endeavour vision

Part 5
UNDERSTANDING ESG AND HEALTHCARE INNOVATION:

WHY HEALTHCARE COMPANIES SHOULD CONSIDER THE GOVERNANCE DIMENSION AND HOW TO DO IT.

This is the fifth and final paper in a series in which we take investors and healthcare leaders on an ''ESG journey'': what it is, why is matters, and how to put ESG into practice.

Introduction

Stakeholder interests and requirements change over time, and it is essential that healthcare organisations and companies change with them. This cannot be done without investing in good governance – the third and final (some might also say "foundational") piece of the three ESG principles.

Part 1 of this series outlines these principles in detail. In **Part 2**, we define the reporting approach Endeavour Vision uses to support our portfolio companies with the development of ESG practices. Building on this, **Part 3** and **Part 4** go on to describe why it is essential for healthcare companies to invest in "Environmental" and "Social" strategies, with each piece offering phased recommendations to support practical implementation. In this **fifth paper**, we will move our discussion to the concept of "Governance" and provide expert insights, tools and resources to help your organisation embed the policies and processes it needs to build and sustain good governance.

Defining "Governance"

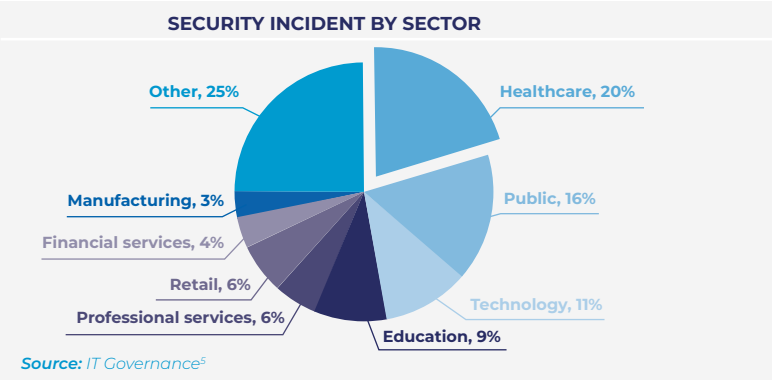
Before we can describe governance in more detail, it is first necessary to define it. It is a broad and complex concept, one that – generally speaking – is used to reference the control mechanisms (e.g. corporate structure, board composition, business ethics and anti-corruption) an organisation uses to prevent and discourage managers and/or suppliers from engaging in activities that are detrimental to the welfare of stakeholders.[1,2]

While the term can be used to cover a wide array of systems and processes, there are three emerging areas of focus that require particular attention. The first is the issue of **cybersecurity**, with the World Economic Forum identifying cybercrime and cyber insecurity as one of the top 10 short and long-term global risks (2-10 years).[3] The second relates to the impact of effective investment in r**esearch and development (R&D)**, while the third relates to organisational codes of conduct, and the due diligence and sustainability of suppliers.

Why good governance matters to the healthcare sector

As a sector, healthcare institutions and organisations hold vast amounts of highly sensitive personal information, from names and birth dates to social security numbers and private health data. This goldmine of information makes the sector extremely vulnerable to cyber-attacks. It is the role of organisational governance systems to protect it.[4]

In 2022, data shows a total of 408 million records to have been breached worldwide.[5] Of these, an estimated **20% of incidents occurred within the healthcare sector**.[5] Further to this, in 2023, the US government's Office for Civil Rights showed



1. Tayan B, Larcker D. Corporate Governance Matters: A Closer Look at Organizational Choices and Their Consequences, 1st edition, Ft Pr. **2.** World Economic Forum. Defining the 'G' in ESG Governance Factors at the Heart of Sustainable Business. https://www3.weforum.org/docs/WEF_Defining_the_G_in_ESG_2022.pdf (Accessed 15 August 2023). **3.** World Economic Forum. The Global Risks Report 2024 18th Edition. https://www.weforum.org/reports/global-risks-report-2023/ (Accessed 11 August 2023). **4.** Withpersona. Top healthcare data breach statistics of 2023. https://withpersona.com/blog/top-healthcare-data-breach-statistics-2023 (Accessed 8 August 2023) **5.** IT Governance. Data Breaches and Cyber Attacks in 2022: 408 Million Breached Records. https://www.itgovernance.co.uk/blog/data-breaches-and-cyber-attacks-in-2022-408-million-breached-records (Accessed 8 August 2023).

healthcare firms reporting 145 data breaches in the first quarter of the year. This follows a recorded 707 incidents in 2022, during which time 51.9 million records were stolen.[4]

With estimates going on to show 95% of identity theft incidents linked to compromised healthcare records,[4] the need to strengthen cybersecurity and other governance systems within healthcare organisations is clear.

