Anybody want to take a stab at this one? Passwords.

Okay so password is proprietary data. Why? Because that's like the key to having access to information and the system. Okay, so I would agree that it’s private data.
Can it be changed? Yes, and typically it can be changed without
being detrimental to your well-being or
well-being of something that you own?
Yes it can be changed.
All right, so not really proprietary
data. What about company statistics?
00:39:03.480 --> 00:39:09.900
Can't be changed? That's an excellent question so
company statistics so, for example, you know
companies put out annual reports which talk
about their financial positions and maybe
there's legal Information as well and if
it took place in the past it cannot be changed
should not be changed but it's a proprietary,
in other words, if the company statistics were to
make it into public hands would it be detrimental
to the company? The answer is the last one; the way you kind of described it it would be

the manufacturing process. Very good. That is that is correct; a manufacturing process is definitely proprietary data. It is something that
had to be perhaps researched or a company had to
find a particular expert in a particular field;
it had to be developed, created, and possibly then
used to create some type of product and in order
for this company to maintain its competitive edge
we would not want the
manufacturing process information
to get out. It would be proprietary
it would be like a company secret.

So yes the answer to this question is definitely
manufacturing processes. Let’s move on.

Okay so this one involves the
IEEE 802.1X standard.

The question: What best describes the
purpose of the IEEE 802.1x standard?

Your choices are: Sending data over a wireless
connection once it has been encrypted;

Gaining access to a network
based on an eight-digit PIN;
A secure way to support various authentication
methods like smart cards, certificates, fingerprint
scanners, and one-time passwords; or Not
activating a Network's Port until the
switch has authenticated the connected
device? Okay, so what do you think here:
And clearly this involves
understanding what 802.1x is.

Does anybody know? I don't
off the bat what 802.1x is?

Okay, so if you don't know that and and let's just say that
yeah you really do but maybe you're in the exam
and you kind of get rattled right or your your
mind has wandered or you're in a testing room
and you know someone you know three
computers down from you is busy banging out an
essay or something and the the noise of the keys is just distracting me,
when you finally refocus
and you look at this information especially
the responses your choices are: sending data
once it's been encrypted;
gaining access,
a secure way to support authentication methods; or
not activating a network's port until a device
has been authenticated? Okay, given those four

choices, which one of those is not like the others?

Someone take a guess which one is not like the others.

Yes, sending data. Okay the other three choices - gaining access to a network;
authenticating; and again authenticating a connected device - so
there's a good chance that we can eliminate the
first answer choice. Okay, now of course, you're
going to study, you're going to prepare before
you take the exam. once you've calmed down from
or gotten over whatever has distracted you
and you've looked at the question in the context
like we just did. You're now down to three choices:
Gaining access to a network based on
an eight digit PIN - that's the qualifier.
The first thought is gaining access to a network.

In the next response a secure way
to support various authentication
methods like smart cards, certificates.
Again, things that help you gain access.
Or the fourth answer: not authenticating or not activating the network's port until the
switch authenticates the connected device. That's
just another way of authenticating something.
So these things might start making it come
back to you when you realize what they're saying.

Hopefully you'll remember that 802.1X is a IEEE
standard for port-based network access control.

So right off the bat we're looking at
network access and we're looking at authentication.

I'm not sure anybody can probably recall
network access being based on an eight-digit PIN.

I'm sitting here thinking
about it and and I can't. However,
smart cards, certificates, fingerprint scanners,
one-time passwords: those things make sense.
But it also makes sense about authenticating
a connected device. We are talking

about network access. In fact that's what the
standard says: port-based network access control.
If you can recall that, then the thing that begins
to become clear is that connected devices are
connected to switches via ports. And the choice "Not activating a network's port until the switch

has authenticated the connected device" is correct.

The bit that we've just gone through
is kind of an example of using the information
there and hopefully some of the information
that you prepared for but you know maybe
you've forgotten it a little bit or maybe it's one
of your weaker points. Just being
able to look at it and choose the right answer
after reading through it and spending a little
time, you may be able to derive the correct answer.

It's another test taking strategy. The thing
is it typically has to happen fairly quickly.

One other thing to consider in
taking certification exams is that
you have a bank of time because they're all timed and you'll know up
front before you go into
it how much time you have and so if
you have - let's say you have you know
90 questions and maybe you have 90 minutes to
take the exam so that's a minute per question.

