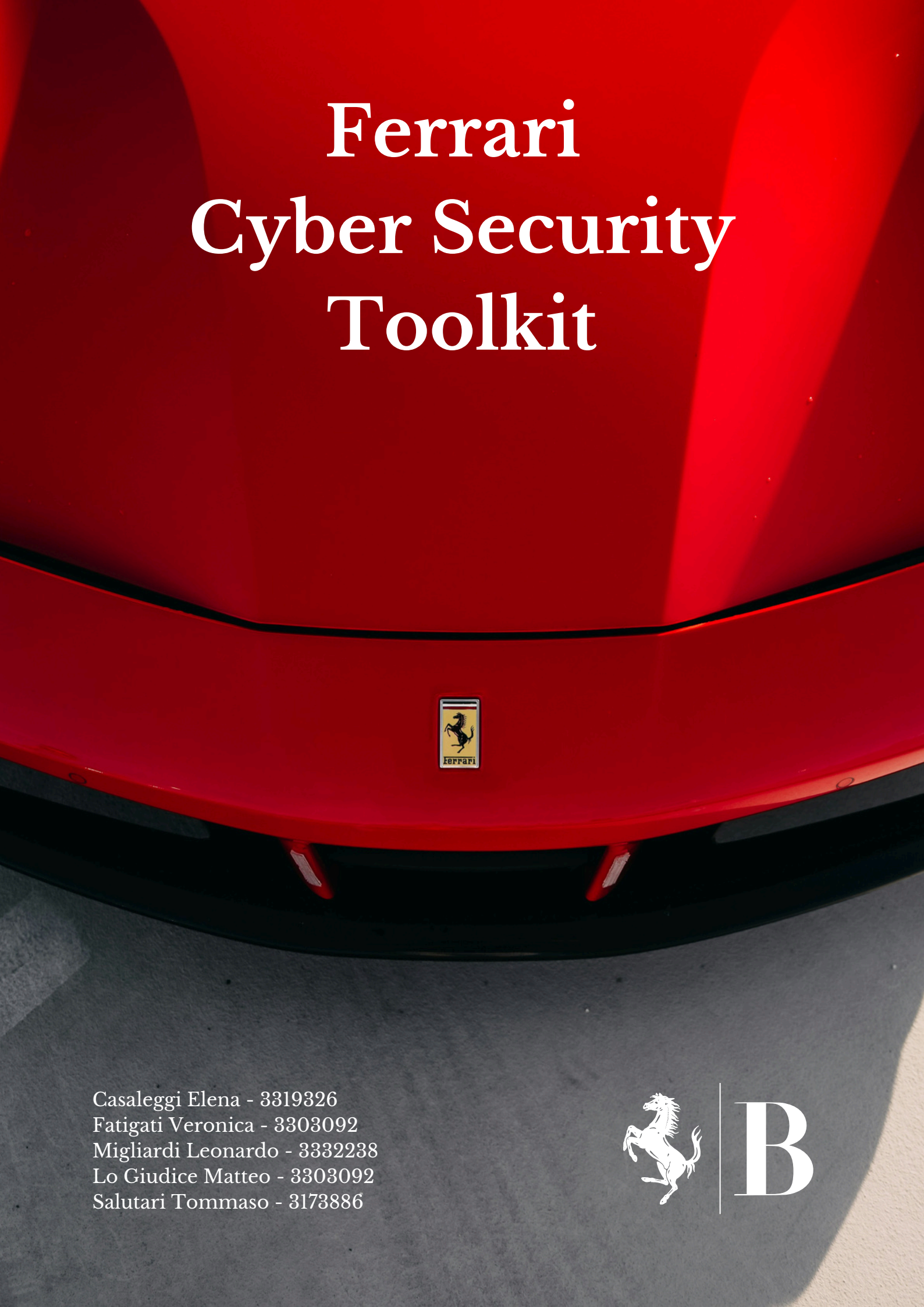
Ferrari Cyber Security Toolkit



Casaleggi Elena - 3319326
Fatigati Veronica - 3303092
Migliardi Leonardo - 3332238
Lo Giudice Matteo - 3303092
Salutari Tommaso - 3173886

Contents

Disclaimer: *The information in this report pertains exclusively to the fiscal year 2024.*

1 | Company Profile

1.1. Industry & Sectors

Ferrari operates in the **automotive sector**, distinguishing itself in two main areas of activity. On one hand, the company is engaged in the **production and sale of luxury sports cars**, creating high-performance supercars and hypercars for an exclusive market. On the other hand, Ferrari is actively involved in **motorsport**, competing with Scuderia Ferrari in Formula 1 and other racing competitions.

In recent years, the brand has also started expanding into the fashion industry, launching collections that reflect the ideals of excellence, innovation, and performance that have always defined the Maranello-based company. This strategy aims to further strengthen the brand's identity, making it an icon not only in the automotive world but also in fashion and luxury.

1.2. Products & Services

Ferrari offers a diverse range of products and services beyond car manufacturing. The company's **core business** revolves around the **production and sale** of luxury supercars and hypercars, known for their high performance, exclusive design, and cutting-edge technology. Some of the most iconic models include the Ferrari 812 Superfast, SF90 Stradale, 296 GTB, and Roma, which represent the brand's commitment to innovation and driving excellence.

Ferrari is also known for its limited-edition and special series models, which celebrate key milestones in the brand's history. These include legendary anniversary models such as the Ferrari F40, Ferrari Enzo (dedicated to the founder), LaFerrari (hybrid hypercar marking a new era), and the new Ferrari F80, which continues the legacy of exclusive high-performance engineering. Additionally, Ferrari has released ultra-limited models like the Monza SP1/SP2 and Daytona SP3, which are part of the brand's "Icona" series, inspired by classic Ferrari race cars.

At the same time, Ferrari is deeply engaged in **motorsport**, competing in Formula 1 with Scuderia Ferrari, the most successful team in the championship's history. Beyond F1, Ferrari also competes in endurance and GT racing, not only by selling race cars to private clients and professional teams but also by fielding its own factory-backed racing team in prestigious competitions such as the FIA World Endurance Championship (WEC), including the 24 Hours of Le Mans.

Beyond automotive, Ferrari has developed an exclusive selection of **personalized experiences** for its customers. The Tailor Made program allows for full customization of vehicles, while experiences like Corse Clienti and XX Programmes give enthusiasts the opportunity to drive

racing cars in controlled environments. Ferrari also offers advanced driving courses to enhance customers' skills on the track.

In recent years, Ferrari has **expanded into the lifestyle and merchandising sector**, launching fashion collections that embody the brand's values of innovation, excellence, and performance. Additionally, Ferrari markets a range of luxury accessories, including watches, eyewear, and fragrances, available in Ferrari Stores both physically and online. Lastly, the company provides **financial and certification services**, such as Ferrari Financial Services, which offers leasing and financing options, and Ferrari Classiche, a restoration and certification service designed to preserve the authenticity and value of historic Ferrari models.

1.3. Headquarters

Ferrari's headquarters is divided into two main locations: its **legal headquarters in Amsterdam**, Netherlands, and its **operational headquarters in Maranello**, Italy. The company is **legally registered as Ferrari N.V.** in the Netherlands, a decision primarily driven by corporate governance and financial structuring considerations, as the country offers a favorable regulatory environment for multinational businesses. However, the true heart of Ferrari remains in Maranello, where the company has been based since 1943.

The Maranello headquarters serves as Ferrari's central hub for **automotive production, research & development, and motorsport operations**. This facility houses the brand's state-of-the-art factory, where its luxury sports cars and hypercars are meticulously assembled using advanced automation combined with traditional craftsmanship. Ferrari's production process is highly specialized, with a strong emphasis on customization, allowing customers to tailor their vehicles to their exact preferences. Additionally, Maranello is home to **Scuderia Ferrari**, the company's legendary Formula 1 team, which operates from its dedicated R&D, engineering, and race strategy departments. The site also includes Ferrari's wind tunnel and simulator, where new race cars are developed and tested before competing at the highest level of motorsport.

Beyond manufacturing and motorsport, Maranello also features the **Ferrari Museum** (Museo Ferrari Maranello), which attracts thousands of visitors each year. The museum showcases the brand's rich history, iconic models, and major achievements in racing, providing an immersive experience into Ferrari's legacy. Together, Ferrari's legal presence in Amsterdam and its operational base in Maranello reflect the company's global strategy, balancing corporate structure with its deep-rooted heritage in luxury automotive and motorsport excellence.

1.4. Company Size

In 2024, Ferrari reinforced its leadership in the luxury automotive industry, demonstrating strong performance across key dimensions such as sales, workforce expansion, and market value. The company reported **total shipments of 13,752 units**, marking a **0.7% increase** compared to the previous year. This growth was primarily driven by strong demand across various regions and an increase in high-margin vehicle personalizations, which continue to be a key revenue driver.

From a geographical perspective, the **United States remained Ferrari's largest market,**

with sales increasing by 12.9%, reflecting a strong and growing demand for luxury sports cars. The **Europe, Middle East, and Africa (EMEA) region accounted for the highest number of total shipments**, maintaining stable performance compared to the previous year. In contrast, **China, Hong Kong, and Taiwan experienced a 29% decline**, primarily due to economic uncertainties and shifting market dynamics. Despite this, Ferrari remains committed to long-term growth in Asia, focusing on brand positioning and targeted customer engagement strategies.

Ferrari's workforce also expanded, reaching **5,435 employees** by the end of 2024, an **8.96% increase** from the previous year. This reflects the company's ongoing investment in engineering, production, and corporate talent, supporting its commitment to technological innovation and operational excellence. To further strengthen its workforce, Ferrari announced plans to hire an additional 250 employees in early 2025.

In terms of financial strength, Ferrari continued to distinguish itself with a market capitalization of approximately €80 billion as of early 2025. This valuation places Ferrari ahead of several major automotive manufacturers, including BMW, Ford, General Motors, Mercedes-Benz, Porsche, Stellantis, and Volkswagen, underscoring its exclusive brand positioning and strong investor confidence. The company's ability to sustain high profitability margins, strong pricing power, and controlled production volumes remains a key factor in its **long-term success**. Additionally, **hybrid models accounted for 48% of total shipments, highlighting Ferrari's strategic shift** toward electrification and future mobility solutions.

