Leveraging ESG and Cybersecurity for Resilient Organisations

Executive summary 2
Introduction 2
1. Definitions 2
1.1. What is ESG ? 2
1.2 What is cybersecurity ? 3
1.3 Cyber Security falls under all pillars of ESG 3
Concrete illustration on how cybersecurity falls under all the pillars of ESG. 4
2. Leveraging Cybersecurity and ESG 4
2.1 The EU regulator is paving the way on both issues 4
2.2 Voluntary frameworks 7
2.3 Same patterns of “People - process - technology” framework 8
2.4 Maturity timeline, process and status 8
3. Integrating cybersecurity & ESG practices into the entire supply chain : a challenge and an opportunity for SMEs 11
3.1 A maturity gap between corporations & SMEs 11
3.2 Resulting in a lack of awareness for SMEs 12
3.3 SMEs are directly hit by regulatory requirements 12
3.4 An opportunity for SMEs to implement robust cybersecurity & ESG practices ? 12
4. Case studies 13
4.1 Proactive: Non-EU companies should develop cybersecurity & ESG strategies to increase their market shares in the EU. 13
4.2 Reactive: An EU company needs cybersecurity & ESG strategies to get access to grants and investors. 16
5. Conclusions and call to action 17
5.1 Conclusions 17
5.2 Call to action 17
Sources 19
Annex 1 : EU-wide cybersecurity legislation 20
Annex 2 : Major EU ESG Regulations 21
Annex 3 : CSRD scope 22

Executive summary

This article, written by two experts in cybersecurity and sustainability, explores the integration of cybersecurity and ESG practices, highlighting how EU regulatory frameworks are setting unified standards across both domains. It emphasizes that similar assessment methods, using the "People-Process-Technology" framework, are being used to evaluate and advance organizational maturity in cybersecurity and sustainability. The article illustrates the evolution of processes and regulatory impacts, offering a clear roadmap for organizations to adapt to the rapidly changing landscape. It also focuses on the challenges and opportunities faced by SMEs in implementing these integrated practices and points out the maturity gap between large corporations and SMEs, which often results in a lack of awareness and preparedness among smaller firms. Through compelling case studies, the authors demonstrate how proactive strategies can help companies—both non-EU aiming to capture EU market share and EU-based firms seeking grants and investments—to not only comply with regulatory demands but also to gain a competitive advantage.

Introduction

The Colonial Pipeline Cyber Incident (2021) – a *ransomware attack which caused the Colonial pipeline to take the proactive measure to shut down its network as a precaution* – is a perfect example of how cybersecurity and Environmental, Social and Governance (ESG) intersect. The cyber incident disrupted society, caused economic damage, and could have resulted in an environmental disaster.

Whilst it is easy to see how climate fits into ESG, it is less obvious in the case of cybersecurity. This paper, inspired by a collaboration between two leading experts in both fields, cybersecurity and ESG, will highlight how these different areas – which are often siloed – converge and diverge, and how, when de-siloed, they can leverage companies' resources and contribute to business success. Case studies are developed to give practical and tangible examples of the areas covered. Our primary focus is SMEs operating with or within Europe, with a certain level of digitalisation achieved. While SMEs account for about 90% of all companies worldwide, they are often overlooked. A more inclusive & sustainable society cannot happen without their involvement. Nonetheless, this paper's principles and conclusions could be applied to large corporations, adapting the context.

1. Definitions

1.1. What is ESG ?

ESG is a non-financial set of criteria used to evaluate a company's sustainability and ethical impact. It is composed of 3 pillars: **environmental** (providing information on how well a company is managing its environmental resources), **social** (addressing social issues) and **governance** (maintaining strong governance practices i.e. regulatory, risk management, internal policies). It has been long been proven that implementing ESG strategies can improve a company's performance[1].

[1] 2025 Executive Benchmark Survey – Workiva, https://www.workiva.com/resources/2025-executive-benchmark-integrated-reporting

1.2 What is cybersecurity ?

The U.S. Cybersecurity and Infrastructure Protection Agency, CISA defines cybersecurity as '*the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information*'[2]. Information security is a related concept. According to NIST[3] 'The term 'information security' means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability.' In practice, the terms cybersecurity and information security are often interchangeable and in the context of EU policies, they cover the full scope of securing all information and Information and Communication Technology (ICT) systems. The EU focus is on national security, critical business processes, systems and services, and digital products, mandating a risk-based approach and taking account of supply chain considerations.

1.3 Cyber Security falls under all pillars of ESG

Reviewing these 2 definitions, one thing is certain : cybersecurity contributes to all pillars of ESG. We can even go as far as to say that an ESG framework cannot be considered as strong if cybersecurity is not included.

In the opening example of Colonial Pipelines, the incident resulted in a **social aspect** (uncertainty and inability to transport people), a **governance aspect** (cybersecurity policies, such as secure password, data backup and recovery testing, and disaster recovery plan were not aligned with the business needs), and it **could have resulted in an environmental disaster**, should the technology used to move oil have been impacted. Another example of a vulnerable critical sector is drinking water. In 2024, the U.S. Environmental Protection Agency Office of the Inspector General raised cybersecurity concerns about existing drinking water systems. According to a 2023 report from the US Water Alliance, a one-day disruption in water service across the United States could jeopardize $43.5 billion in economic activity[4].

Another example is provided by the André - Mignot hospital in France, which in November 2022 fell victim to a cyberattack[5]. The consequences were devastating. Several of these consequences can be mapped to ESG:

- Personal data exposure + surgeries postponed (**social aspect**);
- To limit the damage, the hospital had to shut down its computer systems. With no monitoring, the staff had to revert to using pens and notebook (**governance aspect**).

The financial loss is estimated to be 7 million euros. It took 18 months for the hospital to build a new IT system.

To date, we have been fortunate enough to avoid environmental disasters triggered by cybersecurity but given the lack of data in this area, the probability of such an incident happening in the near future is difficult to estimate.