In addition to the above, investment in R&D is shown to be an essential part of organisational governance. For example, a recent study showed that board characteristics are an important influencing factor on effective R&D strategic decision making.[6] The study concluded that directors of different backgrounds stimulate a firm to improve or develop new products, while older directors are less risk-tolerant than younger ones and invest less in risky R&D investments. The effect of board size on performance is negative and significant, while it has a positive and significant impact on R&D investment.[6] In light of these findings, it is reassuring to see global trends showing R&D spending to account for more than 12% of the total revenue of healthcare companies (topping the chart when compared to other industries).[7]

At a glance: our portfolio companies

Endeavour Vision is committed to helping our portfolio companies streamline and strengthen their core governance systems. As a reflection of this commitment, we are proud to see that when analysing company governance scores, **Endeavour companies scored higher – on average – than the sector benchmark**.

Further to this, all Endeavour companies are shown to invest in R&D and have data protection and privacy policies in place, with the majority having also prepared a Code of Business Conduct and whistleblower policy. Many also now list independent directors on their company board.

While these are undoubtedly results to be proud of, closer analysis does reveal **significant deviations** between companies, with average scores varying from 40% to 80%. In particular, we noticed that many of our portfolio companies were yet to conduct a cybersecurity assessment and prepare a supporting policy framework, company or supplier Code of Conduct.

GOVERNANCE	47%
ESG Strategy	
ESG Materiality Assessment	
Corporate Governance Policy	
Independent Board Members	■
Code of Business Conduct	
Whistleblowing Policy	■
Business Ethica Breach Management	■
Data Protection and Privacy Policy	■
Cybersecurity Policy	■
Cybersecurity Assessment	
Risk Management Training	
Product/Service with ESG Benefits	■
Product/Service UN SDG Alignment	■
R & D Spend 2020	■
Supplier Code of Conduct	
Sustainability Certification Procurement	
Sustainability Certification Sales	

Analysis of governance ESG factors of a company in the Endeavour Vision EMG II portfolio. Boxes highlighted in blue indicate categories for which the company provided a positive response, along with relevant supporting evidence. For this company, the overall score for "social" was 47% (8/17).

6. Johenesse E, Gusti Agung Musa Budidarma, I. Corporate Governance and R&D strategic decision making. East Asian Journal of Multidisciplinary Research (EAJMR). 2022;1(3):239-260. **7.** Statista. Percentage of spending on research and development of total revenue in 2021, by industrial sector. https://www.statista.com/statistics/270324/expenditure-on-research-and-development-by-industry-sectors/ (Accessed 9 August 2023).

Regulatory developments

A supporting pillar for the entire ESG framework, "Governance" is a hot topic for companies and regulators alike, with an overview of headline changes in the regulatory landscape given below.

CHANGES IN US REGULATIONS

In March 2022, Chairman of the **US** Securities and Exchange Commission (SEC), Gary Gensler, observed that "today, cybersecurity is an emerging risk with which public issuers increasingly must contend."[8] His observation comes amidst the **proposal and publication** of new rules that work to enhance and standardise disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting.[8,9]

Specifically, incoming regulation will require public companies to disclose any "material" cybersecurity incident and to describe the incident's nature, scope, timing, and impact.[8] Companies will also be required to describe their processes for assessing, identifying, and managing these risks, as well as the role of management and the Board of Directors* in doing so.[8] Disclosures will be due beginning with annual reports for fiscal years ending on or after December 15 2023.[8]

** Companies that wish to be listed at the Nasdaq or the New York Stock Exchange must have in place a Board of Directors of which the majority is comprised of independent directors.* [10]