1.5. Financial Performace

In 2024, Ferrari demonstrated outstanding financial performance, particularly in revenues and EBITDA, further solidifying its position as a leader in the luxury automotive industry. The company reported **net revenues of €6.677 billion**, reflecting an **11.8% year-over-year increase**. This growth was fueled by an enriched product mix, as well as a strong demand for vehicle personalization, which remains a key revenue driver. Additionally, Ferrari benefited from a positive geographical sales mix, particularly in the Americas, where strong demand further contributed to revenue growth.

In terms of profitability, **EBITDA** reached **€2.555 billion**, marking a **12.1% increase** from the previous year, with a robust **EBITDA margin of 38.3%**. Ferrari also reported a significant rise in operating profit (**EBIT**), which reached €1.888 billion, up 16.7% year-over-year, resulting in an EBIT margin of 28.3%. This strong operational performance translated into a **net profit of €1.526 billion**, reflecting an impressive **21.3% increase** compared to 2023.

The company's industrial **free cash flow** generation remained strong, reaching **€1.027 billion**, demonstrating Ferrari's ability to efficiently convert its earnings into liquidity. The financial structure remains solid, with a net industrial cash position of €1.669 billion, ensuring financial flexibility for future investments and innovation. Additionally, Ferrari's **sponsorship, commercial agreements, and brand activities generated €670 million in revenue, up 17.1% from the previous year**, driven by new sponsorships and lifestyle initiatives.

These financial results highlight Ferrari's pricing power, brand exclusivity, and strong demand for high-value vehicles, reinforcing its ability to maintain high margins despite a competitive and evolving market landscape. With a clear focus on product excellence, personalization, and

brand expansion into lifestyle sectors, Ferrari is well-positioned for continued success in the luxury automotive and high-end experience markets.

1.6. Stock Market

As of March 13, 2025, Ferrari N.V. (ticker: RACE) maintains a **market capitalization** of approximately **$78.5 billion**, positioning it among the most valuable automotive brands. The company's **stock price is $440.66 per share**, with a 52-week high of $509.13 and a low of $399.27, reflecting market fluctuations. Ferrari has **193.92 million shares outstanding**, with a public float of 126.66 million shares.

Over the past decade, Ferrari's market value has grown significantly, rising from $11.54 billion in 2015 to over $80 billion in 2025, representing a **compound annual growth rate (CAGR) of approximately 24%**. The company's stock has shown strong long-term performance, nearly doubling over the last five years, supported by high demand, limited production volumes, and strong financials.

Ferrari's price-to-earnings (**P/E**) ratio stands at **47.73 (trailing) and 45.45 (forward)**, indicating strong investor expectations for continued profitability. Its price-to-sales (**P/S**) ratio is **10.89**, and the price-to-book (**P/B**) ratio is **21.35**, reflecting Ferrari's premium market valuation. The company's ability to sustain high margins, driven by exclusive vehicle production, personalization programs, and strong brand appeal, has been a key factor in maintaining investor confidence.

2 | Corporate Governance

2.1. Governance Bodies

Ferrari N.V. operates within a structured corporate governance framework, with the **Board of Directors** at the core of its strategic oversight and decision-making processes. In accordance with the articles of association, the Board consists of at least three members, with the current composition appointed on April 17, 2024, during the annual general meeting of shareholders. This mandate will expire at the next annual general meeting, expected on April 16, 2025, with the possibility of reappointment for its members. The Board is composed of two *Executive Directors*, **Mr. John Elkann**, serving as *Executive Chairman*, and **Mr. Benedetto Vigna**, as *Chief Executive Officer*, alongside nine *non-executive Directors*. The authority to represent the company is vested in both the Board of Directors and the Chief Executive Officer, with the latter also holding responsibility for the day-to-day management of Ferrari N.V. and its subsidiaries. To support the Board in its governance and operational oversight, three key internal committees have been established: the **Audit Committee**, the **Compensation Committee**, and the **ESG Committee**, each operating under delegated authority and playing a crucial role in ensuring financial integrity, executive remuneration policies, and corporate sustainability strategy.

The **Audit Committee** is entrusted with the fundamental task of ensuring the integrity of Ferrari N.V.'s financial reporting and risk management. Its role extends beyond financial statement oversight, encompassing internal control mechanisms, tax policies, corporate financing strategies, and compliance with legal and regulatory requirements. The committee is also responsible for assessing the effectiveness of both internal and external audits, evaluating risk management guidelines, and monitoring the implementation of the company's ethics and compliance program. Given the increasing importance of digital security, the Audit Committee has also been assigned the task of overseeing the company's application of information and communication technology, with a specific focus on cybersecurity governance. In this regard, the Head of Enterprise Cybersecurity and the Chief Digital Transformation Officer (CDTO) present an annual report to the committee, ensuring continuous monitoring of risks related to digital infrastructure and data security.

In line with corporate governance best practices, the Audit Committee is composed of at least three non-executive directors, all of whom must be independent under the Dutch Corporate Governance Code. The current members are **Mr. Sergio Duca** *(Chairperson)*, **Ms. Francesca Bellettini**, and **Ms. Maria Patrizia Grieco**, with Mr. Duca designated as the audit committee financial expert as required by the Sarbanes-Oxley Act and U.S. Securities and Exchange Commission (SEC) regulations.

The **Compensation Committee** plays an essential role in defining Ferrari N.V.'s executive remuneration policies, ensuring alignment with corporate strategy and regulatory requirements. Its responsibilities extend to determining compensation structures for executive directors, overseeing salary and performance-based incentives, and administering equity incentive plans and deferred compensation benefit programs. Furthermore, the committee evaluates the company's compensation policies in relation to corporate performance and governance, issuing recommendations where necessary and preparing the annual compensation report, which provides transparency on executive pay structures and their alignment with shareholder interests. The Compensation Committee is composed of at least three non-executive directors, with at most one member not required to meet the Dutch Corporate Governance Code's independence criteria. The current members are **Mr. John Galantic** *(Chairperson)*, **Mr. Eddy Cue**, and **Mr. Piero Ferrari**, all of whom are non-executive directors.

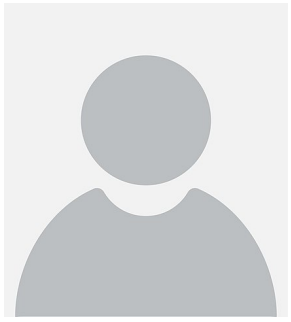
The **ESG Committee** is responsible for overseeing Ferrari's corporate governance, sustainability initiatives, and leadership selection processes. Its duties include defining criteria for board member selection and appointment procedures, conducting periodic assessments of board composition and performance, and providing recommendations for director nominations. Beyond governance matters, the committee plays a crucial role in shaping Ferrari's global sustainability strategy, monitoring ESG-related initiatives, evaluating progress towards sustainability goals, and ensuring transparent disclosure of the company's environmental and social impact. The ESG Committee is composed of at least three directors, with the majority required to be independent and no more than one member being an executive director. The current members are **Mr. John Elkann** *(Chairperson)*, **Mrs. Delphine Arnault**, and **Mr. Eddy Cue**, with Mr. Elkann being the sole executive director on the committee, while the remaining members meet the independence requirements.

2.2. Board of Directors

At the helm of the Board is **John Elkann**, who has served as Ferrari's **Chairman** since 2018. His leadership extends beyond Ferrari, as he is also the **Chief Executive Officer of EXOR** and **Chairman of Stellantis N.V.**, positioning him as a key figure in the strategic direction of multiple global corporations. With a strong background in industrial growth and investment strategy, Elkann has played a central role in preserving Ferrari's exclusivity while steering the company towards innovation in electrification and digital transformation. While his understanding of **cyber risk management** is primarily strategic, he relies on dedicated cybersecurity leaders and advisory committees to guide Ferrari's risk mitigation initiatives.

Benedetto Vigna, Ferrari's **Chief Executive Officer (CEO)**, is an executive whose expertise in semiconductor technology and microelectronics has significantly influenced the company's approach to digital transformation. Prior to joining Ferrari in 2021, Vigna spent decades at *STMicroelectronics*, where he pioneered sensor technologies widely utilized in automotive applications. His in-depth knowledge of **digital ecosystems, artificial intelligence, and connectivity** makes him one of the Board's most technologically adept members. His strong **cybersecurity acumen**, particularly in **data encryption and automotive digitalization**, is instrumental in shaping Ferrari's cybersecurity strategy as the company integrates increasingly sophisticated digital solutions into its vehicles and operational infrastructure.

Among the non-executive directors, **Piero Ferrari** remains a cornerstone of the company's heritage and innovation. As the only living son of Mr. Enzo Ferrari, his extensive experience in **engineering and motorsport** ensures that Ferrari's legacy is preserved while embracing cutting-edge developments in high-performance automotive technology. While his focus is primarily on **product development and racing innovation**, he actively contributes to discussions on **intellectual property protection** and **technology confidentiality**, areas closely linked to cybersecurity.



Sergio Duca, an experienced **corporate auditor** and **financial expert**, chairs Ferrari's Audit Committee, where he is responsible for overseeing the company's **financial transparency, compliance, and risk management**. His expertise in **fraud prevention** and **financial data security** ensures that Ferrari adheres to stringent regulatory frameworks. While his knowledge of cybersecurity is rooted in financial governance, his role is vital in ensuring **data integrity** and **cybersecurity compliance** across Ferrari's financial and operational structures.

Delphine Arnault, as a leading figure in the **luxury industry** and **CEO of Christian Dior Couture**, contributes strategic insights into Ferrari's **brand positioning** and **consumer engagement**. While her direct involvement in **cybersecurity** is limited, her understanding of **digital commerce fraud prevention** and **brand protection** in online environments adds value to Ferrari's cybersecurity discourse, particularly as the company expands its digital presence.

Eddy Cue, **Apple's Senior Vice President of Services**, brings a unique technological perspective to the Board. As one of the leading figures behind Apple's digital ecosystem, Cue is well-versed in **cybersecurity, encryption technologies, and AI-driven security solutions**. His deep knowledge of **digital platforms, user authentication systems, and cloud security** provides Ferrari with critical expertise in securing **connected car technologies, digital services, and data privacy frameworks**. His role is particularly relevant as Ferrari integrates **over-the-air (OTA) software updates, and cloud-based customer services** into its product offerings.

Maria Patrizia Grieco, a seasoned corporate leader with extensive experience in **energy** and **financial services**, strengthens Ferrari's cybersecurity governance with her background in regulatory compliance and risk assessment frameworks. Her experience overseeing **cybersecurity policies in multinational organizations** ensures that Ferrari aligns with best practices in **data protection and governance**.