---

[2]Cybersecurity & Infrastructure Security Agency, "What is Cybersecurity?" https://www.cisa.gov/news-events/news/what-cybersecurity

[3] NIST Computer Security Resource Center, Glossary https://csrc.nist.gov/glossary/term/INFOSEC

[4] Office of Inspector General, U.S. Environmental Protection Agency (2024) Management Implication Report: Cybersecurity Concerns Related to Drinking Water Systems: https://www.epaoig.gov/sites/default/files/reports/2024-11/full_report_-_25-n-0004t_1.pdf

[5]Capital "L'hôpital André Mignot de Versailles bloqué depuis trois mois par une cyberattaque massive" https://www.capital.fr/economie-politique/lhopital-andre-mignot-de-versailles-bloque-depuis-trois-mois-par-une-cyberattaque-massive-1464519

What are the best practices in minimizing the risk of cyberattacks? We asked an asset manager. Indeed, **asset managers rank cybersecurity as their 2nd biggest concern among ESG-related themes[6].**

*"We limit such risks by outsourcing key operations and related infrastructures to third parties that have robust cybersecurity measures in place. Since our inception in 2010, we have been a staunch supporter of telecommuting (now conventionally known as "remote work") to minimize **negative environmental impacts** and, as such, **sound cybersecurity measures** have always been a component in the company's risk management plan".*

***Peterson Frederick**, Chairman & Interim Chief Executive Officer of Northern Providence Investments.*

Concrete illustration on how cybersecurity falls under all the pillars of ESG.

- Environmental : a cyberattack can lead to environmental damages, yet, cybersecurity could become overly resource - intensive (i.e. encryption, logging, AI monitoring, blockchain technologies used for cybersecurity are are energy intensive technologies) ;
- Social : breach in a healthcare security system could expose certain groups to a social risk, lack of cybersecurity measures could undermine the freedom of expression and societal dialogue, and biased cybersecurity measures could limit the protection for certain age, language, social or cognitive groups ;
- Governance : reporting, supply chain considerations and regulatory compliance need to be embedded within the organisation, integrating both environmental (ESG) and security rules and considerations, and risk-based approaches.

2. Leveraging Cybersecurity and ESG

ESG and cybersecurity considerations should be managed in unison to leverage existing strategies, partnerships, methods, processes and data. It is also necessary to ensure that one objective doesn't undermine the other.

2.1 The EU regulator is paving the way on both issues

Both cybersecurity & ESG risks are governed by EU regulations. In both cases, the EU regulator expects companies to use a risk-based approach i.e. to focus on high-risk value chain segments where adverse impacts are more likely to cause significant damage. Being regulated assumes the means for evidencing and validation, which requires a certain maturity and effort in the alignment and formalisation of internal organisation considerations, processes and decisions.

2.1.1 Focus on cybersecurity regulations

There are **two types of EU cybersecurity regulations**: one focusing on the sector of operations and applied at the level of the organisation (**process-based requirements**) and the other

[6] RBC Global Asset Management, "2022 Key Findings" RBC Global Asset ManagementResponsible Investment Survey, 2022

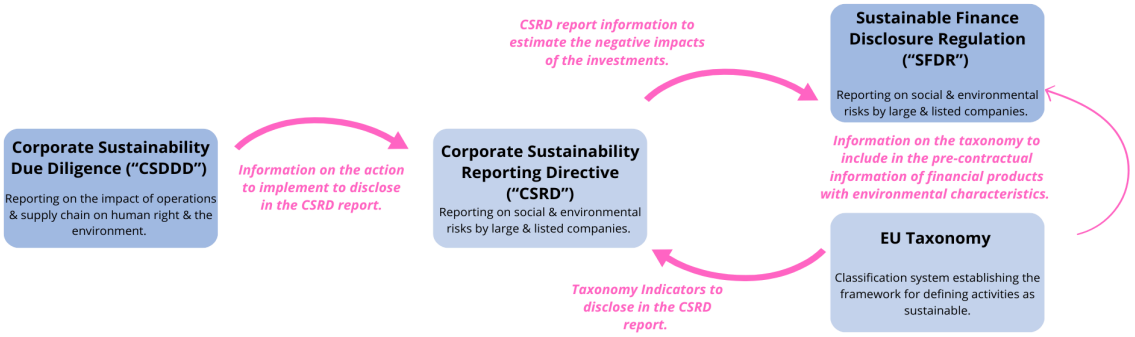
focusing on the products placed on the EU market by the organisation (**product-based requirements**). Companies could fall within one or both categories of regulations, with the **objective of no overlap between process regulations** (the stronger one would apply). For instance, DORA is applicable to the financial sector, as it is more stringent than NIS2. On the product side, it is a more complex picture: depending on the variety of products produced by the company, there may be multiple product regulations to consider. In addition, the producer will also fall within a process regulation (NIS2 covers 'manufacturers' but the EU Medical Devices Regulation (MDR) focuses on the 'product' of the factory). Yet, for one product one (more targeted) regulation is leading. But, for the product line, each product would need to evidence the regulatory compliance.

All EU product and process regulations focus on 1. Risk management approach, 2. Set of minimum security measures, 3. Testing and assessment, 4. Significant incident reporting. The regulations circle around the PDCA (PLAN-DO-CHECK-ACT), a 4-step iterative method for improving processes and products continuously, plus a new requirement that we can call: SHARE. All NIS2, DORA, CRA require formalising (PLAN), implementing (DO), assessing (CHECK), keeping up-to-date (ACT), and communicating (new: SHARE) cybersecurity or ICT incidents, risks, threats, vulnerabilities, and mitigation measures.

2.1.2 Focus on ESG regulations

The EU has developed The European Green Deal, a growth model based on a clean & circular economy. As part of the European Green Deal, regulations pertaining to ESG have been adopted. They are designed to **help companies in reporting their performance** related to sustainability, social responsibility & ethical governance. All these regulations are **interconnected**.

The interconnexion between EU ESG regulations



For more details on EU ESG regulations, please refer to Annex 2.

The Omnibus Regulation : a setback for corporate sustainability ?

In November 2024, the European Commission announced a simultaneous revision of the EU taxonomy, CSRD and CSDDD. This revision is part of a legislative package known as "Omnibus". Its goal is to **simplify the EU's business environment to push innovation and to make the EU more competitive**. A few concerns were raised by large corporations who pushed back against the Omnibus[7]. Indeed, oversimplification could undermine what has been done so far regarding ESG.

In such a context, on February 26th, the "Sustainability Omnibus" was published. The **key takeaways** are:

- **80% of companies to be removed from CSRD & EU Taxonomy scope:** under this proposal, reporting is mandatory only for companies with over 1000 employees;
- **2-year delay** for companies under the 2nd & 3rd wave of reporting of CSRD ("stop the clock");
- **Reduction of European Sustainability Reporting Standards ("ESRS") data points.**
- **CSDDD weakened :** for instance, monitoring frequency reduced from every year to once every 5 years**.**

Is this the end of corporate sustainability? No.

