Committee	Parliamentary Joint Committee on Corporations and Financial Services
Inquiry	Oversight of ASIC, the Takeover Panel and the Corporations Legislation
Question No.	052
Topic	Cybersecurity
Reference	Spoken, 3 November 2023, Hansard page 7
Committee member	Senator Deborah O'Neill

Question

CHAIR: That's a very significant role with incredible levels of responsibility and profound impact. One of the reasons we have professional organisations, professional association registration and licensing processes is that the power differential between those who know and those who don't can lead to very inadvertent outcomes for the one who knows the least in that equation. Are CISOs professionalised in any way? What qualifications are required? What assessments are ongoing to assure that these people are fit and proper for the role?
Mr Day: I'm pretty confident in terms of the processes we take to assess the candidates we've got for roles. In terms of the broader professional accreditation et cetera, I'd have to take it on notice.

Answer

There is no centralised professional accreditation process in Australia for CISOs, nor other cyber security professionals. Similarly, there is no one security qualification that an individual must have to be considered for a CISO role. Instead, and in common with how organisations select candidates for other senior executive roles, it would be each organisation's responsibility to assess an individual for a CISO role on their technical and business acumen, together with their leadership, communication, and stakeholder engagement expertise.

To assist with this assessment process, there are industry bodies for security practitioners and common security certifications. These organisations include international cybersecurity professional certification bodies such as (ISC)^2 and ISACA and nationally, there is the Australian Information Security Association (AISA). AISA is a peak body for cyber security professionals in Australia that works to build the knowledge and capacity of professionals in the local cyber security industry, including the most senior security practitioners such as CISOs.

In addition, there are Graduate and Masters level degree programs from Australian and overseas universities that provide in-depth training in information and cyber security, that ensure that an individual has a solid foundation of security expertise across multiple security domains, as well as broader critical-thinking skills. Considering the security industry certifications, individuals are required to have a minimum number of years of experience in the security industry before they are eligible to be awarded the certification; and upon receipt of the certification, they are required to undertake continuing professional development to maintain their certification(s). This provides a level of assurance that individuals holding industry certifications have a minimum level of relevant security industry experience and are maintaining the currency of their skills.