Francesca Bellettini, a seasoned executive in the luxury and financial sectors, has been the **Deputy Chief Executive Officer of Kering** since July 2023 and the **President and CEO of Yves Saint Laurent** since 2013. As a member of Kering's Group Executive Committee since 2013, she plays a crucial role in shaping the strategic direction of one of the world's leading luxury conglomerates.
Her professional background extends beyond the luxury industry, with early career **experience in investment banking** at *Compass Partners International, Deutsche Morgan Grenfell, and Goldman Sachs International.*

Adam Keswick has held multiple strategic positions within Jardine Matheson, including **Group Strategy Director** and **Group Managing Director of Jardine Cycle & Carriage (2003–2007)**, shaping the company's long-term vision across various industries. In addition to his role at Ferrari, he is a director of *Hongkong Land, Mandarin Oriental, and the Yabuli China Entrepreneurs Forum*. While his expertise primarily lies in corporate strategy and investment management, his governance experience ensures a strong oversight on **risk management and business resilience**, key aspects in Ferrari's approach to digital security and corporate sustainability.

John Galantic, is the **Chief Executive Officer of Tod's Group**. With a career spanning **Procter & Gamble, GlaxoSmithKline, Coty**, and nearly two decades at **Chanel**, where he served as **COO of Chanel Inc.** and **Board Member of Chanel Ltd.**, he has shaped global luxury brands through **strategic leadership** and **digital innovation**. His expertise in **brand positioning, data-driven marketing, and consumer engagement** strengthens Ferrari's approach to digital transformation and cybersecurity, ensuring the brand's exclusivity remains safeguarded in an increasingly connected world.

Mike Volpi, a prominent venture capitalist and technology executive, is a **General Partner at Index Ventures**, where he has led the firm's **North American expansion** since 2009. Specializing in enterprise software and artificial intelligence, he serves on the boards of *Aurora, Confluent, ClickHouse, Scale, Sonos, and Wealthfront*, among others. Prior to joining Index Ventures, Volpi was **Chief Strategy Officer and SVP/GM of Cisco's routing business**. His expertise in **strategic innovation, digital infrastructure**, and **cybersecurity investments** contributes to Ferrari's approach to **technological resilience** and **risk management** in an increasingly connected landscape.

2.3. Board Skills

Skill Area	Corporate governance and risk management	Financial and accounting	Corporate management	Digital and cybersecurity	Innovation	ESG	Automotive and motorsport industry knowledge	Luxury goods industry knowledge
John Elkann (Executive Chairman and Executive Director)	x	x	x		x	x	x	x
Benedetto Vigna (Chief Executive Officer)	x		x	x	x	x	x	x
Piero Ferrari (Vice Chairman and non-Executive Director)	x		x				x	x
Sergio Duca (Senior Non-Executive Director)	x	x	x			x	x	
Delphine Arnault (Non-Executive Director)	x	x	x			x		x
Francesca Bellettini (Non-Executive Director)	x	x	x					x
Eddy Cue (Non-Executive Director)	x		x	x	x	x		
John Galantic (Non-Executive Director)	x		x			x		x
Maria Patrizia Grieco (Non-Executive Director)	x	x	x			x	x	
Adam Keswick (Non-Executive Director)	x	x	x				x	
Mike Volpi (Non-Executive Director)	x		x	x	x		x	

Figure 2.1: Board Skills Area

Directors	Nationality	Executive	Non Executive	Independent		Committees			Directors first term from [1]	Directors current term from	Roles in other listed companies [4]
				NYSE Rules	Dutch Code	Audit	Compensation	ESG			
John Elkann (Executive Chairman and Executive Director)	IT	x						x	April 15, 2016 [2]	April 17, 2024	3
Benedetto Vigna (Chief Executive Officer)	IT	x							September 16, 2021 [3]	April 17, 2024	0
Piero Ferrari (Vice Chairman)	IT		x	x			x		January 2, 2016	April 17, 2024	0
Sergio Duca (Chair of the Board and Senior Non-Executive)	IT		x	x	x	x			January 2, 2016	April 17, 2024	0
Delphine Arnault	FR		x	x	x			x	April 15, 2016	April 17, 2024	2
Francesca Bellettini	IT		x	x	x	x			April 16, 2020	April 17, 2024	0
Eddy Cue	US		x	x	x		x	x	January 2, 2016	April 17, 2024	0
John Galantic	US, CH		x	x	x		x		April 16, 2020	April 17, 2024	0
Maria Patrizia Grieco	IT		x	x	x	x			April 15, 2016	April 17, 2024	2
Adam Keswick	UK		x	x	x				April 15, 2016	April 17, 2024	1
Mike Volpi	US		x	x	x				April 14, 2023	April 17, 2024	3

Figure 2.2: Composition of Ferrari's Board of Directors, showing roles, committees, and tenure