EUROPEAN DEVELOPMENTS

In **Europe** there have also been regulatory developments. In March 2021, for example, the **German** government passed the Supply Chain Act, which requires large German companies to address human rights and environmental violations within their global supply chains. These organisations must monitor and act on violations both within their own operations, as well as those of their direct suppliers, regardless of whether the activity was performed in Germany or abroad.[11] This new regulation is part of a growing trend around the world to hold companies accountable for sustainable and ethical business practices within their global supply chains.[12]

8. SEC. SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies. https://www.sec.gov/news/press-release/2022-39 (Accessed 9 August 2023) **9.** SEC. SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies. https://www.sec.gov/news/press-release/2023-139 (Accessed 9 August 2023). **10.** Skadden. What Exactly Is an Independent Director? (Hint: It's More Complicated Than You Think). https://www.skadden.com/insights/publications/2022/02/the-informed-board/what-exactly-is-an-independent-director (Accessed 9 August 2023). **11.** IBM Envizi. German Supply Chain Due Diligence Act (SCDDA) explained. https://www.ibm.com/blog/german-supply-chain-due-diligence-act-scdda-explained/ (Accessed 9 August 2023). **12.** Eddine, S. The German Supply Chain Act: Navigating third-party risks through effective due diligence. https://www.refinitiv.com/perspectives/regulation-risk-compliance/the-german-supply-chain-act-navigating-third-party-risks-through-effective-due-diligence/ (Accessed 10 August 2023).

A phased approach to enhancing organisational "Governance"

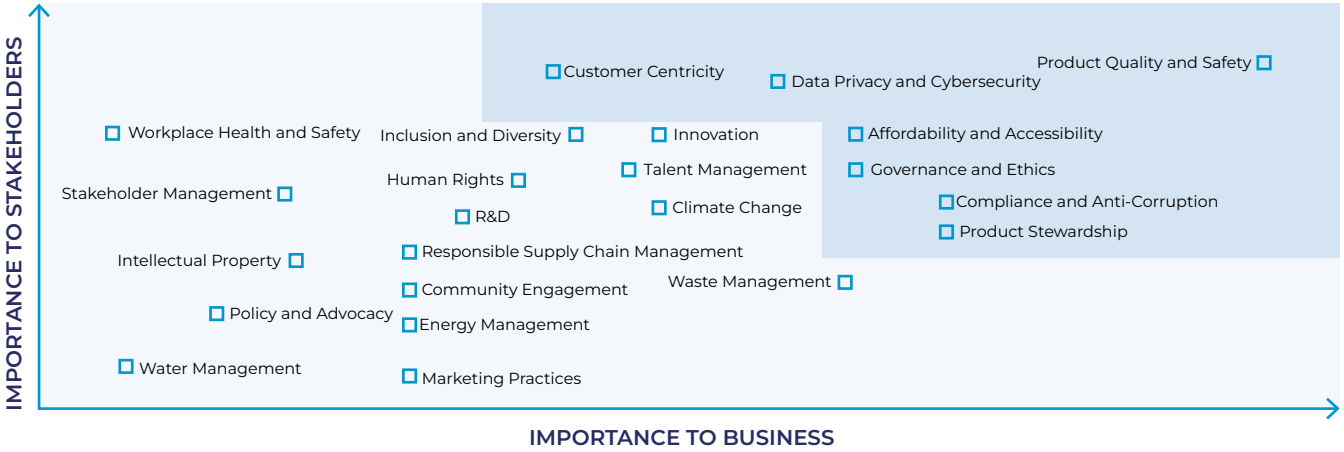
We have developed a four-phase approach for organisations looking to improve their governance agenda. This process will help your company to comply with increasing regulatory standards and cater to growing expectations for enhanced corporate governance. We continue to recommend designating a responsible person or committee within the organisation to oversee and manage this process.

1 PHASE 1:
CONDUCT AN ESG MATERIALITY ASSESSMENT

A materiality assessment is a test that allows for the understanding and prioritisation of key ESG issues, for example by implementing stakeholder views on the policies and/or procedures being developed by the company. Easily transferred to the challenge of managing multiple competing governance priorities, we recommend that all companies conduct an ESG materiality assessment to identify priority points of action.

Last year, Endeavour Vision conducted its own ESG assessment. To do this, we used GRI standard 103, the Sustainability Accounting Standards Board (SASB) and desk-based research into peer organisations to build a list of "material" topics. Next, we asked 30 internal and external stakeholders to assign an anonymous score (1-10) to each topic based on their perceived degree of importance (we also asked if there were additional topics to include). Results were analysed and mapped, with findings integrated into the overall ESG strategy, company strategy and budget.