- First, this is **a proposal** i.e. it is hard to predict the outcome.
- **ESG reporting is here to stay** despite the current climate of uncertainty. Stakeholders (investors, clients…) will continue requesting sustainability data. More than ever, dialogue is important.
- Finally, **let's not forget**: adopting ESG practices is more than performing a compliance exercise. It is a tool for risk management, a driver for profitability and consequently, a competitive advantage. And most importantly, it is **an essential component of making society more inclusive and sustainable**.

2.1.3 Cybersecurity imperatives fit into ESG considerations

The CSRD introduces **significant changes in companies' cybersecurity practices**.

- Before the adoption of the CSRD : there **were no disclosure requirements in the area of ESG** i.e. companies were free to decide if and to "*what extent they would disclose cybersecurity information in their annual report*".
- After the adoption of the CSRD : cybersecurity is **an essential part of sustainability disclosure**. For instance, ESRS S4 focuses on the disclosure of sustainability risks impacting consumers and end users. Thanks to this disclosure, stakeholders will be able to have an understanding on how a company *"identifies, assesses, mitigates, and remediates this material impact"*. From a cyber risk point of view, it means that some of the measures adopted in compliance with Article 32 GDPR & Article 21 NIS 2 can be disclosed in the annual report to meet the disclosure requirements of ESRS 4. This intersection is the perfect illustration on how companies do not start from scratch : they can **leverage the existing risk management processes**.

With cybersecurity being a part of regulatory sustainability disclosure, the message is clear :

- There's a shift in the way cybersecurity is perceived : it **has evolved from an industry issue to a global social issue** ;
- Analysing cybersecurity risk through the ESG lens helps to have a **better understanding of a company's internal operational system** and it **helps investors in their decision-making process**.

Cybersecurity regulations only focus on protecting the information systems and supporting facilities against threats (in this case, environmental threats). **Sustainability considerations are not sufficiently referred to in EU cybersecurity rules and legislation**. NIS2 and GDPR set requirements for

[7] Open letter by major businesses, Jan 2025: https://media.business-humanrights.org/media/documents/Omnibus_Business_Statement_17_January_2025.pdf

'appropriate and proportionate technical, operational and organisational measures to manage the risks' (Article 32 GDPR & Article 21 NIS 2). This could be an area for future improvement, where the 'environmental' impact of cybersecurity / ICT incidents reported is evaluated. If one wants to go further, 'appropriate and proportionate' security measures to be implemented would be measured in terms of security, privacy, but also in terms of environmental impact. Nonetheless, given the current political situation and organisations' cybersecurity maturity, this would not be feasible. For now, **encouraging organisations to report the environmental impact and cost of cyber(in)security** (for both measures + incidents) would be a **great step further in increasing the transparency and linking both major objectives together**.

2.1.4 ESG imperatives should fit into cybersecurity considerations

While the ESG principle of governance is at the heart of cybersecurity, with management, continuous assessment and reporting obligations, the social and environmental impacts of cyber security considerations are in their infancy. The objective to protect society from cyber threats is a trigger for many EU regulations (GDPR, NIS2, DORA, AI Act, CRA, to name a few). In these regulations, concrete assessment of the societal impact of security measures or the lack of such is scarcely considered. For example, are modern cybersecurity measures working for all parts of society? Captcha may not work equally well for young people as for elderly, or for autistic people and people with sensory impairments. Are security monitoring cases designed fairly, with no discrimination or biased results? Is cybersecurity a universal right?

Whilst environmental threats are considered, the environmental objectives are not considered in cybersecurity. For example, the question of intensive energy utilisation by AI models is largely debated, but not yet fully estimated and applied in user organisations context. The cybersecurity team training or deploying an AI model for network monitoring and alerting, for instance, would not have an input on the energy utilisation of the given choice. Similarly, data encryption mandated by EU regulations as a major data confidentiality security measure has an impact on energy and battery life (if encrypted in a connected device). As such, more research is needed to provide data for an informed decision, making and aligning both ESG and cybersecurity considerations. As a first step, companies may consider the environmental, social and resources impact of their chosen cybersecurity measures, and settle for those that are most "appropriate and adequate".

2.2 Voluntary frameworks

Companies can adhere to voluntary standards/frameworks - **aligned with the company strategy** - to **reinforce their commitment to cybersecurity & ESG** and to **stand out from the competition**. As with regulations, we can find cybersecurity aspects in sustainability standards. The opposite is less obvious.

Sustainability standards containing a cybersecurity aspects

- Sustainability Accounting Standards Board (SASB) **:** requires companies in the software industry to report cybersecurity attacks.

Other notable sustainability standards

- Voluntary Sustainability Reporting Standards for non-listed SMEs (VSME) : for SMEs that

fall outside the CSRD but who face growing sustainability requests from business counterparties (i.e. banks, investors or larger companies for which non-listed SMEs are suppliers).

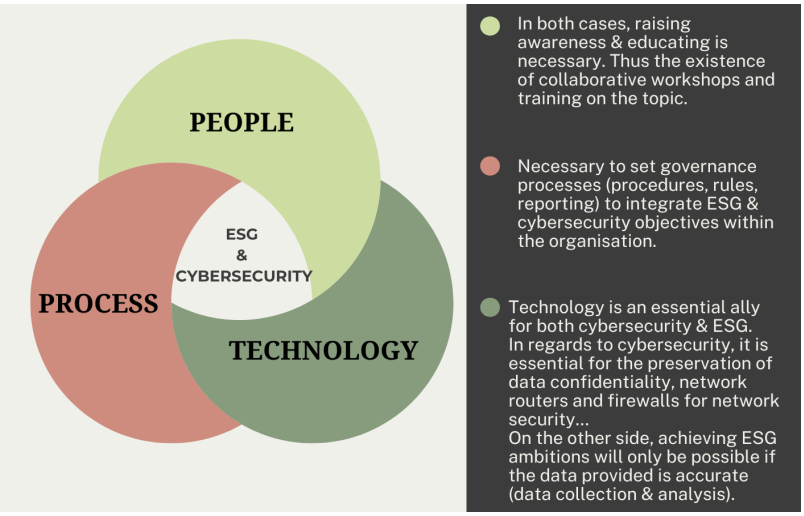
- B-Corp Certification : measurement of the entire company's social & environmental status.

Information security standards

- Many of these contain environmental considerations but no sustainability objectives.
  - ISO27001, Service Organization Control (SOC)2, Cloud Security (EUCS, CSA), include controls for the protection against environmental threats (fire, floods)

Once again, the company is never really starting from scratch. A mapping between the **regulations and various standards or between cybersecurity obligations and sustainability requirements** can be performed in order to facilitate the work.