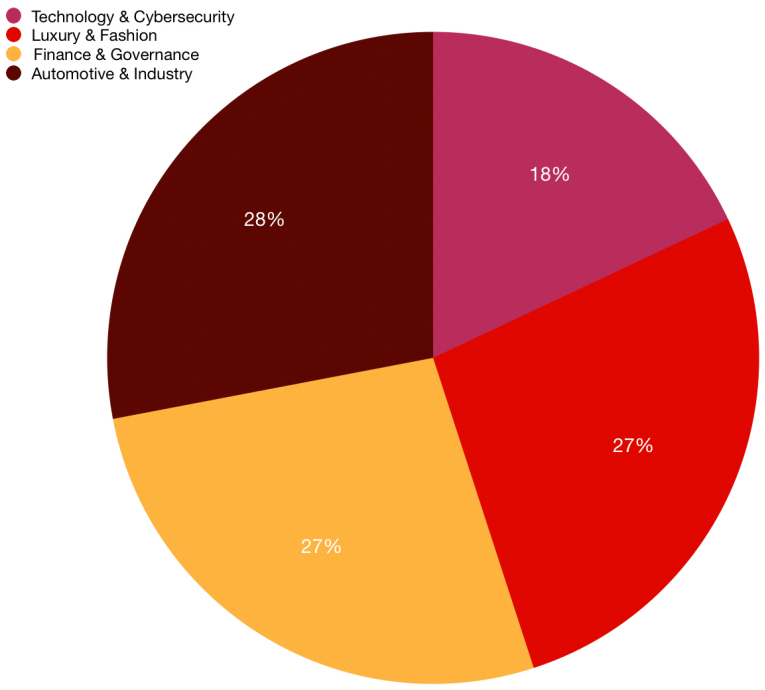


Figure 2.3: Distribution of Ferrari Board Members' industry backgrounds

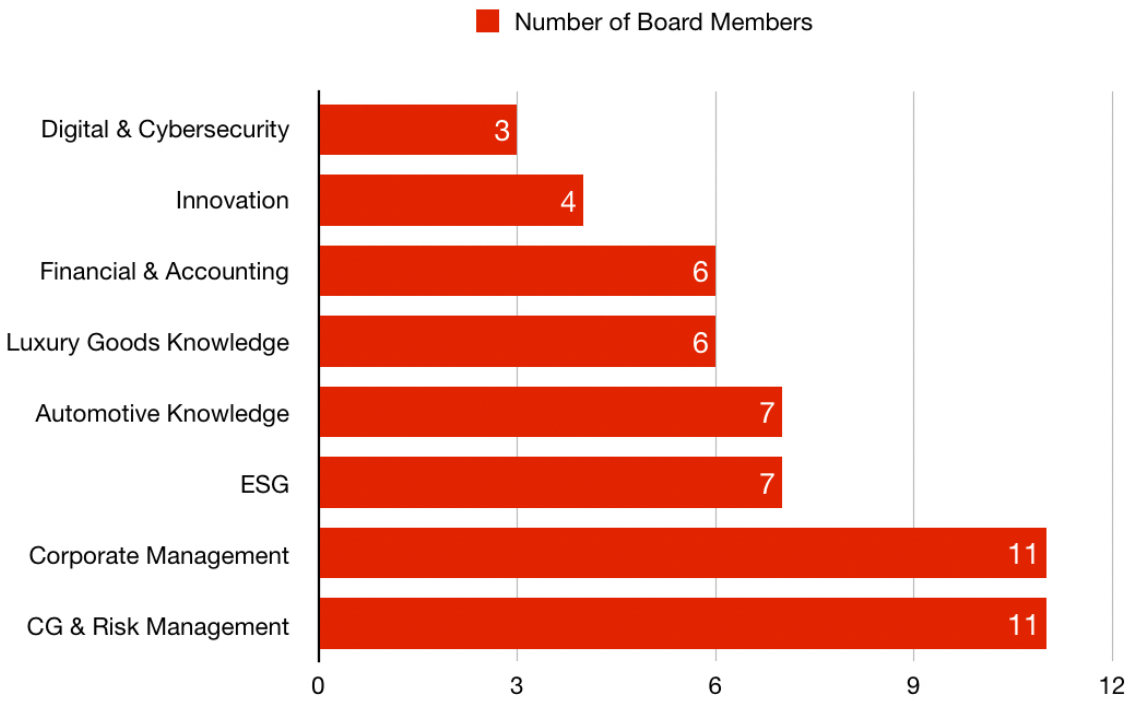


Figure 2.4: Competencies of Ferrari's Board Members across key strategic areas

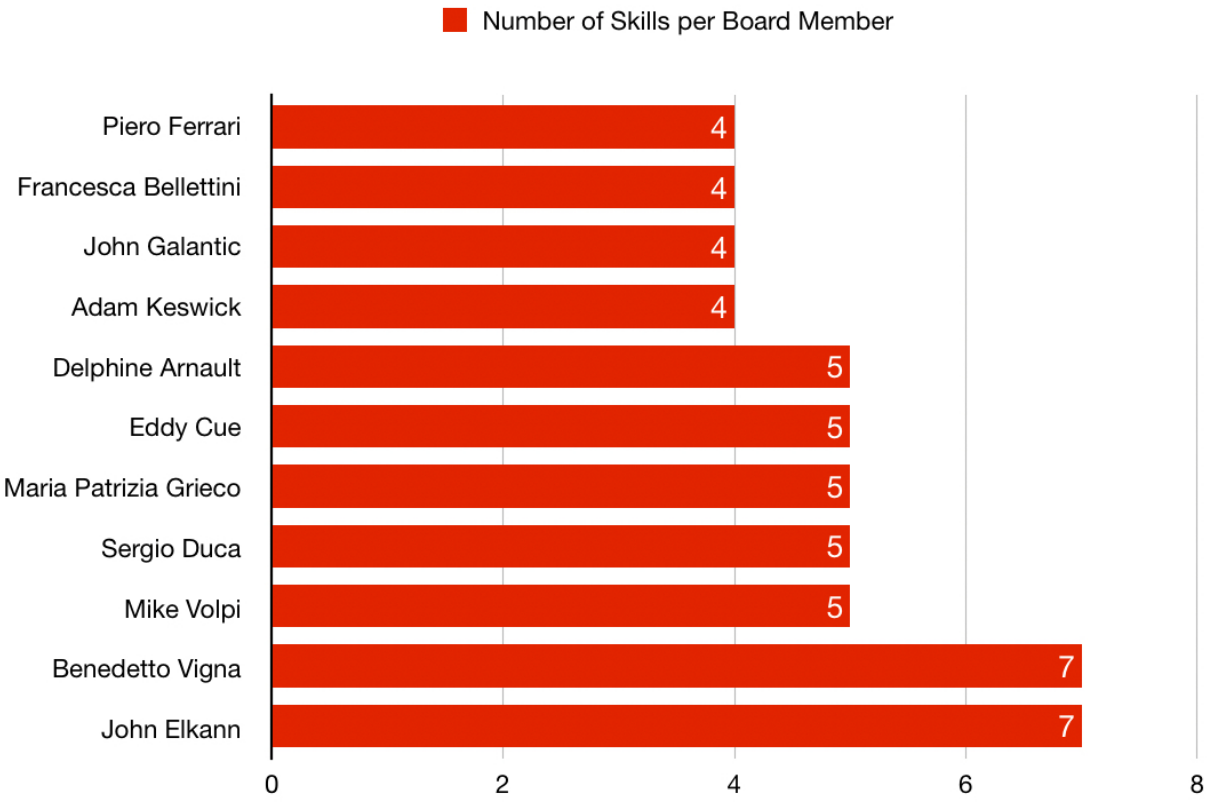


Figure 2.5: Number of skills per Ferrari Board Member

3 | Corporate Strategy

3.1. Cyber Strategy and Digitalization

Ferrari's corporate vision is deeply rooted in its core values, which guide its strategic decisions and define its brand identity as a leader in the luxury automotive industry. The company embraces three fundamental values: **Individual and Team, Tradition and Innovation, and Passion and Achievement**. "Individual and Team" reflects the balance between personal excellence and collective effort, emphasizing how Ferrari's employees work together to achieve extraordinary results. "Tradition and Innovation" underscores the company's ability to evolve by integrating groundbreaking technology while staying true to its heritage and craftsmanship. "Passion and Achievement" represents the relentless pursuit of excellence and success, both in racing and in the production of world-class automobiles. While these principles shape Ferrari's long-term vision, the company does not explicitly define a dedicated cyber vision statement. The absence of such a statement highlights the need for Ferrari to establish a clearer direction in cybersecurity, ensuring that its risk management framework aligns with its innovation-driven business model.

Despite not having an explicitly stated cyber vision, Ferrari has developed a detailed cybersecurity strategy embedded within its Enterprise Risk Management framework. The company recognizes that cybersecurity risks encompass a wide range of potential threats, including data breaches, intellectual property theft, fraud, regulatory non-compliance, and disruptions to operational and technical infrastructure. To mitigate these risks, Ferrari has implemented a comprehensive cybersecurity strategy that prioritizes proactive identification, detection, and response to potential threats. The company has stated that *"cybersecurity risks related to our business, technical operations, privacy and compliance issues including any Ferrari confidential information about vehicles, services, projects and all non-public activities related to Racing Department, employees, clients and fans' personal data are identified and addressed through a multi-faceted approach."* This approach includes advanced penetration testing, red-teaming exercises, and phishing simulations to evaluate the organization's cyber resilience. Additionally, Ferrari conducts regular cybersecurity audits and employs third-party security analysts to assess vulnerabilities and ensure compliance with industry standards.

Ferrari follows a structured incident response and breach management process that includes four interconnected stages: **preparation, detection and analysis, containment and recovery, and post-incident review**. The company maintains a Cyber Crisis Committee that is responsible for handling significant cyber threats, ensuring that response measures are efficiently coordinated among key business functions. Ferrari has also implemented a cyber insurance policy to mitigate the financial impact of cyber incidents, covering damages caused by hacking, system failures, and data breaches. Moreover, cybersecurity risks associated with third-party

suppliers and dealers are addressed through a rigorous evaluation process, where suppliers are required to undergo cybersecurity assessments and audits. Those that fail to meet Ferrari's standards must implement corrective measures before securing contracts with the company.

While Ferrari has made significant strides in enhancing its cybersecurity framework, its broader digital strategy remains focused on digitalization rather than a full-scale digital transformation. **Digitalization** at Ferrari refers to the strategic adoption of digital tools to optimize efficiency, enhance customer experience, and support innovation without fundamentally altering the company's core business model. One of the most notable digital initiatives is the establishment of the **E-Building in Maranello**, a cutting-edge manufacturing facility designed to support Ferrari's transition toward electrification. This facility incorporates smart production technologies and digitalized workflows, reinforcing Ferrari's commitment to sustainable innovation.

A crucial element of Ferrari's digitalization efforts is the role of the **Chief Digital Transformation Officer (CDTO)**, a position created to oversee the company's technological evolution and cybersecurity strategy. The CDTO reports directly to the CEO and is responsible for ensuring that Ferrari's digital investments align with its corporate objectives while mitigating cyber risks. The necessity of this role is driven by both internal and external factors. Internally, the CDTO coordinates cybersecurity governance across multiple business units, ensuring that IT, operational technology (OT), and vehicle cybersecurity are integrated into Ferrari's broader risk management framework. Externally, the role is essential for maintaining compliance with stringent regulatory requirements, such as the **UNECE R155 automotive cybersecurity standard** and data protection laws like GDPR. Additionally, as Ferrari expands its connected vehicle services, including over-the-air (OTA) software updates and AI-driven vehicle enhancements, the CDTO plays a critical role in ensuring that these technologies are developed with robust cybersecurity protections.

Ferrari's cybersecurity strategy is primarily **cascaded rather than fully embedded**, meaning that security policies and protocols are implemented through top-down governance rather than being inherently integrated into every aspect of product development. While Ferrari has taken significant steps to strengthen its cyber resilience, the absence of a dedicated cyber vision statement suggests an opportunity to further align cybersecurity with its long-term strategic goals. Establishing a clearly defined cyber vision would enhance Ferrari's ability to proactively address emerging threats and reinforce its commitment to innovation and security in the digital age. Furthermore, as the company continues to expand its use of digital technologies, refining its cybersecurity framework will be essential to protecting both its brand reputation and its customers' trust.

3.2. Current and Future Crown Jewels

Ferrari's **crown jewels** represent the company's most valuable assets, encompassing both its current competitive strengths and the future pillars that will shape its long-term success. These assets define Ferrari's market position, brand identity, and strategic direction, ensuring its continued dominance in the luxury automotive and motorsport industry.

At the core of Ferrari's **current crown jewels** lies its unparalleled **brand value and heritage**. Ferrari is synonymous with exclusivity, craftsmanship, and prestige, qualities that have cultivated a fiercely loyal customer base and sustained the company's ability to command premium pricing for its vehicles. The strength of the Ferrari brand is reinforced by its limited

production strategy, ensuring demand consistently exceeds supply. This scarcity not only protects the brand's desirability but also enhances the residual value of Ferrari models, making them not just luxury items but also highly sought-after investments. Beyond financial value, Ferrari's *heritage* is deeply ingrained in a legacy of engineering excellence and innovation, elements that continue to attract new generations of enthusiasts while maintaining its historic clientele.

Another key asset is Ferrari's **motorsport dominance**, particularly in *Formula 1 (F1)* and endurance racing. As the most successful team in F1 history, Ferrari's participation in the sport transcends competition, serving as a vital marketing tool and technological incubator. Every innovation developed in F1, from aerodynamics to hybrid powertrains, contributes directly to Ferrari's road cars, reinforcing the synergy between competition and commercial production. In endurance racing, Ferrari's participation in the *World Endurance Championship (WEC)* and its recent success at *Le Mans* reaffirm its position as a leader in high-performance engineering. Motorsport success not only enhances brand prestige but also drives continued advancements in aerodynamics, hybrid systems, and materials science, ensuring Ferrari remains at the forefront of automotive performance.

Ferrari's expertise in **high-performance engineering** further solidifies its position as an industry leader. The company's commitment to *internal combustion engine (ICE)* excellence, particularly through its **V12 and hybrid technologies**, is a key differentiator. The naturally aspirated V12, a hallmark of Ferrari's identity, continues to embody the pinnacle of mechanical precision and driving emotion. Simultaneously, the introduction of hybrid technology, such as in the *SF90 Stradale*, represents a strategic balance between traditional performance and regulatory adaptation. These engineering triumphs have allowed Ferrari to maintain a unique value proposition, combining technological sophistication with the visceral experience that defines the brand.

While these current assets remain the foundation of Ferrari's strength, the company is also actively investing in **future crown jewels** to secure its leadership in a rapidly evolving industry. One of the most significant transformations underway is Ferrari's commitment to **electrification and technological advancements**. The company has officially announced the launch of its **first fully electric vehicle (EV)** in 2025, a historic milestone that will mark Ferrari's expansion into the high-performance electric segment. Unlike mass-market EV manufacturers, Ferrari's approach is expected to maintain the exclusivity and performance standards that define its brand, ensuring that electrification enhances rather than dilutes the driving experience. The development of proprietary battery technology, lightweight structures, and innovative electric powertrains will be critical to ensuring that Ferrari's EV offerings align with its legacy of uncompromised performance.

Alongside product innovation, Ferrari's future in **motorsport remains a crucial element** of its strategy. The company's renewed focus on reclaiming dominance in *Formula 1*, highlighted by the recent signing of seven-time world champion **Lewis Hamilton**, signifies a clear ambition to return to the top of the sport. This move not only enhances Ferrari's competitive standing but also strengthens its commercial appeal, as F1 success directly translates to heightened brand exposure and increased demand for road cars. Furthermore, Ferrari's continued commitment to the *WEC* and its prototype racing programs demonstrates an integrated approach to endurance competition, reinforcing its reputation as a leader in cutting-edge automotive technology.

