Deloitte.

The First Year

For a new CISO, the first year is critical in establishing credibility, formulating strategy, and demonstrating business value. Although CISOs should tailor the below to their own needs and organizational context, our timeline offers a good starting point.

0-30 Days

- Connect with key stakeholders, direct reports, and one level down to establish a preliminary understanding of what needs immediate attention and how to operate in the organization.

30-90 Days

- Continue conversations with stakeholders to define starting priorities and develop an initial plan.
- Complete a talent assessment and new organization model.
- Assess the capabilities of direct reports and other staff to understand talent needs and appropriate structure.
- Decide which projects can be discarded or deferred to free up resources for priority initiatives.
- Conduct an audit of meetings to reduce the number of them or ensure they are effective (with objectives, agendas, outcomes, and actions).

90-180 Days

- Deliver initial projects and quick wins.
- Complete restructuring of the CISO organization.
- Conduct strategic and functional reviews to assess security strengths and weaknesses.
- Review the organizational structure and determine if the risk management function and team are aligned to the organization's strategic plans.
- Work with enterprise risk management to reassess the risk appetite framework vis-à-vis the organization's cyber risks.

180-365 Days

- Define a strong three-year security strategy and roadmap to enable the business.
- Finish establishing the new organizational and governance models for security oversight.
- Learn how to delegate in your new role. Determine how to prioritize the workload, then empower team members to assume greater levels of responsibility.