2.3 Same patterns of "People - process - technology" framework



2.4 Maturity timeline, process and status

Understanding where industries are currently at and the direction they are taking is crucial in order for businesses to be able to respond to growing stakeholders' concerns. One thing that seems to be agreed upon is that maturity-wise, though the history is different, **ESG seems to be following the "maturity curve" that cybersecurity went through**. 3 phases can be identified :

PHASE 1 - AWARENESS (PRE 2000s)

- Pre-NIS 1 directive, the industry and policy makers were **mostly discussing privacy and data security issues**.
- On the sustainability side, given that there were no rules, **sustainability was mostly seen as a communication tool**. The **context was prone to greenwashing**. ESG-related actions were mostly voluntary and standalone.

PHASE 2 - REGULATIONS ARE PAVING THE WAY (2010 - 2030)

- Cybersecurity is **no longer just an "IT issue"**: it is a business, social and national security concern.

  On the economy and business side, cybersecurity became **a matter of business survival**, with 57% of SMEs admitting that they would likely going out of business six months after a cyber incident[8], with days to weeks of business disruption and average of 7,4 months recovery time[9]. Data breaches also cost on average USD 4.88 Million[10] per year. While many CEOs admit concerns about cybersecurity, with 92% of SMEs recognising cybersecurity is important to their enterprise[11], in practice, much of the enhancement proposals coming from CISOs are being under-budgeted, and only 16% of SMEs feel very well prepared for an attack[12]. As such, **Regulations put the accountability to Board-level and C-level decision makers**. New (CRA, DORA) and enhanced (NIS2) cybersecurity regulations are quickly adopted. Cybersecurity requirements are embedded in other product regulations (AI Act, MDR). Significant cybersecurity incidents (and vulnerabilities exploitation) are now a regulatory obligation. Specific harmonised standards and EU cybersecurity certification schemes are under development to support compliance.

  On the social and national security side, **cybersecurity plays a role in the security of democratic processes / elections**. Most recently, major revelations for cyber attacks contributed to the annulment of the Romanian 2024 Presidential elections[13]. Cyber attacks are used as a weapon of war, with NATO recognising Cyberspace as a 'Domain of Operations' at the Warsaw Summit in 2017. The cyber dimension is a first and clear signal of all armed conflicts (eg in Ukraine critical infrastructure cyber attacks started years before the conventional war, and continue ever since) and political tensions (e.g. Europe is continuously under DDOS or spyware attacks that aim to undermine institutions and 'punish' opposing views).

- ESG-wise, the Green came fully into force : competent authorities are building a standardized framework (with talks for amendment as previously mentioned). Disclosures are now a regulatory requirement. In the EU's banking & financial sector, "**climate related greenwashing incidents declined by 20% in 2024[14]"**.

  However, the political situation in Europe has changed in 2024, moving from left to the right in the political spectrum, with quickly evolving economic and security threats that take priority, resulting in strong emphasis on simplification (rather than new regulation).

  One aspect that we should pay particular attention to is how to **simultaneously leverage both security and ESG objectives**. For instance, in 2025, the state-of-art security technology such as cryptography methods, AI-monitoring, block chain are energy intensive, with one

[8] ENISA (2021) Cybersecurity for SMEs - Challenges and Recommendations, available: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Cybersecurity%20for%20SMES%20Challenges%20and%20Recommendations.pdf
[9] Cyber Magazine (2024), "Fastly: Incident Recovery Taking 25% Longer – Why It Matters" https://cybermagazine.com/articles/fastly-incident-recovery-takes-25-longer-why-it-matters
[10] IBM (2024) Cost of Data Breaches Report, available: https://www.ibm.com/reports/data-breach
[11] Google (2023) Europe's SMEs in the Digital Decade 2030: Building Cyber-resilience, Overcoming Uncertainty, available at https://storage.googleapis.com/grow-with-goog-publish-prod-media/documents/Europes_SMEs_in_the_Digital_Decade_2030_report.pdf(2023)
[12] Ibid
[13] The New York Times (2024) "Romanian Court Annuls Presidential Election Results and Orders a New Vote", https://www.nytimes.com/2024/12/06/world/europe/romania-election-court.html
[14] RepRisk, Special report (2024) "A turning tide in greenwashing? Exploring the first decline in six years" https://www.reprisk.com/research-insights/reports/a-turning-tide-in-greenwashing-exploring-the-first-decline-in-six-years?mtm_campaign=pressreleaseq424-greenwashing2024&mtm_kwd=reportsq424&mtm_source=pressrelease-traffic

study finding encrypting the data on a connected device reduces its battery lifespan in half. Regarding the **disclosure of sensitive information in the report**, the VSME mentions that the company can omit to disclose "classified or sensitive information" and it shall state the omission in the report.

PHASE 3 - AUTOMATION & MATURITY (2030s onwards)

A likely scenario for the next phase is as follows:

- **Cybersecurity**: machine learning and AI completely take over the technical domains of cybersecurity (i.e. monitoring, detection, and reaction). Global divide in cybersecurity capability. Supply chain and IoT devices' attacks leverage the scale and speed of attacks, resulting in the first Global and record breaking disruptive cyber incident, certainly with an economic and social impact, and potentially with an environmental impact.
- **Sustainability**: on data, with the development of ESG data providers, it will be standardized and its collection will be automated. AI use will play a prominent part. Here, AI must be developed in a way that fully supports sustainability (i.e. developing a sustainable AI).
- **Aligning Cybersecurity and Sustainability objectives**: cybersecurity measures would need to be further improved to remain sustainable, and sustainability disclosure requirements would need to consider the cybersecurity risk it creates to disclosing entities.
- **People**: the heavy reliance on narrowly focused 'experts' will slowly diminish with the automation tools' improvement and self-design and control. Experts with system-view, rather than narrow specialisation, combining business, sustainability, process, IT and people skills would nonetheless be required to make organisation-wide strategic decisions. Such experts are needed for creating feedback loops for system correction and improvement, and steering the use of AI development in the most beneficial direction for the organisation.

3. Integrating cybersecurity & ESG practices into the entire supply chain : a challenge and an opportunity for SMEs

Because they do not possess the same resources and capacity as big corporations, integrating cybersecurity & ESG practices into the entire supply chain can be a challenge. For both issues, there seems to be a maturity gap between corporations and SMEs.