Beyond traditional automotive ventures, Ferrari is expanding its **strategic partnerships and**

market reach. The recently signed **engine supply agreement with Cadillac** for its upcoming *Formula 1 entry in 2026* positions Ferrari as a key powertrain supplier in the evolving motorsport landscape. This partnership underscores Ferrari's engineering expertise and broadens its influence beyond its own racing team. Additionally, Ferrari's **lifestyle and brand diversification initiatives** aim to capitalize on its ultra-luxury positioning. With plans to double lifestyle-related sales by 2026, the company is investing in exclusive brand experiences, high-end merchandise, and limited-edition collaborations to strengthen its presence beyond the automotive industry. This strategic diversification aligns with Ferrari's vision of becoming a holistic luxury brand while maintaining its automotive excellence.

Ferrari's **crown jewels, both present and future**, encapsulate a legacy of unparalleled performance, brand prestige, and relentless innovation. While the company continues to leverage its existing strengths, it is simultaneously charting a course for the future through **electrification, motorsport ambitions, and strategic brand expansion**. These initiatives ensure that Ferrari remains a dominant force in the luxury automotive sector, seamlessly blending heritage with forward-thinking technological advancements. The ability to preserve its core values while embracing the opportunities of a changing industry will be the key to Ferrari's sustained success in the years to come.

3.3. Goals and Objectives

Ferrari's strategic goals and objectives align with its vision for sustained growth, innovation, and leadership in the luxury automotive and motorsport sectors. These objectives are structured along a defined **timeline**, balancing short-term performance targets with long-term sustainability and technological advancements.

In the **short-term (1-2 years)**, Ferrari is committed to launching its **first fully electric vehicle (EV) by 2025**, marking a pivotal step in the company's electrification journey. This initiative aligns with Ferrari's dedication to technological innovation while preserving the brand's core identity of high-performance engineering. Additionally, Ferrari aims to surpass **€7 billion in revenue**, capitalizing on strong demand, product personalization, and brand diversification. Alongside financial growth, Ferrari continues to optimize **digitalization and customer experience**, ensuring that its digital platforms, retail interactions, and online services reflect the brand's exclusivity and customer-centric approach.

In the **long-term (3-10 years)**, Ferrari is working towards **achieving carbon neutrality by 2030**. This ambitious goal reflects the company's commitment to sustainability, with continued investment in hybridization, electrification, and energy-efficient production processes. Furthermore, Ferrari will advance **hybrid and EV technologies** to sustain its position as the leader in high-performance automotive engineering. By leveraging cutting-edge battery innovation and aerodynamics, Ferrari aims to ensure that future models retain the exhilarating driving dynamics synonymous with the brand. Beyond product development, Ferrari seeks to **maintain its motorsport dominance**, reinforcing its presence in Formula 1 and endurance racing while translating track innovations into road cars.

By pursuing these goals, Ferrari aims to fortify its legacy as a leader in automotive excellence, ensuring that future advancements in electrification, sustainability, and motorsport innovation remain aligned with its heritage and performance-driven philosophy.

4 | Compliance System

As underlined in Ferrari's **Code of Conduct** [7], Ferrari is committed to upholding the highest **standards of integrity, transparency, and ethical business practices** across its global operations. The company has established a robust **compliance framework** covering key areas such as **anti-corruption** [5], **antitrust** [6], **third-party compliance** [10], **tax strategy** [13], **environmental responsibility** [8], **human rights** [9], and **data protection** [11]. These policies ensure adherence to international regulations while reinforcing Ferrari's commitment to sustainable growth and corporate responsibility.

Cyber risks directly impact Ferrari's compliance obligations, requiring stronger security measures, third-party oversight, and proactive monitoring to safeguard Ferrari's operations, reputation, and regulatory standing.

4.1. Data Protection

Ferrari complies with global data protection laws, including GDPR (EU, UK), CCPA, and other relevant regulations. The company has established a Privacy Organizational Structure, with a Privacy Committee and a Data Protection Officer (DPO) responsible for ensuring GDPR compliance. Ferrari has specific privacy policies for its workforce, which apply to all employees and subsidiaries worldwide, with local privacy notices for each jurisdiction. The company prioritizes data protection, handling personal and sensitive data in a safe, transparent, and legitimate manner.

Personal data is processed with the highest level of confidentiality for purposes like vehicle orders, marketing, profiling, and customer relationship management. Ferrari's policies apply to all stakeholders, ensuring fairness and transparency in data usage without discriminating against any individual or group. Data protection is integrated into Ferrari's Human Rights Practice, ensuring compliance with privacy laws and safeguarding personal data across operations.

Data breaches, hacking, and insider threats can expose customer, employee, and proprietary data, leading to violations, regulatory fines, and reputational damage. To mitigate this, Ferrari must continuously monitor cybersecurity threats, encrypt sensitive data, and strengthen access controls.

4.2. Third-Party Compliance

Ferrari's compliance framework extends to all third parties it engages with, including dealers, suppliers, agents, consultants, and joint venture partners. The company enforces strict ethical, legal, and transparency standards for all third parties to protect its business integrity,

reputation, and legal standing.

Key measures include:

- **Pre-engagement Compliance Evaluation**: Assessments of financial stability, ethical reliability, and adherence to anti-corruption, anti-money laundering, and international sanctions laws.
- **Contractual Obligations**: Require third parties to comply with Ferrari's Code of Conduct and relevant compliance policies.
- **Monitoring & Audits**: Ensure continued compliance, and reserve the right to terminate relationships if violations occur.
- **Training & Awareness**: Help third parties understand and uphold Ferrari's compliance expectations.
- **Whistleblowing & Disciplinary Actions**: Allow reporting any breaches confidentially, with protections against retaliation.

Ferrari's suppliers and external partners may have weaker cybersecurity, making them entry points for supply chain attacks. To mitigate this, Ferrari must constantly enforce cybersecurity standards in contracts, conduct rigorous assessments, and ensure data-sharing practices.

4.3. Antitrust Compliance

Ferrari is committed to fair competition and full compliance with global antitrust laws, including EU competition regulations, U.S. antitrust laws, and equivalent laws in other jurisdictions. The company recognizes that violations can lead to severe financial penalties, legal consequences, reputational harm, and even criminal liability for individuals involved.

Key aspects of Ferrari's antitrust compliance include:

- **Prohibition of Anti-Competitive Practices**: Ferrari forbids anti-competitive agreements, price-fixing, bid-rigging, market allocation, and the abuse of dominant market positions.
- **Guidelines on Competitor and Customer Interactions**: Employees must avoid discussing prices, production volumes, market divisions, or exchanging sensitive business information with competitors.
- **Supply Chain & Distribution Compliance**: Ferrari ensures that its dealers, distributors, and suppliers comply with competition laws, avoiding practices like resale price maintenance or unfair trade restrictions.
- **Monitoring and Enforcement**: The company's Group Compliance Department oversees the implementation of the antitrust policy, provides training, conducts audits, and ensures that all employees and third parties act in compliance with the rules.
- **Whistleblowing & Disciplinary Actions**: Employees and stakeholders are encouraged to report any suspected violations, with Ferrari guaranteeing confidentiality and protection against retaliation.

Unauthorized data sharing or cyber espionage can result in competitor price-fixing, market manipulation, or insider trading risks. Cyberattacks could also compromise Ferrari's competitive strategies. Ferrari must protect market-sensitive information, monitor internal communications, and prevent cyber-enabled antitrust violations.

4.4. Environmental Compliance

Ferrari is committed to sustainable business practices, aiming to minimize its environmental impact while ensuring long-term business success. The company integrates environmental responsibility into all aspects of its operations and expects the same commitment from its suppliers, partners, and third parties.

Key Commitments:

- **Reducing Greenhouse Gas Emissions**: Ferrari is actively working on lowering its carbon footprint by optimizing its production processes, increasing energy efficiency, and adopting low-emission fuels and renewable energy sources.
- **Water & Waste Management**: The company prioritizes water conservation, recycling, and circular economy principles, aiming to minimize waste and maximize material reuse.
- **Value Chain & Supplier Engagement**: Suppliers must also comply with sustainability requirements
- **Transparency**: Ferrari follows all environmental laws and regulations while maintaining open communication with authorities and communities.
- **Training & Awareness**: Employees receive environmental training, and a sustainability culture is promoted across all departments
- **Whistleblowing & Disciplinary Actions**: The company has dedicated whistleblowing channels for reporting environmental violations and applies disciplinary actions for non-compliance

Cyberattacks on smart grids, energy management systems, or emissions control data could lead to inaccurate sustainability reporting or regulatory non-compliance. Ferrari must secure environmental data systems, prevent tampering with sustainability metrics, and safeguard regulatory reporting platforms.

4.5. Human Rights Compliance

Ferrari is committed to respecting, protecting, and promoting human rights across all aspects of its business, including employees, suppliers, partners, and local communities. The Human Rights Practice, aligned with Ferrari's Code of Conduct, outlines the company's approach to fostering a responsible and ethical work environment while ensuring compliance with international human rights standards such as the UN Guiding Principles on Business and Human Rights, ILO conventions, and OECD guidelines.

Key Commitments:

- **Workplace Rights**: Ensuring fair, inclusive, and safe working conditions - prohibiting forced labor, child labor, and discrimination.
- **Freedom of Association & Collective Bargaining**: Employees have the right to join unions and negotiate working conditions without interference.
- **Diversity & Equal Opportunities**: Ferrari promotes a culture of inclusion, ensuring fair treatment based on merit.
- **Health & Safety**: Strong focus on workplace safety, well-being programs, and maintaining high occupational health standards.
- **Fair Wages & Benefits**: Commitment to equal pay, competitive compensation, and social welfare initiatives.
- **Whistleblowing & Disciplinary Actions**: Confidential reporting mechanisms are in place, with strict actions taken against human rights violations.

Cyberattacks on HR databases can expose sensitive employee data, diversity metric, or workplace conditions, leading to legal risks and reputational harm. Ferrari must protect HR systems from data breaches, enforce ethical AI use in workforce management, and prevent cyber-enabled human rights violations.

4.6. Anti-corruption

Ferrari is committed to the highest standards of integrity and transparency, enforcing strict anti-corruption measures across its global operations. The policy ensures compliance with major international anti-corruption laws, including the Italian Legislative Decree 231/2001, the U.S. Foreign Corrupt Practices Act (FCPA), the UK Bribery Act, and OECD anti-bribery conventions.

