PCM THE RIGHT TECHNOLOGY, DELIVERED™

New York State DFS 23 NY CRR 500
CISO DESIGNATION REQUIREMENTS

A Virtual CISO is a cost-effective approach to manage critical compliance and security programs.

The cyber security requirements set forth by New York's Department of Financial Services require banks, insurance companies and other covered entities to designate a **Chief Information Security Officer (CISO)**, either an employee or a virtual CISO or consultant acting in that capacity.

What are the right knowledge and skills needed when hiring a CISO? **Dallas Bishoff**, PCM Director of Security Services, offers the following recommendations, based on over 40 years of experience including, acting as a virtual CISO for several companies. These questions apply to anyone acting in a CISO capacity, either full-time or as an external consultant serving as a "virtual" CISO.

1. Does the CISO have subject matter experience in your vertical sector?
2. Does the CISO have knowledge of cyber, data breach, and non-compliance insurance coverage commensurate with an organization's risk profile?
3. Does the CISO have a strong IT infrastructure background coupled with regulatory security control requirements needed throughout the IT infrastructure footprint?
4. Does the CISO have experience conducting and performing security risk assessments?
5. Does the CISO have experience in developing risk profiles, security baseline definitions, and performing gap analyses for regulatory compliance?
6. Does the CISO know the various federal, state, and if applicable, international requirements for compliance, security, and privacy, such that a proper compliance strategy and compliance management plan can be developed?
7. Does the CISO have the ability to communicate compliance, security, and privacy business challenges into simple and easy-to-understand translations for executive governance decisions?
8. Does the CISO have experience in developing executive leadership and board presentations on compliance, security and privacy?
9. Does the CISO know how to position compliance, security, and privacy gaps, and utilize data to obtain proper funding approvals from the executive leadership and board?
10. Does the CISO have experience in working collaboratively with legal/general counsel, CFO, CIO, HR, and board-level governance discussions?

If you have company-specific questions regarding the role, qualifications and expectations in appointing a CISO or virtual CISO, we are happy to provide a free consultation. Contact **pcmsecurity@pcm.com**