3.1 A maturity gap between corporations & SMEs

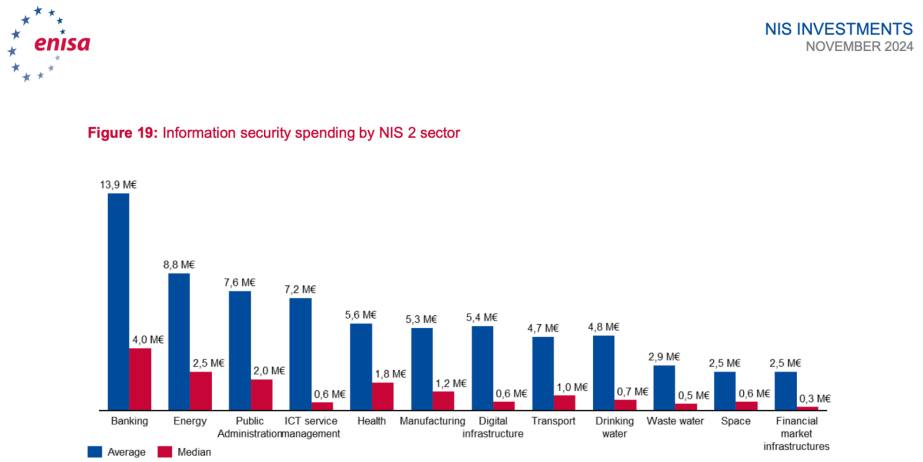
Large corporations face high financial impact and understanding of the material cyber risks and Sustainable Development Goals (SDG) breaches. Those who have transparency obligations such as

listed companies and government organisations bear more accountability, leading to emphasis and higher maturity in compliance and reporting. In addition, corporations have more resources and are legally obligated by regulations to follow specific rules. Regulated sectors, e.g. critical sectors have higher maturity in corporate governance, compliance, reporting. Consequently, **large corporations tend to have a proactive approach** towards ESG & cybersecurity practices i.e. it is part of their business strategy.

For instance, Orsted – a Danish multinational power company – voluntarily published its CSRD-compliant report from the 2023 reporting year i.e. before the required date by the regulator. The same can be said for cybersecurity: due to economies of scale, corporations have control over/possess their own AI & data-driven tools.

Despite the "shifting political winds", large corporations are not stopping **their investments in the green transition.** In January 2025, Nicolai TAIGEN, the CEO of Norges Bank Investment Management - the world's largest sovereign fund - reiterated the Bank's commitment to ESG. In 2024, the fund divested from 49 companies based on sustainability assessments.

At the outset of cybersecurity regulations, in 2018 a coalition of global corporations from diverse industries set a Charter for Trust with its ten principles[15], according to which they commit to set a direction and demonstrate thought leadership 'For a secure digital world': https://www.charteroftrust.com/. Financial sector corporations have led the way when it comes to cybersecurity. For example, in 2021 the Bank of America CEO announced spending more than USD 1 Billion in cybersecurity yearly. In Europe, the ENISA NIS 2024 investment report[16] revealed that in 2023 Banks continue to lead by far when it comes to information security investment, albeit very modest compared to their US competitors, with EUR 13.3 Million average yearly spendings, compared to 8.8 Million for the next in line (energy) critical sector.



[15] The ten principles are: Ownership of Cybersecurity, Responsibility Throughout the Digital Supply Chain, Security by Default, User-Centricity, Innovation and Co-Creation, Transparency and Response, Regulatory Frameworks, Education, Certification for Critical Infrastructure and Solutions, Security Baseline

[16] Enisa European Union Agency for Cybersecurity "NIS Investments 2024" (2024) https://www.enisa.europa.eu/publications/nis-investments-2024

In contrast, SMEs tend to have a **reactive approach** towards ESG & cybersecurity practices i.e. it is not part of their business strategies. They see it as compliance issues i.e. they will act on it mostly because of supply chain requirements.

3.2 Resulting in a lack of awareness for SMEs

SMEs need to be more aware of the extent of their supply chain regarding both ESG & cybersecurity risks. Currently, there is a lack of awareness.

71%[17] of "the smallest organizations by annual revenue have not been asked to prove their cyber security posture by their supply chain partners". On the contrary, 71%[18] of the largest organizations by annual revenue have been asked this question. This makes SMEs more prone to cyberattacks. **To build a more secure cyber environment, collaboration & communication between the various stakeholders is crucial**.

Moreover, most SMEs tend to minimise their ESG actions. For some, they are **not even aware that some of their existing actions are ESG practices**. For instance, mentoring young entrepreneurs or students fits into the S of ESG. As such, they do not communicate ESG practices and **miss out on the reputational benefits from informing the public**.

3.3 SMEs are directly hit by regulatory requirements

As previously mentioned, the regulatory landscape is evolving. Cybersecurity and ESG regulations do have **an impact on SMEs and their supply chain**. Even SMEs not in the scope of these regulations still bear the responsibility linked to the business relations with corporations.

NIS2 indicates that the businesses under its scope must consider the vulnerabilities specific to each direct supplier and service provider as well as the quality of their product. **Should the suppliers & services providers be considered "high risk", the business will change suppliers & service providers**. As for the CSRD, it requires companies to collect ESG data from their suppliers so that they can include the data in their report. **In other words, SMEs outside the scope of EU regulations may still need to implement the minimum requirements and provide relevant data to their clients in the EU**.

Failing the above would limit the **potential for customer recruitment and retention for SMEs** as clients may choose to prioritise NIS2/DORA/CSRD-compliant suppliers or suppliers that are not considered "high risk" .

[17] World Economic Forum, "Global Cybersecurity Outlook 2024" (2024) https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf
[18] Please refer to footnote 16.

3.4 An opportunity for SMEs to implement robust cybersecurity & ESG practices ?

Incorporating cybersecurity & ESG practices into the supply chain is more than just a compliance exercise. It is **an opportunity for companies to be more competitive**. In such a context, collaboration between corporations and SMEs is necessary for things to go smoothly in their supply chain. It will allow SMEs to:

- Deepen their relationships with large corporation: it has been shown that SMEs productivity and large corporation firm productivity are interconnected[19];
- And consequently, develop robust cybersecurity & ESG practices that will make them more competitive.

4. Case studies

4.1 Proactive: Non-EU companies should develop cybersecurity & ESG strategies to increase their market shares in the EU.

Scenario : Company A is an ICT company based in the UK (30 employees). It provides services to the EU market. Company A has no dedicated cybersecurity nor ESG team. To increase its market shares in the EU market and work with larger companies, company A is thinking about developing cybersecurity & ESG strategies. It faces a double challenge : strengthening its cybersecurity system while developing sustainable practices. However, it is not sure on where to start given the latest regulatory updates & debates on both topics. Consequently, guidance is needed.