Key Commitments:

- **Bribery & Corruption**: Ferrari prohibits any form of bribery, kickbacks, or improper payments to public officials or private entities.
- **Gifts & Hospitality**: Any gifts or business courtesies must be modest, transparent, and not aimed at influencing decisions.
- **Internal Oversight**: A Group Compliance Function monitors anti-bribery efforts, reports to top management, and ensures adherence through audits and risk assessments.
- **Training & Awareness**: Employees receive mandatory training on corruption risks, ethical decision-making, and compliance best-practices.
- **Whistleblowing & Disciplinary Actions**: Ferrari has confidential reporting channels for bribery concerns, with strict protection against retaliation and penalties for violations.

Attackers could manipulate financial records, impersonate executives, or exploit security gaps for fraud and bribery schemes. Ferrari must monitor financial transactions, implement anti-fraud cybersecurity controls, and strengthen identity verification for high-risk activities.

4.7. Tax Strategy

Ferrari is committed to full compliance with global tax laws, ensuring that taxes are paid ethically and transparently in the jurisdictions where the company operates. The strategy, approved by the Board of Directors, aligns with Ferrari's Code of Conduct and is overseen by the Audit Committee to maintain high integrity in tax management.

Key Principles:

- **Integrity & Transparency**: Ferrari embraces both the letter and the spirit of the law, such as the use of the tax incentives provided for by the relevant tax legislation.
- **Tax Evasion**: The company does not engage in aggressive tax planning or use tax havens to artificially lower tax burdens.
- **Proactive Engagement**: Open and cooperative relationships with authorities ensure compliance and resolve disputes fairly.
- **Internal Tax Risk Management**: A Tax Control Framework or TCF - in line with OECD guidelines, as transposed by the Italian Tax Authorities, to properly identify, measure, manage and control any tax risks.
- **Whistleblowing & Disciplinary Actions**: Employees and stakeholders can report tax-related misconduct anonymously, with zero tolerance for retaliation.

Attackers targeting financial and tax data could lead to fraud, financial manipulation, tax evasion accusations, or stolen corporate tax records. Ferrari must secure tax systems, prevent unauthorized access to financial data, and implement real-time monitoring for cyber fraud attempts.

5 | Background on Cyber Risk

5.1. Risk Management Process and Internal Control System

The **Board of Directors** is responsible for controlling and managing risks for Ferrari, an element crucial to achieve its identified business targets and to ensure continuity of the Group. Ferrari has in place an internal control and risk management system based on the model provided by the Committee of Sponsoring Organisations of the Treadway Commission Report (COSO) and the principles of the Dutch Corporate Governance Code. The approach is top-down, risk-based, enabling to focus on areas of higher risk. The internal control and risk management system is structured according to the following principles: multiple parties are involved, with responsibilities assigned in line with the international best practice of the Three Lines of Control Model. These parties are described as follows:

1. **First Layer**: assessment and management of relevant risks and response actions, comprising core business risk owners, staff functions risk owners and FLT.
2. **Second Layer**: overseeing key risks to verify the effective operation of the first line, while also supporting it through compliance, strategic, operational, and reporting functions.
3. **Third Layer**: evaluating the effectiveness of internal control, risk management, and corporate governance processes through a risk-based approach, within the scope of the Internal Audit Department.

The **Audit Committee** supports the Board of Directors by providing advisory input. The company has implemented a dedicated **Internal Control and Risk Management System Policy** to clearly define responsibilities. In December 2023, the System was strengthened through the establishment of a new department responsible for coordinating the entire framework: the Internal Audit, Risk and Compliance Department. This unit reports directly to the CEO and aims to ensure that business operations are conducted transparently and in alignment with stakeholder interests. The department is headed by the **Chief Internal Audit, Risk & Compliance Officer**, who reports to the CEO, and is composed of the following groups:

- **ERM**: responsible for identifying, assessing, managing, and monitoring the principal risks that may hinder the achievement of the company's objectives.
- **Compliance**: ensures adherence to internal rules, ethical standards, laws, and regulatory requirements.
- **Internal Audit**: provides an independent and objective evaluation of the system's adequacy and operational efficiency, reporting to the Audit Committee of the Board.

Then there is the **Internal Control Committee**, which oversees the System and promotes an integrated approach to risk and control management among the relevant functions and other departments involved in control activities. It includes the CFO, General Counsel, CDTO, Chief Internal Audit, Risk and Compliance Officer, Chief Human Resources Officer, and Chief Accounting Officer. The ERM system follows the COSO Framework and is structured as follows:

1. **Risk Governance**: guides, oversees, and reports on risk management activities;
2. **Risk Culture**: reflects the organization's values and attitudes toward risk analysis;
3. **Risk Strategy & Appetite**: defines risk tolerance, thresholds, and related protocols;
4. **Risk Assessment & Measurement**: regularly identifies and quantifies potential risks;
5. **Risk Management & Monitoring**: involves managing, mitigating, avoiding, sharing, or accepting risks, and leveraging risk and control insights to enhance business performance;
6. **Risk Reporting**: provides visibility into the strengths and weaknesses of the risk management process, supporting informed decision-making.

Risks are assessed based on their likelihood, impact, level of preparedness, and velocity. Ferrari has developed an information framework aimed at ensuring timely and updated reporting to Corporate Governance and Control Bodies, enabling them to promptly evaluate and implement any necessary corrective actions. The risk map, generated through the Integrated Risk Assessment, is first shared with top management and subsequently presented to the Group's Audit Committee.

5.2. Cybersecurity Governance and Reporting

When it comes to Cybersecurity Governance structure and organization at Ferrari, the following departments are involved:

- **Enterprise Cybersecurity**: responsible for overseeing cybersecurity across the Group, including IT, OT, and vehicle cybersecurity. The Head of Enterprise Cybersecurity reports to the CDTO and maintains a direct reporting line to the CEO;
- **Internal Control Committee (ICC)**: periodically reviews, evaluates, and discusses cross-enterprise risks, and approves related initiatives. It includes executives and C-level representatives from Enterprise Cybersecurity, Digital Transformation, Legal, Finance, Internal Audit, Compliance and Risk, and Human Resources departments;
- **Cyber Crisis Committee (CCC)**: activated in the event of major cyber incidents. It includes members from the Enterprise Cybersecurity department and C-level executives from Digital Transformation, Legal, Finance, Communication, and Compliance, as well as key internal business functions;
- **Audit Committee**: appointed by the Board of Directors, it ensures the adequacy of the risk management and internal control system. The Head of Enterprise Cybersecurity and the CDTO are invited to participate in its sessions.

In addition, the CEO is promptly and directly informed of any significant cybersecurity incident and holds regular monthly meetings with the Head of Enterprise Cybersecurity and the CDTO. This direct communication channel ensures top-level oversight and facilitates rapid strategic decision-making in response to emerging cyber threats.

5.3. Head of Enterprise Cybersecurity

Luca Pierro is currently the **Head of Enterprise Cybersecurity** at Ferrari, where he leads the company's cybersecurity strategy, ensuring the protection of IT infrastructure and sensitive data against evolving cyber threats. His expertise spans across **cybersecurity**, **IT governance**, and **compliance**, developed through a solid track record in both the financial and automotive sectors.

He holds an **Executive MBA** from Bologna Business School, a degree in Legal Informatics from the University of Eastern Piedmont, and a technical diploma from I.T.I.S. Sobrero. His career has progressively evolved from IT governance roles to senior leadership positions in cybersecurity and data protection.

Prior to joining Ferrari, he built a robust foundation in IT security and risk management. At Cedacri, he served as a **Project Manager**, overseeing governance and compliance initiatives related to IT security. He later joined FCA Bank, where he was responsible for **IT security** and the implementation of **risk mitigation strategies** in the financial domain. His expertise deepened further at Fiditalia, where he acted as **Data Protection Officer (DPO)**, ensuring compliance with privacy regulations and establishing effective cybersecurity frameworks to safeguard sensitive financial data.

At Ferrari, Luca Pierro plays a pivotal role in defining and implementing cybersecurity strategies to protect one of the world's most iconic brands. His efforts focus on securing Ferrari's digital landscape, mitigating cyber risks, and ensuring the resilience and continuity of business operations. Thanks to his **Project Management Professional (PMP)** certification and in-depth knowledge of IT governance, risk, and compliance, he brings both strategic vision and technical depth to Ferrari's cybersecurity governance—positioning the company at the forefront of digital protection and resilience.

5.4. Previous Cyber Incidents

Ferrari defines a cyber incident as any event that negatively impacts the **Confidentiality, Integrity, and Availability (CIA)** paradigm. Among the incidents recorded in 2024, none was classified as critical or had a significant impact on business operations.

However, between October 2022 and March 2023, Ferrari experienced two noteworthy cybersecurity incidents involving ransomware and data breaches—underscoring the growing cyber threats faced by high-profile luxury brands and the importance of robust security measures.

October 2022 – Alleged RansomEXX Attack: In October 2022, the **RansomEXX** ransomware group claimed responsibility for infiltrating Ferrari's systems and leaking 7 GB of internal data on the dark web. The exposed files reportedly included repair manuals, internal documentation, and technical information. Ferrari denied evidence of a system breach or ran-

somware activity, affirming that no operational disruption occurred and no ransom demands were received. Nonetheless, cybersecurity analysts noted that the nature of the leaked data suggested unauthorized access, even if it did not qualify as a full-scale ransomware incident.

March 2023 – Customer Data Breach & Ransom Demand: In March 2023, Ferrari publicly disclosed a cybersecurity incident involving the unauthorized access to customer data, followed by a ransom demand. The exposed information included customer names, addresses, email addresses, and phone numbers. In line with cybersecurity best practices, Ferrari refused to pay the ransom, aiming to discourage further criminal activity. The company reassured clients that no financial data (e.g., credit card details) or information regarding owned or ordered vehicles had been compromised. Additionally, the incident had no impact on Ferrari's operations or production processes.

A further example of the growing cyber risk landscape can be seen in the ransomware attack against **Speroni S.p.A.**, a known supplier to Ferrari, which was targeted by the Everest ransomware group. The attackers claimed to have exfiltrated and leaked sensitive company data, illustrating the potential vulnerabilities associated with third-party risk exposure. This reinforces the necessity for continuous monitoring and strong cybersecurity measures across the extended supply chain.