But there will be questions that you come across
that perhaps are knowledge based and things that
you know really well; for some reason they were
just really easy to learn or they really resonated
with me and you look at a question and even you'll
read it twice right you'll know the answer and in
15 seconds or so you're done you've answered
the question successfully and you've moved on.

The way to think about that is it's great
that you can answer in 15 seconds but now
you have 45 more seconds back in the bank
okay and the more this happen the more time
- sort of extra time - you have in the bank, the
less you have to worry when you come to a
question (perhaps like this one) where it takes you
a minute or a minute and a half to read through
and derive an answer. So what I'm telling
you is that the things you know really well
can serve you well when you're working on the
questions that for one reason or another you

may not know well or maybe not at this moment.
Let's move on to the next one.
Okay

This one involves ISO standards: An organization
observes ISO standards 27017 and 27018. What kind
of security standards is this organization
reviewing? And this is one of those situations
where you just have to know the standard.
Does anybody have an idea for this one

Or want to take a guess?

Amina? Go ahead just
throw a guess out there.
The fourth one? Legal liability factors?No. Okay, these
standards involve cloud security. All right, and and you simply just have
to know
that 27017 certification demonstrates
cloud service security to users
and 27018 ensures that personal data is processed
securely. This is a straight-up knowledge-based
kind of question because you're given two
standards, you're asked what kind of security
basically are these standards involving and
then you're just given choices straight out.
So this is one of those that you come across
and you either know it and you answer it
or you look at it and maybe you try to think
and remember you know you should study your
ISO standards or you didn't and you guess
and then you move on. If you know for a fact you
don't know this okay maybe it got missed
you take your best guess and you move on.

We're still good here.

We’re gonna go to the next question here.

NIST framework - so the question is: Where
the _____ focuses on practical cybersecurity
for businesses, the _____ is more prescriptive and
principally intended for use by federal agencies.

So you're given answer pairs: CIS/CIA; CSF/CIA; CIS/RMF; CSF/RMF.

Acronyms - God alone. So this question depends fairly
heavily on you knowing what the acronyms are but
you also get the clue in the question. One of these
in the first part of the pair focuses on practical
cyber security for businesses; the second one
in the pairs suggested is prescriptive and
principally intended for use by federal agencies. Anybody have a
selection for this question?

Or want to take a guess? CIS/CIA?

Okay, no, that is not correct.

CIS stands for Center for Internet Security;

CIA is the fundamental goals of information
security which are what? Anybody know? Basic stuff.

Okay, I'll give you a hint: The
first one is confidentiality.

I is what?

okay so it's Integrity and the last
one is Availability. The correct answer
is the last answer: CSF being Cyber Cecurity
Framework and it was initially developed
for critical infrastructure and RMF
stands for Risk Management Framework.

It's more prescriptive and it was designed
with the federal government in mind originally.

So a few facts there that you have to know and
also knowing the acronyms and I can't say it
enough: Like 'em, love 'em, hate 'em. Acronyms are
everywhere. Let's get in another one
Let's see here where are.

Your organization requires you to change
your password every 180 days as well as ensure
that the passwords cannot be changed more than
once within a 180-day interval. You want to match
your organization's configuration settings with
your personal configuration settings so everything
is organized. Which of the following should you
configure to match your organization settings?
So your choices are: Maximum password age; Password
history; Password reviews or; Minimum password age.

When you look at this question
the important information is here:

Your organization requires you to change your
password every 180 days and here: Ensure that
the passwords cannot be changed more than once
within a 180-day interval. What do you think
we're talking about: Is it maximum password
age, history, reuse, or minimum password age?

Minimum password age? Minimum password age - that
is correct. How did you come to that? It's like
the minimum is 180 days, right? Yes you have to have
it that, you can't change it before that time.
What do you think is the purpose
of doing this - setting a minimum password age?
And it makes sense because a lot of people
would do it if they could get away with it.

Please, go ahead. Where people keep
changing their password and like every few,

every - what was it - every so often so they can get to a password that they want? I don't know if that’s. Yeah, that’s definitely heading in the right direction. People would revert to their old passwords that maybe they're comfortable with after an enforced password change.
But if you have a minimum password age, once you change it it has to stay for that 180-day interval.

So it's a best practice and it's also you should know used often very often with password history and what that does is it keeps users from reverting back to, say, a list of old passwords. Maybe the list is five passwords long or maybe it's time based.