50 CRITICAL QUESTIONS TO ASK
ABOUT DIGITALIZATION

This annex features a series of questions that directors may ask in support of their digital leadership roles. We encourage directors to adapt the questions to the context of their specific organizations, (e.g., the size, industry, etc.).

Advice and counsel

Offering advice and counsel to the executive management based on experience and expertise.

Digital maturity of the organization

1. Have you got a sense of the digital maturity of your organization and capabilities?
    a. Is there a framework in place that measures the maturity, allows to prioritize the digital initiatives with the biggest business impact and measure progress?
    b. What trade-offs did you make in prioritizing?

2. What is the digital savviness of your functional leaders?
    a. Do they well understand what the technology trends are in their specific domain, back and front office?
    b. What is their appetite to digitize the company?
    c. How do you inspire them?
    d. How do you build the required digital expertise in the business?

3. Can we get a view on the enterprise architecture? (Importance often underestimated, it gives a clear view on business/IT connection in the long run, and gives an indication on the complexity of the platforms and solutions, and thus, a base, or not, for future investment)

4. What are your biggest business pain points, and have you thought to apply technology to get insights (link to truly data-driven organization) or solve the problem?

Talent - People

5. What are the engagement scores of the IT Team, the core engineering teams more specifically?
    a. What is attrition rate?
    b. How do you attract, develop and retain IT talent, in general, and more specifically for the new technologies?
    c. Given the war for talent, do you have a plan to reskill resources to be ready for the future?

Cloud

6. Do we have a cloud strategy on 3-5 years? What is our cloud strategy?
7. Do we realize cloud is an enabler?
8. Do we have a view on the financial impact?
    a. Move from CAPEX to OPEX
    b. Do we pay enough attention to the impact of the changing cost structures/need to monitor the use to avoid to pay for non-used capacity/licenses?
9. Do we invest in the appropriate knowledge?
10. Is our IT infrastructure robust enough?
11. Cloud changes the approach of cyber security. Are the right operational processes in place?

Data

12. Do we have a data strategy and roadmap?
13. Are employees sufficiently sensitized about the importance of data?

Networking, lobbying, legitimating and communication

Acting as boundary spanners of the organizations and the environment, providing access to resources, lobbying, legitimating and communicating.

14. Do we know the regulatory barriers for our digital strategy and do we bring them to the right channels?

Strategic participation

Active involvement in strategic decision making, i.e., initiating strategic analysis, strategy formulation and strategy implementation.

Challenges/opportunities from the external environment

15. Any success stories on digitization from the competitors, have they emerged, how are they threatening the business?
16. What innovative technology is likely to disrupt your current business model?

Innovation

17. Do you/does your company realize the potential of embracing digital for your business/organization?
18. Do you have the culture/an approach in place to stimulate and monitor digital innovation?
19. Is digital transformation high on the agenda? Do you have a structured approach in place? Or do you consider digital transformation as an organic process that remains unplanned?
20. Is there someone within the company who drives the digital transformation?
21. Where are most decisions taken regarding digital innovation in your business? (site, head office Belgium, head office abroad)
22. Who drives digital innovation within your business? (management, IT, business,…)
23. How high is digital innovation on the agenda of the Board of Directors?
24. Do we monitor new possibilities to see what they can bring to our organization? (e.g. blockchain, Ai, RPA, 5G,..)
25. Do we use the potential of online collaboration for the employees?

Behavioral control

Monitoring of management behavior and operational control.

Cybersecurity

26. Do you understand the cybersecurity risks towards your organization and its digital assets? What are your biggest threats right now?
27. Are we considering the cybersecurity aspects of our major business decisions, such as M&A, partnerships, new product launches, etc., in a timely fashion?
28. Do you have someone responsible in your organization for cybersecurity?
29. Does he/she have the mandate and resources available to control your cybersecurity risk to an acceptable level aligned with your business priorities?
30. What is the cybersecurity report and frequency you get as a board member? Does it meet the level of detail and assurance you require?
31. Do you have an active plan in place to attract and keep designated cybersecurity staff and/or trusted suppliers to protect your digital assets?
32. Are your employees appropriately trained on cybersecurity and privacy?
33. Are we spending appropriately on cybersecurity tools? Do we know if our spending is cost-effective? Are we actually improving security or just completing compliance requirements?

34. Do you know how to respond in a cyber security incident (as a board)?
35. Does our organization participate in any of the public or private sector ecosystem-wide cybersecurity and information-sharing organizations?
36. Does the company have adequate insurance, including Directors and Officers, that covers cyber events? What exactly is covered? Are there benefits beyond risk transfer to carrying cyber insurance?
37. Does your cybersecurity program also cover specific Operational Technology (OT) risks, such as industrial controls systems, connectect (medical) devices, cameras, IoT devices, ...

Risk management

38. Does the company make a yearly risk assessment?
39. Which important risk mitigations are not taken because of budget restrictions?
40. For the High risks, does the Board decide to accept the residual risks ?... or to ask for action and give a budget ?

Compliance

41. Do you have an overview of your compliance obligations?
42. Is the organization adequately monitoring current and potential cybersecurity and privacy related legislation and regulation?
    a. sector specific
    b. security – NIS
    c. privacy – GDPR
    d. guidelines from Data Protection Authorities
43. Is a specific person responsible for all compliance risks in the company?
44. Has the compliance officer been given enough resources to carry out the mission?
45. What is the compliance report and frequency you get as a board member? Does it meet the level of detail and assurance you require?
46. In case of a data breach, who is accountable to inform the authorities?
47. Are your employees appropriately trained on compliance?
48. What are your metrics to demonstrate your compliance management system effectiveness?

Output control

Controlling organization output with attention to all organization stakeholders.

Disclosure of security & privacy breaches

49. In case of a data breach, who is accountable to inform the authorities?
50. Have we considered how we would manage our communications in the case of a cyber event or data breach, including communicating with the public, our shareholders, our regulators, our rating agencies? Do we have segmented strategies for each of these audiences?

This practical instrument was created based on the insights offered by a team of experts part of the Fastfwd initiative.

Danielle Jacobs, CEO Beltug

Abigail Levrau, Member Mgmt Committee Guberna

Sabine Everaet, former CIO Coca-Cola EMEA

Jocelyn Darbroudi, CIO Securex

Sebastien Deleersnyder, CTO Toreon

Steven De Haes, Dean Antwerp Management School

Stefan Dierckx, CEO ProjectiveGroup