An example of a completed assessment conducted by public medical device company Insulet Corporation, is shown below.[13]



Source: *Insulet 2022 Sustainability Report*

13. Insulet. 2022 Sustainability Report. https://www.insulet.com/sites/insulet/files/2023-05/Insulet-2022-Sustainability-Report.pdf (Accessed on 9 August 2023).

2 PHASE 2:
DEVELOP A CYBERSECURITY PLAN AND CONDUCT A CYBERSECURITY ASSESSMENT

The first step to developing a cybersecurity plan is to identify potential risks and vulnerabilities. When developing this list, it is important to remember that cybersecurity is not just about IT. It is also about people, and employees will need to be trained on how to mitigate risks, identify and report incidents, suspicious activity, and scams. Once the full list is in place, policies and procedures that systematically address each one should be prepared, together with a detailed plan on how to report and respond to breaches and incidents.

As part of the above, organisations also need to ensure that their IT network is secure. This should include the use of firewalls, intrusion detection and prevention systems, as well as anti-virus software. All cybersecurity systems should be regularly updated and tested, with data protected through encryption tools and regularly backed-up.

Tools to support the development of cybersecurity systems and processes include:

- CISA: Free cybersecurity processes and tools
- CSO: 21 best free security tools
- SANS: Security policy templates

3 PHASE 3:
PREPARE A (SUPPLIER) CODE OF CONDUCT

A Code of Conduct is key to achieving good governance, as it clearly outlines organisational norms and expectations. A non-exhaustive list of potential topics includes:

- Organisational vision, missions and values
- Anti-trust
- Bribery and gifts
- Conflict of interest
- Equal opportunities
- Grievance mechanisms and procedures
- Political activity and lobbying
- Proper record keeping

Many public companies have published their Code of Conduct online. These can be a useful starting point for early-to growth-stage organisations looking to develop their own code.

In addition to the above, we recommend that companies also look to create a Supplier Code of Conduct. The aim of this piece is to illustrate a company's commitment to sustainable and ethical business practices and to minimise supply chain risks. To do this, it is first necessary to identify all material third parties and suppliers. Once this list is in place, organisations should formalise a supplier risk assessment and management process and engage with them to promote consensus around key sustainability issues.

4 PHASE 4:
DEVELOP A GOVERNANCE POLICY

The fourth and final phase is to develop a supporting governance policy that establishes and communicates clear and consistent management structures and processes. The policy should show that the organisation is committed to acting in the best interests of its stakeholders as well as promoting personal and professional integrity and ethical behaviour. A non-exhaustive list of topics to include are:

- Board size and composition
- Directors' and Board committee responsibilities
- Directors' communications with third parties
- Directors' compensation
- Management evaluation and succession.

Conclusion

Good governance is the foundation of ESG, with cybersecurity and ethical business practices emerging as priority issues. As a sector, healthcare organisations regularly document and store sensitive peraonal information. With this comes a risk to cybersecurity, with new regulations in the United States requiring public companies to disclose more information about their risk assessment, mitigation, and management strategies concerning cybersecurity. Further to this, recent years have also seen a noted move towards enhanced due diligence with more companies (e.g. in Germany) now required to define their processes regarding the engagement, practice and sustainability of suppliers.

Recognising the importance of these headline issues, this paper outlines a four-phase approach to help early- to growth-stage organisations improve their governance. This includes a materiality assessment to identify priority development areas, as well as the preparation of a cybersecurity policy, and organisational and supplier Code of Conduct. Activities should be underpinned by a supporting governance policy that works to establish and communicate clear and consistent management structures and processes across the organisation.

About the authors

Bernard Vogel is co-founder and managing partner of Endeavour Vision. He leads the firm's operational, financial, investor relations, HR, and legal functions, and is responsible for its ESG strategy.
Contact: bv@endeavourvision.com

Robert Oosterloo is a financial analyst at Endeavour Vision where he is involved in financial, legal, and administrative matters, including investor reporting and ESG policy.
Contact: ro@endeavourvision.com

Stay up to date with our latest news by signing up to our newsletter here.