I have picked IBM for this part of the assignment. Here is a link to their 2021 proxy statement: https://www.ibm.com/annualreport/assets/downloads/IBM\_Proxy\_2021.pdf

Any large organization dealing with retail, manufacturing, healthcare, and the government is more likely to be under a cyberattack. It is no surprise that IBM was under such attack in 2019 when 8.5 billion records were leaked. IBM has been taking preventive measures to bolster Cybersecurity ever since. Investors and stakeholders are now more involved in understanding how a company deals with cybersecurity incidents. Companies can follow various guidelines and regulations to disclose their risk incidents. We are looking at the National Association of Corporate Directors (NACD) framework for this essay. It talks about the five principles boards should consider while providing oversight of cybersecurity risks.

Here is a breakdown of whether IBM follows the five principles of the NACD framework.

First, on page 9, the chart represents all the board members and their experiences. IBM advertises that all the company directors are highly skilled and equipped with Cybersecurity. This detail shows that as a vigilant company, IBM gives more significance to Cybersecurity and risks and does not treat it as just another IT issue. However, details regarding how each of these directors takes part in risk management would provide a deeper look into how Cybersecurity is treated as an enterprise-wide operation.

Similarly, page 22 states that risk management is the Board's responsibility and is expected to regularly review and update the risk management framework and procedures. The Board contains three committees - The Audit Committee, The Executive Compensation and Management Resources Committee, and The Directors and Corporate Governance Committee, each examining different elements of risk oversight. Hence, satisfying the 4th principle of the NACD framework, which mentions that adequate staffing, budget, and regular meetings are highly recommended.

Page 22 also contains parts involving clear identification and classification of various risk types, which is the core of principle five. It mentions that IBM's senior management comes into play while dealing with risk management as a day-to-day activity. They are responsible for coming up with programs and policies. IBM has an elaborate enterprise risk management framework which helps them identify which risks to avoid, which to accept, and which to mitigate. Nevertheless, it needs to capture details regarding how they plan to go about each of these identified risks and what steps need to be taken for them accordingly.

Principle 3 states that regular discussions about Cybersecurity with experts can help an organization better deal with cyber risks. IBM has appointed a Chief Information Security Officer (CISO) whose team is responsible for leading enterprise-wide information security strategy, guidelines, norms, architecture, and operations. CISO team collaborates with the Enterprise and Technology Security (ETS) organization, which works across all companies' organizations to protect IBM, its brand, and its clients against cybersecurity risks. They take regular updates from cybersecurity experts in various areas such as threat intelligence, major cyber risk areas, emerging global policies, best practices, etc.

Sadly, I could not find any relevant information regarding principle two, which indicates the director's understanding of legal implications based on the company's circumstances.

In conclusion, IBM does a modest job covering all the NACD principles. The report could have had more details regarding the people involved and the exact framework they plan to use. But then again, I also see an issue with disclosing all these details, as it may lead to potential risks due to the sensitive information shared.