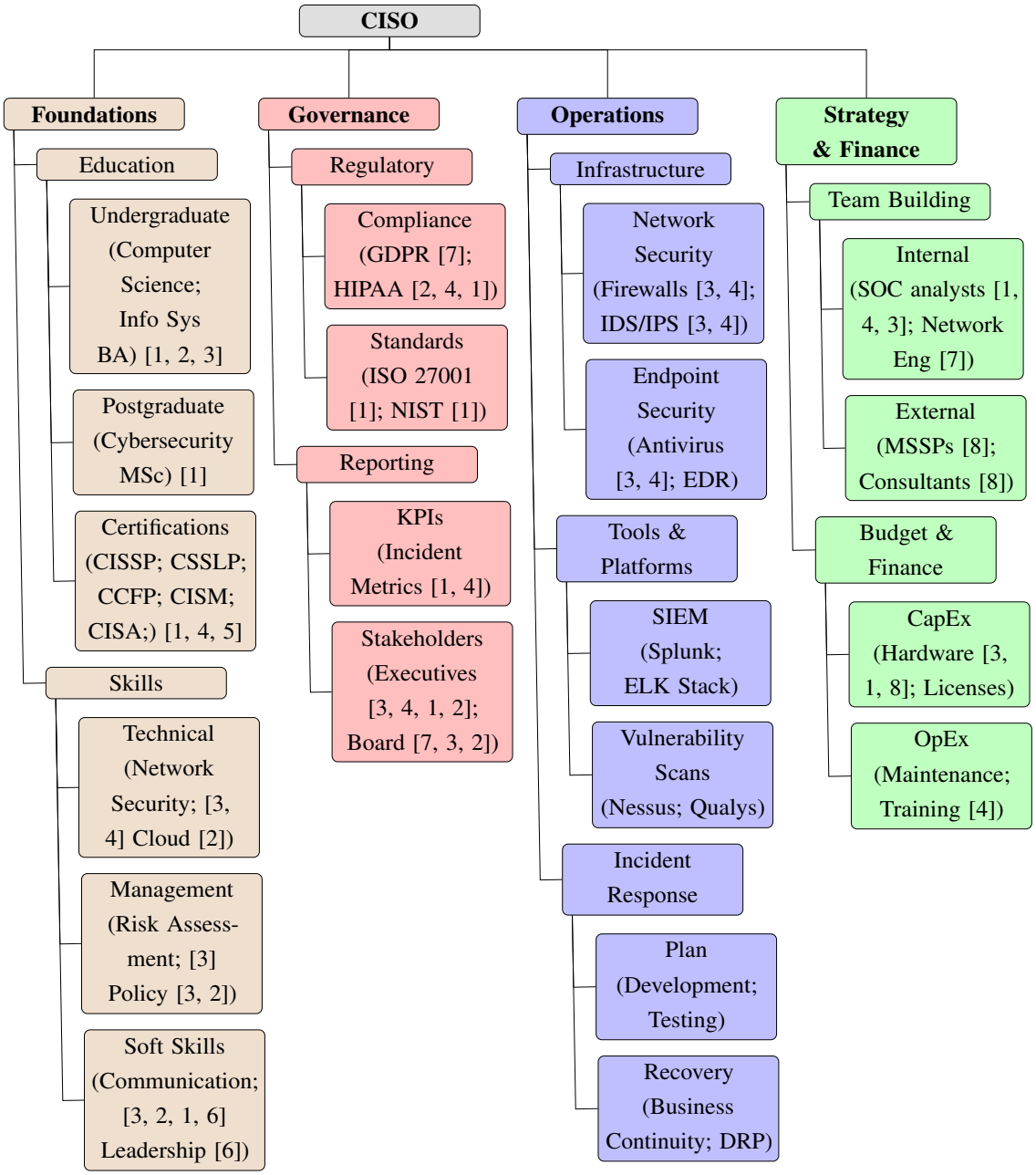
TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Joosep Parts 221963IVCM 14.09.2023

HOMEWORK 1: CISO ROADMAP

Cyber Security Management (ITC8230)

Tallinn 2023



Chief information security officer(CISO), also known as chief security officer(CSO), is the executive responsible for an organization's information and data security. The CISO directs staff in identifying, developing, implementing, and maintaining processes across the enterprise to reduce information and information technology(IT) risks [1, pp. 587–588]. CISO is bridge the between the executive team and the IT department who must be able to sense what real risks are and plan accordingly [4, p. 261]. To be successful, CISO must have a broad range of both soft and hard skills and be able to communicate effectively with both technical and non-technical audiences.

