Alexis Kennedy: My name is Alexis Kennedy and I am a manager in the cybersecurity practice here at Plante Moran. My work in the cybersecurity practice consists primarily of security compliance engagements, and today I want to talk a little bit about the HITRUST Common Security Framework, or HITRUST CSF.

So what is the HITRUST CSF? If you're in the healthcare industry or deal with protected healthcare information, you have probably head the terms "HITRUST CSF" and "HITRUST Certified" thrown around, so let's define it a little better for you. The HITRUST CSF is a security framework developed by the HITRUST Alliance and other healthcare industry leaders. The framework was designed specifically for healthcare organizations. It is risk-based, scalable, prescriptive, and of course, certifiable. It was developed to address the many security and regulatory challenges facing the healthcare industry.

At its core, it takes the gray, non-prescriptive HIPAA security regulation, and maps out specific requirements necessary to be in compliance with the HIPAA Security Rule. Today, there is not a way to state that your organization is HIPAA-certified. A certifying body does not exist to do this. The HITRUST Alliance created the HITRUST CSF to showcase compliance with the HIPAA Security Rule through a common framework that can be certified.

As mentioned before, the framework is scalable and risk-based. What that means is that it takes into consideration specific risk factors to generate an appropriate control baseline for your organization. This ensures a one-location healthcare data center doesn't have to comply with all the same requirement statements as a 10-location healthcare system.

Generally speaking, a typical framework that has been scoped to your organization's specific risk factors will include anywhere from 120 to 350 requirement statements that your organization will have to show compliance with. Once your applicable framework is established, you can begin the process of becoming HITRUST certified.

At a high level, organizations will undergo, first, a self-assessment, which allows you to do just that: assess your controls against the HITRUST CSF and identify any gaps or improvements necessary. After that exercise you would move forward with a validated assessment, at which point you would hire a certified assessor firm to come audit your controls against your instance of the HITRUST CSF. Once the audit is complete, you will be issued a validated report. If the audit is complete and all certification requirements are met, you will also be issued certification. Certification is valid for two years, and an interim assessment must be conducted on the one-year anniversary of that certification to maintain that certification through the two years.

Now let's take a step back and identify why an organization would undergo this process. After all, as with any compliance initiative, it takes time, money, and employee resources, so let's answer why. There are a few reasons. One, your customers are requiring it of you. It is becoming a cost of doing business. New contracts are coming in the door, you're signing on new customers, and within that contract they're requiring you to become HITRUST certified or maintain a certification. Two, you want to showcase your organization's compliance with the HIPAA Security Rule, or three, you just want a competitive advantage and a marketing tool. Information security has been an increased focus when choosing third parties to work with, so being able to prove you are a HITRUST certified firm can give you a leg up in the sales process.

Whatever your reason may be for this initiative, you should understand that it is an undertaking, and choosing the correct partner to navigate through this process is key to your success. We are a certified assessor firm with four certified practitioners on staff. We have years of experience in security compliance, and when working with us you get full access to our extensive cybersecurity practice. To learn more about how we can help you navigate through the HITRUST certification process, please feel free to reach out to me directly, or you can find us at plantemoran.com by visiting our cybersecurity page.