Step 1 - Determine ESG requirements

Before diving into the requirements (mandatory and/or voluntary), let's **identify the Sustainable Development Goals** ("SDG") that an ICT company can attain[20]. It helps **frame the ESG strategy & define the ESG objectives**. To prepare, a deep dive into company A's universe led by a sustainability specialist[21] is to be performed to fully understand the company DNA and to create a **tailor-made sustainability plan**. Below are a few examples of SDGs that company A could work on.

[19] McKinsey Global Institute, "A microscope on small businesses: Spotting opportunities to boost productivity" (2024) https://www.mckinsey.com/mgi/our-research/a-microscope-on-small-businesses-spotting-opportunities-to-boost-productivity

[20] There are 17 SGD. Created by the United Nations in 2015, they aim to bring peace and prosperity for people and the planet, while tackling climate change and working to preserve the environment and oceans.

[21] According to a report by the UK firm Burges Salmon, out of the 361 U.K companies polled, 32% were "completely unprepared" to meet their supply chain disclosures obligations, and only 29% believe their companies fully understand the legislative and regulatory landscape governing ESG corporate disclosure.

As an ICT company , company A should aim to create smart manufacturing and IT solutions (**SGD 8 : decent work & economic growth**). The solutions developed should aim to reduce costs & consumption i.e. environmental footprint (**SGD 12 : responsible consumption and production**). Finally, the IT sector suffers from a shortage in women which prevents it from being competitive[22] (**SDG 5 : gender equality**). Actions should be put in place to decrease this gap.

Now that the objectives are clear, let's identify the **applicable requirements**.

- **Regulation** : besides being a non-EU company, company A is a non-listed SME. Consequently, it falls outside the scope of the CSRD. However, because of **supply chain requirements**, an EU large company will request ESG data in order to include the data in their report (in regards to the Omnibus, large companies continue to be in scope). Should company A be unable to provide such data, gaining contracts with large companies will be hard.
- **Voluntary framework** : there are many frameworks available. However, because company A wants to i**ncrease its market shares in the EU market**, the best option is to follow the **VSME framework**[23]. The VSME framework is divided into two modules in order to cater to the diverse needs of SMEs : the **basic module** (an entry level framework) and the **comprehensive module** (for larger SMEs or SMEs with advanced sustainability practices). Given its size and the non-existence of sustainability practices within its business, company A should follow the basic module. A gap analysis to check compliance with the VSME Basic module will be performed and will result in a roadmap for gap implementation with **key performance indicators to reach**.

Step 2 - Assessment of cybersecurity requirements

In the proactive scenario, for a non-EU company expansion to a new market, it needs to list its client sectors and locations to identify which regulations would be relevant or expected by its customers, partners or regulators. Then it will check the sectoral regulations in Annex A, and identify those applicable to its business or clients.

Then, Company A needs to identify if it is placing any products placed on the EU market, i.e. making available for purchase a standalone product or service. If yes, then it would look into Annex 1 product regulations to identify which regulations apply.

After confirming the scope, Company A will look into the specific conformity assessment procedures, and if there are any standards or certifications required or accepted as a presumption of conformity. For instance, ex-post checks like GDPR will allow doing business but assume an audit after an incident. Ex-ante conformity assessment like CRA or MDR would require planning of compliance

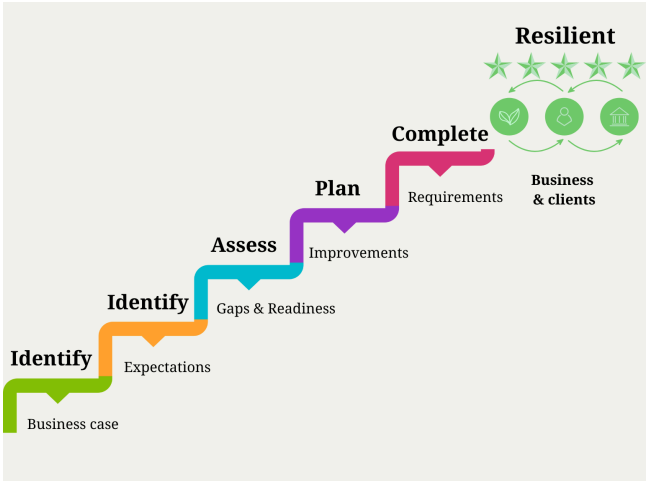
[22] McKinsey Digital "Women in tech: The best bet to solve Europe's talent shortage" (2023) https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/women-in-tech-the-best-bet-to-solve-europes-talent-shortage
[23] For SMEs outside the CSRD scope.

efforts before placing the product on the market. These considerations would have an impact on the business.

Company A will then draw a list of requirements to be verified. The list of requirements to be verified will include scope, requirement, means of verification. It will be either originating from an industry standard (if widely required by specific industry), or from regulations. Most likely, a combination of at least one standard (presumption of conformity) and one regulation will be required. Additional requirements, specific for the regulation, like incident classification and reporting, testing frequency and scope, management accountability and sign off. Completing the verification of implemented measures will take a few months, a collaborative effort between management, IT/security department, HR, team leads, suppliers, possibly external specialised cybersecurity compliance consultants. The verification will result in a gap assessment and a roadmap for gap implementation. Some sector-specific requirements (e.g. DORA) will be difficult (time + cost) to implement in the short term, as such, Company A decides to pause the financial sector targeting for now, developing a special department in the future, and prioritise other sectors for its general services. These considerations would have an impact on the business.

The applicable requirements for the selected sectors will feed into a programme, with its priorities and budget, responsible and timeline for implementation.

Step 3 - Leveraging ESG & cybersecurity efforts



In view of the above, the VSME-compliant report should first disclose **general information** such as the company profile and the "*practices, policies and future initiatives for transitioning towards a more sustainable economy*".

In other terms, compliance with both cybersecurity & ESG requirements should be displayed (policies implemented, risk management processes…) in this part of the report. The targets to monitor the

implementation of these policies as well as the progress achieved towards meeting these targets should also be included here.
Initiatives include, for instance, efforts to reduce the environmental footprint, initiatives to improve gender equality in the workplace or how technology innovation helped to create a smart solution.

The report should then **disclose the following metrics** :

- **Environmental metrics** such as total energy consumption (and include how much of it is renewable), scope 1 emissions (emissions owned or controlled by a company), scope 2 emissions (emissions that a company causes indirectly like the emissions caused when generating the electricity in the company building) : this is a **sign of reliability to large companies under the CSRD scope that seek aligned suppliers**.
- **Social metrics** such as the workforce composition or the training programs (how many people did attend the cybersecurity training? This number can be obtained from the info collected from the cybersecurity requirements). This demonstrates a **commitment to social responsibility & talent upskilling**. And also, it raises investors' interest should company A be looking for investors.
- **Cybersecurity information** for products with digital elements placed on the EU market, such as confirmation of the fulfilment of the applicable cybersecurity regulations (see Annex 1 for Europe), the vulnerability handling processes put in place by the manufacturer, the assessment of the product life cycle cybersecurity risks.