Foundations: The foundational aspects of the CISO role, comprising key educational and skill-based competencies. Fundamental to understanding cybersecurity theories and

technologies. A bachelor's degree forms the groundwork for specialized knowledge. As there are little cybersecurity bachelor's programs, a computer science or information systems degree is a good starting point. Advanced studies provide a deeper understanding of cybersecurity. Proof of expertise is often required for senior roles, that's why having some certifications is a requirement. A versatile skill set is crucial, both technical skills and soft skills. CISO should not do everything by himself, rather delegate tasks. For that he nees necessary skills for leading teams and influencing stakeholders.

Governance: Governing policies and compliance to avoid risks. Ensures compliance with laws and regulations like GDPR and HIPAA. Compliance frameworks that have legal implications. Setting the guidelines and best practices is critical for organizational transparency. Monitors key metrics to measure security performance and regulary updates information to executive's for strategic alignment.

Operations: Day-to-day management of security operations. This core skill is key in defending against cyber threats. There are tools which can help in intrusion detection and prevention. A CISO must be familiar with these tools. I don't mean the CISO himself must be scrolling through logs, but he must be able to understand the data if presented to him to make decisions based off it. Plans and actions for security incidents. Implements a well-thought-out strategy for incident management and plans for resuming normal operations post-incident. CISO must be familiar with all the IR steps including dedection and containment, however I do feel that CISO's role during that phase is mostly coordination between different teams and stakeholders. It is however CISO's responsibility to ensure that the organization has a well-thought-out IR plan and how to recover from it.

Strategy & Finance: Deals with long-term planning and resourcing. Investments in long-term assets and keeps an eye on day-to-day expenses that need to be managed efficiently. Creates teams / departments who can amplify a CISO's effectiveness. Such as in-house staff specialized in different areas. External expertise for specialized tasks might be required from the CISO, e.g.: when the company CISO works for is a service provider and clients must be informed. Or just public relations in general, disclosing a breach to the public and media.

There appears to be no consensus on the exact skills and knowledge required for a CISO [5]. The role is still evolving and the CISO's responsibilities are expanding.

References

[1] Val Hooper and Jeremy McKissack. "The emerging role of the CISO". In: *Business Horizons* 59.6 (2016). CYBERSECURITY IN 2016: PEOPLE, TECHNOLOGY, AND PROCESSES, pp. 585–591. ISSN: 0007-6813. DOI: https://doi.org/10.1016/j.bushor.2016.07.004. URL: https://www.sciencedirect.com/science/article/pii/S0007681316300635.

[2] Erastus Karanja. "The role of the chief information security officer in the management of IT security". In: *Information & Computer Security* 25.3 (Jan. 2017), pp. 300–329. ISSN: 2056-4961. DOI: 10.1108/ICS-02-2016-0013. URL: https://doi.org/10.1108/ICS-02-2016-0013.

[3] Dwayne Whitten. "The Chief Information Security Officer: An Analysis of the Skills Required for Success". In: *Journal of Computer Information Systems* 48.3 (2008), pp. 15–19. DOI: 10.1080/08874417.2008.11646017. eprint: https://www.tandfonline.com/doi/pdf/10.1080/08874417.2008.11646017. URL: https://www.tandfonline.com/doi/abs/10.1080/08874417.2008.11646017.

[4] Todd Fitzgerald CISSP, CISA, and CISM. "Clarifying the Roles of Information Security: 13 Questions the CEO, CIO, and CISO Must Ask Each Other". In: *Information Systems Security* 16.5 (2007), pp. 257–263. DOI: 10.1080/10658980701746577.

[5] Sylvester Cotton. "Experience and Qualifications Required for a Chief Information Security Officer: An e-Delphi Study". English. Copyright - Database copyright ProQuest LLC; ProQuest does not claim copyright in the individual underlying works; Last updated - 2023-03-08. PhD thesis. 2022, p. 142. ISBN: 9798351430911. URL: https://www.proquest.com/dissertations-theses/experience-qualifications-required-chief/docview/2725631467/se-2.

[6] Joseph Da Silva. "Teacher, enforcer, soothsayer, scapegoat: the purpose of the CISO in commercial organisations". English. PhD thesis. Royal Holloway, University of London, 2023.

[7] Pedro Monzelo and Sérgio Nunes. "The Role of the Chief Information Security Officer (CISO) in Organizations". In: (2019).

[8] Khalid Kark et al. "Market overview: Managed security services". In: *Report, Forrester Research, Cambridge, MA* (2010).