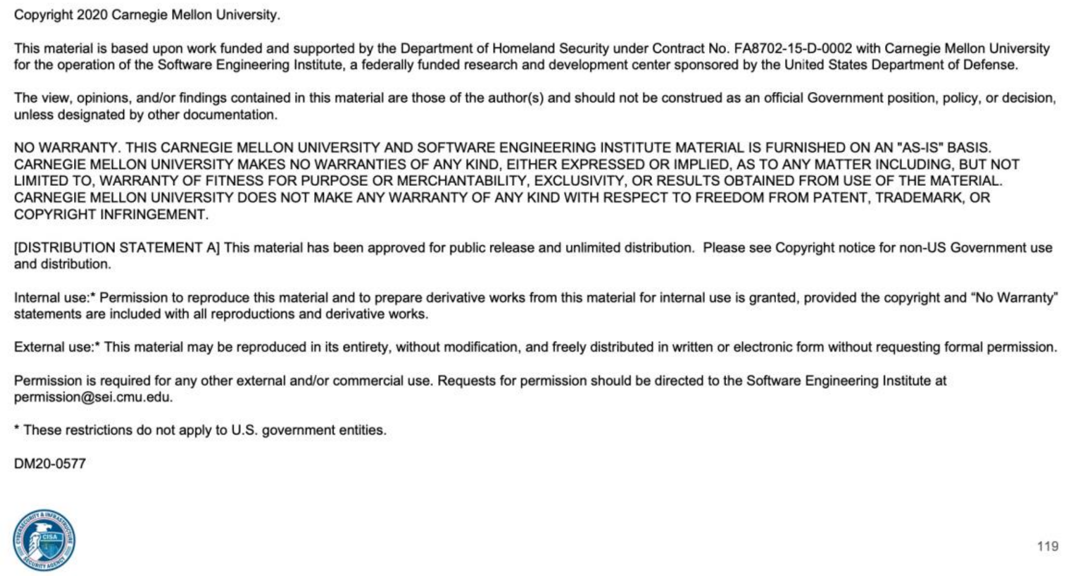
Cloud Computing Risk Assessment by ENISA

Demo



Instructor: In this video we're going to take a look at the cloud computing risk assessment done by ENISA, the European Network and Information Security Agency. This document is not just for the European Union. It does a good job of evaluating cloud technologies and risks, comes up with some recommendations, including legal and research, among others, identifies top security benefits and security risks.

The magic is really when we get to Section 2 of the document, where we talk about risk assessment, and then give you a nice introduction to the risk assessment process, where you can identify various incidents and specifically the likelihood from very low to very high of that incident occurring, and what the business impact of that would be from, again, very low to very high. From there, they are cross-referenced on this table to develop a quantitative score, and then you can see they'll be based off of a value of 0 to 2, they're low risk, 3 to 5 would be medium, and your high risks are 6 to 8.

First one we're going to look in is Risk 1, Lock-in. Probability is high, as you're looking to Azure or Amazon Web Services or Google Cloud. You're going to develop a area of expertise understanding the system, the tools, et cetera, and once you have that time investment and you've got your services up and running in there, you're pretty sure to keep continuing to grow using that provider. If that provider then develops some proprietary technologies or capabilities, then maybe not transitioning well to another provider, you're kind of stuck there.

The big three probably aren't going away any time soon, but if you re using a different cloud provider, it does somehow go away for some catastrophic reason, then you risk the loss of service delivery or potentially sensitive data. So you could see that the probability of lock-in is high, the impact if they do go away is medium. You could probably still recover your services, depending on, again, how you've architected for failure. But overall the risk is high of lock-in.

If we return to our Probability and Impact graph, one of the neat things about this resource is that we can click on one of these risks and jump over to it. So if we look at loss of governance, that's another one that we consider high risk overall, has a score associated with it. We'll see how that score's calculated in just a bit, but we have a probability of loss of governance being very high. Generally that has a lot to do with our shared responsibility model and not understanding exactly what the roles and responsibilities of that cloud service provider may be versus you and your organization.

Also unclear asset ownership, where some of those assets, infrastructure and servers that your services are running on belong to somebody else. So understanding clearly who owns what assets might be a little confusing. Certainly you own the data, but how is that data protected, stored, et cetera? And in the affected assets, again, there is risk of service delivery, customer trust and reputation if you fail to deliver those services, loss of data, that type of thing. We can even click on some of the assets or the vulnerabilities and go to that area of the document as well.

So we'll click on Service Delivery, Realtime Services, and this is really neat. It jumps us over here to the document where we have identified what that means. So Asset 9, Service Delivery, Realtime Services, all those services are time critical and need to be up nearly a hundred percent of the time, and this Very High corresponds to this column heading over here, the Perceived Value. So in your own environment, you can adjust your value of these particular things. Company Reputation might not be very high to you. Maybe it's just high or medium, you know, whereas Service Delivery would be very high consistently across the board.

So this is just a framework, again, based off of your organization. You have to go through something like this and figure out whether intellectual property is high for you, low, et cetera. But this gives you a good baseline or reference point for developing your risk assessment.

And now, going from our regulation and compliance risks, we see some technical risks, like resource exhaustion, and one of the interesting parts here is we have a different in--a difference in probability, so depending on how you've configured your resources, you might have a probability of medium or low. So if you have a highly provisioned instance and maybe you're not even close to capacity, then the probability of resource exhaustion would be low. But if you've under-provisioned and you're trying to run lean and conserve costs, maybe there is a greater chance of exhaustion of your resources.

Let's go to the next page, and this allow us to continue with that assessment. You can see the different vulnerabilities that we might have, like I said, inadequate resource provisioning might be one, and again you risk disruption service delivery, and/or we have a medium risk.

Let's look at one more technical vulnerability. Or I should say technical risk. The probability of isolation failure in a private cloud is low. You're dealing with your own private instance, either your data center or dedicated facility or resources for you, so there's low risk of bleed-over from another tenant or customer. But in a multi-tenant environment, in a public cloud solution, that probability has a greater chance of occurring. So the impact if that does happen is very high. That means that a potential threat actor or another customer could then access your resources, your information, et cetera, by taking advantage of something like a hypervisor vulnerability, and again, these are clickable. So if we click on A5 here, we have a bunch of information about this particular vulnerability and how it might apply in a cloud environment and how it would expose your organization potentially.

So returning to isolation failure, we can drive on here. We see a couple of other things, considerations in a technical area, such as malicious insider or management interface compromise, and then again you can drill through these and see the different risks that they have associated with technical controls, governance risks, et cetera, how they have them broken down, and then once we get through the risks that are identified, the subsequent chapters are vulnerabilities, as we saw, and assets, as we also saw an example of, and then you get into details for recommendations and key messages.

So again, a very good document, a very comprehensive document regarding cloud computing and doing a risk assessment of a cloud computing architecture and various technologies.