After publication of the report and information, the cybersecurity and sustainability plans should be regularly updated to see the company progress on both areas with key impact indicators.

4.2 Reactive: An EU company needs cybersecurity & ESG strategies to get access to grants and investors.

Scenario : Company B is an ICT company based in the EU. Company B has no dedicated cybersecurity nor ESG team. To raise capital through private investments and/or EU grants, company B needs to develop cybersecurity & ESG strategies. It faces a triple challenge : strengthening its cybersecurity while developing sustainable practices, in a short timeframe. It does not have the expertise and resources to devote full time to carry out the project. Consequently, it needs support.

Company B will have to go through a market due diligence (incl. Regulatory considerations) by investors or compliance attestation by granting authorities. The scenario will run with the steps in scenario 1, except that business and technology choices have already been taken, leading to a small space for manoeuvre to break down the compliance project to achievable stages. Following the gap assessment, the regulations, industry standards, and measures implementation (for this specific example) would require a minimum 6 months with full speed external support on the project, with expensive technical adaptations to be made on the project. No affordable option is available to company B to prove its viability and sustainability. As a result, the grants/investment are directed to the company B's competitor, which had a strategy and proactive approach to ESG & cybersecurity.

Most of the companies will find themselves in the middle, somewhere between both extreme scenarios. However, selecting these scenarios we wanted to provide the considerations in an extreme situation to enable business leaders to make their own choices and control the narrative.

5. Conclusions and call to action

5.1 Conclusions

It is clear that cybersecurity & ESG intersect. More than that, cybersecurity falls within all three pillars of ESG - good governance, social and environmental impact. Cybersecurity requires good governance. Lacking cybersecurity could pose societal risks, especially for weak democracies, vulnerable groups. Cybersecurity breaches could trigger environmental crises (e.g. major energy or water or space systems out of order) or harm the environment if designed to overly-rely on energy intensive security measures such as encryption, big data and/or AI monitoring.

Each objective: ESG and cybersecurity provide a competitive advantage to organisations. As they are based on common objectives and similar regulatory mechanisms, if both ESG and cybersecurity are considered and achieved, the organisation could leverage its compliance efforts, avoiding environmental and cyber risks and unlocking growth opportunities.

5.2 Call to action

To fully enjoy the benefits of integrating cybersecurity & ESG practices into their businesses (growth opportunities), companies need to :

- Adopt a proactive approach towards both ESG and cybersecurity, integrating it into the business strategy.
- Implement Industry Standards and Regulations (even if not mandatory for your company). Providing assurance and communicating it through standardised frameworks (standards, regulations) can unlock trust and new markets.
- Financial institutions should leverage DORA and CSRD to build dual-compliance strategies.
- Balance the benefits of cybersecurity with its environmental impact/cost.
- Embrace automation for daily tasks to free the time needed for team members to enhance and leverage the available processes, information, resources.
- Upskill teams, for instance, prioritise cybersecurity talent development alongside ESG training.
-

To leverage and facilitate the update of both cybersecurity and ESG objectives, policy makers need to:

- Synchronise governance requirements
- Identify opportunities and support the update of cybersecurity and ESG certifications
- Consider cybersecurity in ESG requirements, and ESG in cybersecurity rules.

—----------END—----------

For more information, please contact :

Iva TASHEVA, Cybersecurity Lead : iva.tasheva@cyen.eu
Clémence BETESUKU, ESG Lead : clemence@theupliftagency.fr

Sources

Reports :

- Global Cybersecurity Outlook - Insight Report January 2024, *World Economic Forum* : https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf
- Responsible investment 2024 - *Norges Bank Investment Management* : https://www.nbim.no/en/responsible-investment/divesting-from-companies/
- A microscope on small businesses - spotting opportunities to boost productivity, *McKinsey Global Institute* : https://www.mckinsey.com/mgi/our-research/a-microscope-on-small-businesses-spotting-opportunities-to-boost-productivity
- NIS Investments 2024, *Enisa* : https://www.enisa.europa.eu/publications/nis-investments-2024
- Cybersecurity for SMEs - Challenges and Recommendations, ENISA 2021 : https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Cybersecurity%20for%20SMES%20Challenges%20and%20Recommendations.pdf

Research paper

- Reporting cybersecurity to stakeholders: A review of CSRD and the EU cyber legal framework - *Science Direct* : :https://www.sciencedirect.com/science/article/pii/S0267364924000542
- Which SMEs are greening? Cross-country evidence from one million websites, *OECD SME and Entrepreneurship Papers* : https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/07/which-smes-are-greening_ffa14385/ddd00999-en.pdf
- 2025 Executive Benchmark on Integrated Reporting, *Workiva* : https://www.workiva.com/resources/2025-executive-benchmark-integrated-reporting

Press Release :

- Decrease in greenwashing for first time in six years, *RepRisk* : https://www.reprisk.com/research-insights/news-and-media-coverage/reprisk-data-shows-decrease-in-greenwashing-for-first-time-in-six-years-but-severity-of-incidents-is-on-the-rise

Articles :

- Why cybersecurity is a critical component of ESG - *WeForum.org* : https://www.weforum.org/stories/2022/03/three-reasons-why-cybersecurity-is-a-critical-component-of-esg/
- ESG & C: Does Cybersecurity Deserve its own pillar in ESG Frameworks - *Harvard Law, School Forum on Corporate Governance* : https://corpgov.law.harvard.edu/2022/11/14/esg-and-c-does-cybersecurity-deserve-its-own-pillar-in-esg-frameworks/
- Colonial Pipeline Cyber Incident, *US Department of Energy* : https://www.energy.gov/ceser/colonial-pipeline-cyber-incident
- Exclusive: The EU Commission's draft programme for 2025, *Euractiv* : https://www.euractiv.com/section/politics/news/exclusive-the-eu-commissions-draft-programme-for-2025/
- Women in tech: The best bet to solve Europe's talent shortage, *McKinsey* : https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/women-in-tech-the-best-bet-to-solve-europes-talent-shortage

Others :