In response, Ferrari implemented immediate security measures: affected customers were notified, specialized cybersecurity firms were engaged to investigate the breach, and the company's IT security infrastructure was reinforced to prevent future incidents. These attacks reflect a broader trend in which luxury brands are increasingly targeted due to the value of their data and the high-profile nature of their clientele.

6 | Induction Toolkit for the Board

6.1. Cyber Vision Statement

A well-defined cybersecurity strategy provides Ferrari with a structured approach to managing cyber risks; however, the company has yet to articulate a formal **Cyber Vision Statement**. While Ferrari has implemented robust cybersecurity measures, a Cyber Vision Statement serves as a foundational guide, ensuring that security initiatives align with corporate values, operational objectives, and long-term digitalization strategies.

Ferrari's current cybersecurity framework already reflects a multi-faceted approach to protecting its digital assets. As outlined in the 2024 annual report:

> "Cybersecurity risks related to our business, technical operations, privacy and compliance issues, including any Ferrari confidential information about vehicles, services, projects, and all non-public activities related to the Racing Department, employees, clients, and fans' personal data, are identified and addressed through a multi-faceted approach, through e.g. red-teaming, pentesting, friendly phishing, and third-party-managed cybersecurity posture analysis."

Despite this solid foundation, the absence of a clearly defined Cyber Vision Statement leaves Ferrari without a unified strategic direction that explicitly integrates resilience, regulatory compliance, and proactive risk mitigation. Given Ferrari's legacy of excellence and innovation, a structured cyber vision would reinforce its commitment to securing both its digital and physical ecosystems.

Based on our analysis, we propose the following Cyber Vision Statement:

> *"To uphold Ferrari's tradition of excellence by securing our digital future through proactive cybersecurity, ensuring the protection of critical assets, client data, and continuous innovation in the luxury automotive and motorsport ecosystems."*

This delcaration encapsulates Ferrari's need for a proactive, forward-looking approach to cybersecurity, ensuring alignment with its brand values and industry leadership.

6.2. Cyber Risk Priorities

As a crucial next step, the board must be educated on Ferrari's **top three cybersecurity priorities**. This requires an **Induction Toolkit** that highlights critical risks and the best practices necessary to address them. Ferrari's three cyber risk priorities, **confidentiality, third-party supply chain risks, and security and resilience in smart vehicles**, represent the most pressing threats to the company's digital integrity. To enhance the board's ability

to oversee cybersecurity effectively, Ferrari must ensure clear communication of these risks and provide structured best practices drawn from the **NIST Cybersecurity Framework** and MITSloan's **"The Board's Role in Managing Cybersecurity Risks"**.

Before detailing these cyber risk priorities, it is essential to emphasize the distinction between **security** and **resilience**. Security focuses on preventing cyber threats through proactive protection mechanisms such as encryption, network segmentation, and authentication controls. Resilience, on the other hand, refers to the organization's ability to withstand and recover from cyber incidents while maintaining business continuity. Striking a balance between the two is imperative for Ferrari. A strategy solely focused on security may lead to rigid systems that are difficult to adapt to evolving threats, whereas an overemphasis on resilience without strong preventive controls may leave Ferrari vulnerable to frequent breaches. A well-integrated cybersecurity framework ensures that both elements complement each other, implementing robust protection measures while simultaneously developing the ability to respond and recover swiftly from incidents.

Ferrari has identified the following **three most critical cybersecurity priorities**, considering their potential impact on operational integrity, regulatory compliance, and customer trust. These priorities were selected based on recent cyber threats within the automotive industry, Ferrari's increasing digitalization, and previous security breaches that highlighted vulnerabilities in these areas.

The first priority is the protection of **confidentiality**, particularly regarding intellectual property, customer data, and proprietary vehicle technology. Given Ferrari's legacy of high-performance engineering, safeguarding intellectual property against industrial espionage and cyber theft is essential. The automotive industry is a prime target for nation-state actors and corporate spies who seek to steal design blueprints, proprietary engine technologies, and advanced software algorithms that provide Ferrari with a competitive edge. Additionally, unauthorized access to IT systems could expose sensitive customer data, potentially leading to privacy breaches, financial fraud, and reputational damage. Regulatory frameworks such as GDPR impose strict obligations on data protection, making compliance a crucial factor. To address this, Ferrari should adopt the MIT Sloan recommended best practices of *distinguishing between security and resilience* and *making security and resilience strategic business issues. Distinguishing between security and resilience* involves recognizing that security focuses primarily on preventing cyber incidents through technical safeguards like encryption, whereas resilience refers to the ability to minimize damage and swiftly recover operations after a cyber incident occurs. *Making security and resilience strategic business issues* means treating cybersecurity as integral to Ferrari's overall business strategy, requiring active board engagement, adequate resource allocation, and regular alignment of cybersecurity initiatives with strategic objectives. The NIST framework emphasizes **Data Security (PR.DS)** and **Asset Management (ID.AM)**, ensuring that Ferrari's data governance policies align with global cybersecurity standards.

The second priority concerns Ferrari's **third-party supply chain vulnerabilities**, particularly in the context of its advanced digitalized manufacturing (e.g., the E-building) and supplier network. The increasing reliance on external vendors, software providers, and cloud-based services exposes Ferrari to potential cybersecurity risks beyond its immediate control. A supply chain attack can occur when malicious actors exploit weak security measures within a supplier's network, leading to unauthorized access to Ferrari's infrastructure. Such breaches could disrupt production lines, delay vehicle deliveries, compromise software integrity, or result in financial and reputational damage. To effectively mitigate these risks, Ferrari should imple-

ment the MIT Sloan best practice of *educating company leadership*. *Educating leadership* means providing directors and executives with ongoing awareness, training, and regular briefings on evolving cybersecurity threats in the supply chain, enabling them to make informed decisions and prioritize risk mitigation actions. The NIST framework reinforces this approach through **Supply Chain Risk Management (ID.SC)**, **Response Communication (RE.CO)**, and **Security Continuous Monitoring (DE.CM)**. Continuous monitoring provides Ferrari with real-time visibility into potential threats arising from third-party relationships, while transparent and rapid communication ensures prompt detection and effective incident management across the supply chain.

The third priority revolves around **security and resilience in Ferrari's smart and connected vehicles**, particularly against cyber threats targeting over-the-air (OTA) updates and AI-driven vehicle systems. As Ferrari integrates more digital features into its high-performance cars, the risk of cyberattacks on vehicle connectivity, data privacy breaches, and potential remote hacking incidents becomes a significant concern. A compromised OTA update could introduce malicious software that manipulates vehicle behavior, while vulnerabilities in AI algorithms could be exploited to interfere with autonomous functions. Such incidents pose not only security risks but also safety concerns, as malicious actors could theoretically gain control over critical vehicle operations. Ferrari must therefore implement the MIT Sloan best practices of *developing a common cybersecurity language* and *making security and resilience a strategic business issue*. *Developing a common cybersecurity language* across the company involves establishing a uniform terminology and understanding of cyber risks among various teams, facilitating cross-departmental communication, and fostering cohesive cybersecurity strategies. By *treating security and resilience as strategic business issues*, Ferrari ensures that cybersecurity initiatives in vehicle development are prioritized at the highest organizational levels, embedding protective measures throughout the entire lifecycle of connected vehicle products. The **NIST framework's CSF 2.0** provides comprehensive guidance on safeguarding connected systems, thus ensuring Ferrari's approach remains robust against evolving cyber threats.

Additionally, Ferrari must focus on **enhancing communication strategies** following a cybersecurity incident. Previous breaches have demonstrated the necessity of a **transparent, efficient, and structured communication plan** that addresses both internal stakeholders and external partners, including customers and suppliers. In the event of a cyberattack, Ferrari must ensure that clear, real-time information is disseminated to mitigate reputational damage and maintain trust. A delayed or poorly managed communication strategy can lead to confusion, loss of customer confidence, and regulatory penalties. Ferrari must establish predefined response protocols, ensuring that executives, technical teams, and legal departments work in unison to manage crisis situations effectively.

By adopting these best practices and proactively addressing these cyber risk priorities, Ferrari can enhance its digital resilience and maintain its reputation as a leader in innovation, luxury, and performance while ensuring robust cybersecurity governance at the highest levels of the organization.

6.3. Suggested list of questions

To further strengthen Ferrari's cybersecurity governance, the board may ask the following strategic questions to evaluate the company's cyber resilience:

Confidentiality (Intellectual Property, Customer Data, Regulatory Compliance)

- How do we ensure that Ferrari's intellectual property, including proprietary vehicle designs and engineering data, is protected from cyber espionage and theft?
- What measures are in place to monitor and control unauthorized access to customer data, including personal information and transaction records?
- How does Ferrari align its cybersecurity policies with global regulatory requirements, such as GDPR, to ensure compliance and avoid legal repercussions?
- What incident response protocols do we have in place to mitigate the impact of a data breach, and how frequently are these tested?
- How do we balance the need for open innovation and collaboration with suppliers and partners while maintaining strict access controls to sensitive data?

Third-Party Supply Chain Risks

- How do we assess and verify the cybersecurity posture of our suppliers, particularly those involved in critical manufacturing processes such as the E-building?
- What level of visibility do we have into third-party networks and IT systems that integrate with Ferrari's infrastructure, and how do we monitor for vulnerabilities?
- In the event of a cyberattack on a key supplier, how does Ferrari ensure continuity of operations and prevent cascading disruptions?
- How are cybersecurity responsibilities and incident reporting obligations defined in Ferrari's contracts with suppliers and technology partners?
- What proactive measures are taken to educate and enforce cybersecurity best practices among Ferrari's supply chain partners?

Security and Resilience in Smart Vehicles

- What specific security measures are embedded in Ferrari's connected vehicle architecture to prevent hacking, unauthorized access, and data manipulation?
- How do we ensure the integrity and security of over-the-air (OTA) software updates to Ferrari's smart vehicles, and what safeguards are in place to prevent malicious tampering?
- What processes are in place to detect and respond to potential cyber threats targeting Ferrari's AI-driven vehicle systems in real time?
- Are there emerging automotive cybersecurity regulations to maintain security and resilience in connected vehicles, and are we implementing these?
- What contingency plans do we have to address cybersecurity-related recalls or potential vulnerabilities discovered post-production in our smart vehicle fleet?

By integrating these elements into Ferrari's cybersecurity governance, the board can ensure proactive risk management and alignment with best practices. The formulation of a dedicated **cyber vision statement**, coupled with Ferrari's structured risk mitigation strategy, will strengthen the company's ability to anticipate and address cyber threats in an increasingly digitalized automotive landscape.

7 | Budget Request

Ferrari stands as a global icon of excellence, embodying innovation, performance, and luxury. However, the increasing integration of digital technologies, interconnected systems, and a globally connected supply chain exposes the company to escalating cyber threats that could severely impact intellectual property, customer trust, and operational resilience. To preserve Ferrari's competitive edge and brand reputation, immediate investment in cybersecurity is required, focusing on three critical priorities: data confidentiality, third-party supply chain security, and the resilience of smart and connected vehicles.

We initially chose to implement the **Fear Strategy** because we believe it is an effective way to create immediate urgency among the Board of Directors, who do not have deep cybersecurity expertise. By leveraging real-world cyber incidents affecting automotive, luxury, and technology companies, we can demonstrate tangible risks, such as financial losses, regulatory fines, and reputational damage. This approach ensures swift decision-making and prioritization of critical cybersecurity initiatives without prolonged negotiation.

Ferrari's legacy is built on engineering excellence, proprietary vehicle designs, and a highly exclusive customer base. Yet, the company's increasing reliance on digital operations makes it a prime target for cybercriminals seeking to exploit **confidential data**. Recent cyberattacks underscore the severity of this risk. In October 2022, the RansomEXX ransomware group claimed to have stolen 7GB of Ferrari's internal data, including confidential contracts, invoices, and technical vehicle documentation. While Ferrari officially reported no evidence of a direct system breach, the leak of proprietary documents highlighted critical vulnerabilities in Ferrari's data protection framework. Just a few months later, in March 2023, another ransomware attack targeted Ferrari, demanding a ransom for stolen client data. The exposed information included customer names, addresses, email addresses, and telephone numbers, sensitive details that could be exploited for identity theft, fraud, or targeted phishing attacks. Ferrari chose not to pay the ransom, following cybersecurity best practices, but the repeated incidents signal an urgent need to strengthen encryption measures, access controls, and breach detection capabilities.

The consequences of inadequate data protection have been seen across the industry. In November 2024, the New York Attorney General fined Geico $9.75 million after a data breach compromised 116,000 drivers' personal information. Similarly, Travelers Indemnity Company faced a $1.55 million penalty for exposing thousands of customers' sensitive data. These cases illustrate the real **financial and reputational risks** associated with regulatory non-compliance and inadequate cybersecurity investment.

Without enhanced security measures, Ferrari risks falling prey to more sophisticated cyberattacks, potentially compromising its vehicle R&D blueprints, proprietary hybrid and electric powertrain data, and strategic business agreements. Regulatory penalties under GDPR and emerging EU and US data protection laws could result in millions in fines, further damaging

the company's standing with investors and stakeholders.

The Everest ransomware attack on Speroni, a **critical third-party supplier** within Ferrari's production ecosystem, illustrates the severe vulnerabilities in the automotive supply chain. This breach demonstrated how cybercriminals can infiltrate weaker third-party networks to indirectly compromise Ferrari's manufacturing processes. If a major supplier of engine components, vehicle software, or electronic modules were to suffer a cyberattack, production lines could be halted, deliveries delayed, and quality control compromised, leading to millions in financial losses and dissatisfied customers.

The 2021 Toyota supply chain attack provides a chilling precedent. A ransomware attack on a single supplier forced Toyota to shut down 14 factories in Japan for a full day, leading to an estimated production loss of 13,000 vehicles. Similarly, in 2023, a cyberattack on Denso Corp., a major supplier for Ferrari and other automakers, compromised classified vehicle development data, threatening future innovation and exposing trade secrets.

As Ferrari expands its e-Building smart manufacturing facility, the company's reliance on digitalized workflows, IoT-driven automation, and cloud-based production planning will increase exponentially. However, these advancements also introduce new entry points for cyberattacks. Failure to establish strict cybersecurity requirements for suppliers, real-time monitoring of third-party systems, and contingency plans could lead to devastating disruptions, putting Ferrari at risk of production halts, revenue losses, and regulatory penalties.

Ferrari's transition toward over-the-air (OTA) software updates presents a growing cybersecurity challenge. While the company remains averse to full-autonomous driving, maintaining the core driving experience, its connected car ecosystem and embedded digital functionalities introduce new cyber risks.

To ensure that the Board of Directors also understand the long-term investments needed to secure Ferrari's digital future, we deemed it necessary to incorporate the **Gap Analysis** strategy as an extension. This way, we can provide a structured, data-driven approach to identifying Ferrari's cybersecurity weaknesses compared to industry benchmarks and best practices. By assessing the current security posture against leading frameworks and competitors, we can align cybersecurity investments with long-term business strategy, build trust with the Board, and ensure sustainable improvements rather than reactive fixes. This approach fosters informed decision-making and promotes a proactive cybersecurity culture within the organization, one that is currently not present at Ferrari.

The automotive industry has already witnessed the catastrophic consequences of inadequate vehicle cybersecurity. In 2022, a group of cybersecurity researchers hacked into a Tesla Model 3's infotainment system, exploiting a vulnerability that allowed them to remotely control critical vehicle functions. Similarly, the 2023 Toyota API breach exposed over 2.3 million vehicles to remote hacking, demonstrating how poorly secured cloud infrastructures can be weaponized against automakers.

For Ferrari, an exploited software vulnerability could result in malicious manipulation of vehicle performance, unauthorized data collection, or even the remote disabling of critical driving functions. The absence of proper safeguards in Ferrari's OTA update process could enable attackers to inject malware into vehicle firmware, potentially triggering recalls, legal liabilities, and reputational harm. Compounding these risks, regulatory frameworks in the EU and US are rapidly evolving. The UNECE R155 and R156 automotive cybersecurity regulations mandate

strict risk assessments and compliance measures, requiring automakers to demonstrate the resilience of their connected vehicle systems. Non-compliance could lead to prohibitive fines and restrictions on vehicle sales in key global markets.

Ferrari's commitment to cybersecurity, though commendable, currently highlights a substantial **investment gap** compared to other leading automotive brands. In 2024, Ferrari allocated approximately €4 million to cybersecurity through operational and capital expenditures, as outlined in the latest annual report. By contrast, the leading OEMs, including Tesla, General Motors, and Volkswagen, collectively dedicated over $5 billion toward cybersecurity defenses in 2023 alone. This stark discrepancy underscores the scale of Ferrari's underinvestment relative to industry leaders. While Ferrari's cybersecurity strategy has matured significantly through partnerships and internal initiatives, the comparatively limited budget increases the company's exposure to emerging cyber threats and potentially hampers its ability to respond swiftly and comprehensively to sophisticated attacks. Closing this investment gap is critical, not only to mitigate immediate cyber risks but also to ensure Ferrari's long-term competitive position in an increasingly digital and connected automotive market.

The cyberattack on Honda's connected vehicle system in 2020, which caused a global production shutdown, serves as a stark warning. Ferrari cannot afford to be reactive, proactive investments in vehicle cybersecurity must be prioritized to prevent similar crises.

Ferrari has built its legacy on precision, performance, and exclusivity. However, in an era where cyber threats are becoming as significant as physical safety risks, failing to act is not an option. Cybercriminals have already targeted Ferrari twice in recent years, and third-party attacks are an increasing threat. The growing integration of AI, cloud services, and digitalized manufacturing makes Ferrari more vulnerable than ever.

Ferrari has the opportunity to lead the industry in cybersecurity excellence rather than being forced to react to future breaches. This is not simply a question of IT infrastructure, it is a fundamental business strategy to protect Ferrari's legacy, financial stability, and competitive edge. Ignoring these threats risks catastrophic financial, operational, and reputational damage. The time to act is now.

Bibliography

[1] R. CyberSecurity360. Ransomware a ferrari: l'azienda conferma e annuncia che non pagherà alcun riscatto, cosa sappiamo, 2024. URL https://www.cybersecurity360.it/news/ransomware-a-ferrari-lazienda-conferma-e-annuncia-che-non-paghera-alcun-riscatto-cosa-sappiamo/.

[2] R. C. della Sera. Ferrari colpita da attacco hacker: cosa sappiamo finora. maranello era stata avvisata dei rischi con altre aziende, 2023. URL https://www.corriere.it/tecnologia/23_marzo_24/ferrari-colpita-da-attacco-hacker-cosa-sappiamo-finora-maranello-era-stata-avvisata-dei-rischi-con-altre-aziende-00a3738a-32c8-4268-8c9d-d98aaea43xlk.shtml.

[3] R. W. Italia. Ferrari ha subito un attacco informatico, 2024. URL https://www.wired.it/article/ferrari-attacco-informatico/.

[4] N. C. S. C. (NCSC). *Cyber Security Toolkit for Boards*. National Cyber Security Centre, 2024. Consultato il 18 marzo 2025.

[5] F. N.V. *FERRARI N.V. ANTICORRUPTION COMPLIANCE PRACTICE*. Ferrari N.V., 2023.

[6] F. N.V. *FERRARI N.V. ANTITRUST COMPLIANCE PRACTICE*. Ferrari N.V., 2023.

[7] F. N.V. *FERRARI GROUP CODE OF CONDUCT*. Ferrari N.V., 2023.

[8] F. N.V. *FERRARI N.V. ENVIRONMENTAL PRACTICE*. Ferrari N.V., 2023.

[9] F. N.V. *FERRARI N.V. HUMAN RIGHTS PRACTICE*. Ferrari N.V., 2023.

[10] F. N.V. *FERRARI N.V. THIRD PARTIES COMPLIANCE PRACTICE*. Ferrari N.V., 2023.

[11] F. N.V. *Annual Report and Form 20-F 2024*. Ferrari N.V., 2024.

[12] F. N.V. Cyber incident in ferrari, 2024. URL https://www.ferrari.com/en-EN/corporate/articles/cyber-incident-in-ferrari.

[13] F. N.V. Governance practices, 2024. URL https://www.ferrari.com/en-EN/corporate/practices.

[14] N. I. of Standards and Technology. The nist cybersecurity framework (csf) 2.0. NIST Cybersecurity White Paper (CSWP) NIST CSWP 29, National Institute of Standards and Technology, Gaithersburg, MD, 2024. URL https://doi.org/10.6028/NIST.CSWP.29.


Ferrari