- CSRD-CSDDD-Taxonomy > Our position on the Omnibus , *Open Letter by corporations* ; https://www.we-support-the-csddd.eu/wp-content/uploads/2025/01/240106-lt-C3D-Lettre-Commission-europeenne-6-janvier-2025.pdf
- CEO of World's Biggest SWF applies for Second Term, *Bloomberg Live* : https://www.youtube.com/watch?v=pp91Px7Cgsg

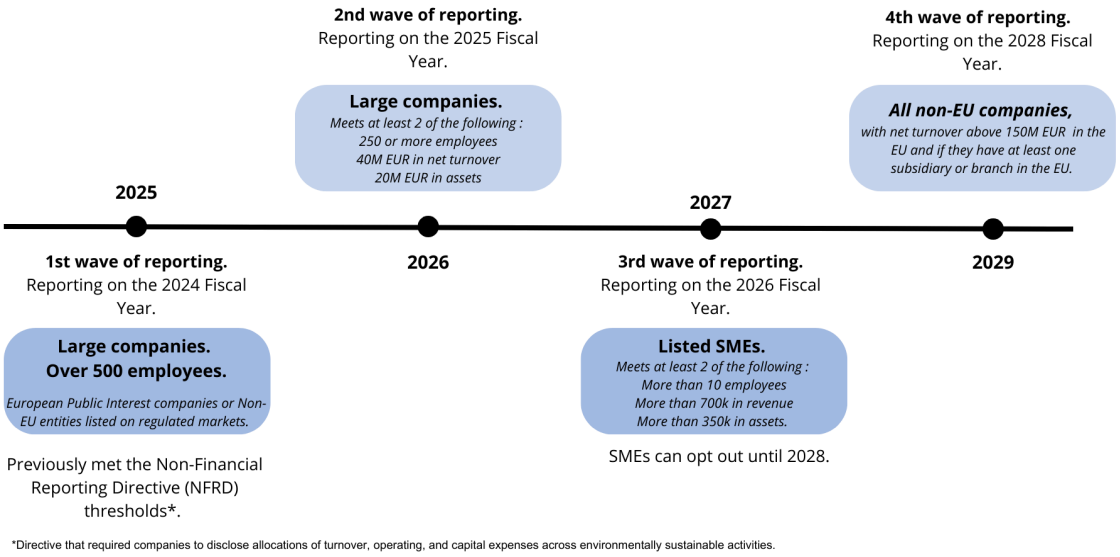
Annex 1 : EU-wide cybersecurity legislation

Process Legislation	**Measures for a high common level of cybersecurity across the EU (NIS2)** Directive (EU) 2022/2555 - applied across countries since **Oct 2024.**
	• Extensive list of cybersecurity requirements, incl. Suppliers, incidents reporting, and Board/C-level accountability. • Applicable to specific sectors: critical infrastructure ('Essential entities') or economic sectors, such as manufacturing, digital providers, research ('Important entities')
	Digital Operational Resilience Act (DORA) Regulation (EU) 2023/2554 - applied since **Jan 2025.**
	• Extensive list of ICT resilience & testing requirements, incl. suppliers, and incident, threats, vulnerability and risks' reporting. • Applicable to the financial sector at large (banks, insurance, digital infrastructure,..)
	General Data Protection (GDPR) Regulation (EU) 2016/769 - applied since **May 2016**
	• Article 32: Security of processing mandates implementing appropriate technical and organisational measures to ensure a level of security appropriate to the risk. • Scope: Processing of personal data of EU entity or persons in the EU
Product & process Legislation	**Cyber Security Act (CSA)** Regulation (EU) 2019/881 - applied since **Oct 2018**
	• Lays down minimum requirements for cybersecurity certification, defines its level of assurance in a risk-based approach, and lays down governance standards. • Scope: ICT products, services and processes • Several candidate frameworks, incl. EUCC for trust products (active), Cloud & 5G (under development), digital identity wallets (to start)
Product Legislation	**Cyber Resilience Act (CRA)** Regulation (EU) 2024/2847 - applied as from **Sep 2026 - Dec 2027**
	• Lays down minimum security requirements, incident and vulnerabilities notification, user transparency of cybersecurity risks and mitigation measures. • Scope: Products with digital element placed on the EU market (e.g. consumer electronics, software, firewalls)
	AI Act Regulation (EU) 2024/1689 - cybersecurity requirements applied as from **Jul 2026**
	• Lays down cybersecurity objectives for high-risk AI systems lifecycle.
	Medical Devices (MDR) Regulation (EU) 2017/745 - transition period ended in **May 2024**
	• Manufacturers shall set out minimum IT security requirements, incl. protection against unauthorised access, necessary to run the software as intended. • Scope: Medical devices placed on the EU market.

Annex 2 : Major EU ESG Regulations

	EU Taxonomy - entered into force in July 2020.
Process Legislation	• Classification system establishing a list of environmentally sustainable economic activities to facilitate sustainable investments. • **Scope**: aligns with the scope of the Corporate Sustainability Reporting Directive. See Annex 3 - CSRD Scope.
Product & process Legislation	**Sustainable Finance Disclosure Regulation (SFDR) - applicable since March 2021.**
	• Sets out how financial market participants must disclose sustainability information. • Applies to all financial market participants & financial advisors within the EU (asset managers, institutional advisors, insurance companies, pension funds, investment firms among others…) & to all financial products.
Process Legislation	**Corporate Sustainability Due Diligence Directive ("CSDDD") - entered into force in July 2024.**
	• Companies must now conduct **appropriate human rights and environmental due diligence** with respect to their operations, operations of their subsidiaries and operations of their business partners in companies' chain of activities. • **Scope**: EU companies with more than 1000 employees if they had an annual worldwide net turnover of more than 450M EUR in the last financial year / Non-EU companies with a net turnover in the UE of more than 450M EUR in the financial year preceding the last financial year.
	Corporate Sustainability Reporting Directive (CSRD) - applicable January 2024.
	• Replaces the **Non-Financial Reporting Directive.** • **Modernizes and strengthens** the rules concerning the social and environmental information that companies must report. A key component of this regulation is **double materiality** i.e. the impact of sustainability on a company business and the company impact on sustainability. • **Scope and timeline** : please see Annex 3 - CSRD Scope. . • **Limited external assurance on sustainability reporting** : level of assurance provided by auditors or reviewers. • Introduces the European Sustainability Reporting Standards **(ESRS)** for reporting under the CSRD. There are 12 ESRS with a simplified version for: listed SMEs, small banks & capture insurers. A mapping between **sustainability matters and the ESRS** is also to be performed.

Annex 3 : CSRD scope



*Directive that required companies to disclose allocations of turnover, operating, and capital expenses across environmentally sustainable activities.