



Financial Reporting Council

# FRC Lab Report: Digital Security Risk Disclosure Example bank

# Contents

<b>Introduction</b>	<a href="#">3</a>
<b>Key findings relating to:</b>	
• Strategy	<a href="#">4</a>
• Governance	<a href="#">5</a>
• Risk	<a href="#">6</a>
• Events	<a href="#">7</a>
<b>Examples relating to:</b>	
• Strategy	<a href="#">8</a>
• Governance	<a href="#">14</a>
• Risk	<a href="#">33</a>
• Events	<a href="#">42</a>

## Examples used

This example deck, and the [report](#) to which it relates, highlights examples of current practice that were identified by the Financial Reporting Council Lab (the Lab) team and investors. Not all of the examples are relevant for all companies, and all circumstances, but each provides an example of a company that demonstrates an approach to useful disclosures. Highlighting aspects of reporting by a particular company should not be considered an evaluation of that company's annual report as a whole. Investors have contributed to this project at a conceptual level. The examples used are selected to illustrate the principles that investors have highlighted and, in many cases, have been tested with investors.

However, they are not necessarily examples chosen by investors, and should not be taken as confirmation of acceptance of the company's reporting more generally. If you have any feedback, or would like to get in touch with the Lab, please email us at: [frclab@frc.org.uk](mailto:frclab@frc.org.uk).

# Introduction

## Business continuity and resilience

Digital security is fundamental to business continuity, resilience and value creation. Reporting on these areas should provide relevant information to investors and other stakeholders to assist them in assessing a company's ability to remain viable and resilient.

## Context

As part of the project, the Lab reviewed current disclosure practices (up to May 2022) to identify examples of better practice.

This example bank supplements the [full project report](#) which provides insight into investors needs, challenges for companies and some suggestions for disclosures which align to investor needs.



This example bank is designed to be read alongside the main report but can be used separately as a guide relating to current better practice disclosure.

The key findings from the project have been included in the following pages to provide further context for this example bank.

## Disclosure, materiality and the risk of 'over-disclosure'





As part of the project we engaged widely with various stakeholders. Participants noted that, on average, current disclosures are not sufficient to meet investor and other stakeholder needs. While there were concerns expressed from some that additional digital security-related disclosure in itself could create risks for companies, there was an equal number who highlighted the opposite, noting in their view, that a lack of disclosure or overly static 'boilerplate' disclosure was in itself a flag that a company was not sufficiently emphasising digital security.

The examples in this bank link to key aspects of disclosure identified as useful in the project. When determining which disclosures to provide, consideration should be taken of materiality for the company, potential sensitivity of the information and whether they provide sufficient information to users.

These examples are based on our review of market practice up to May 2022. As reporting and disclosure practice in this area develops we may consider updating these examples.



# Strategy

<b>Investors want (where relevant) disclosures that:</b> 	<b>Audit committees should consider whether the disclosures:</b> 	<b>Reporting and risk disclosure teams should consider:</b> Core disclosures that:  Enhanced disclosures that: 	
<ul style="list-style-type: none"><li>• provide the context for digital security and strategy and its importance to the company's broader strategy and business model and ability to generate value;</li><li>• indicate how external trends associated with digital security and strategy are integrated into the company's approach; and</li><li>• link digital security and strategy disclosure to the company's broader strategy.</li></ul>	<ul style="list-style-type: none"><li>• make sense in the context of the company's broader strategy;</li><li>• clearly communicate the company's digital transformation and data strategy; and</li><li>• explain how digital transformation and its related risks can advance or hinder the attainment of future strategic objectives.</li></ul>	<ul style="list-style-type: none"><li>• set out how the business model and strategy impact, and are impacted by, digital and data;</li><li>• set out the company's (planned) approach to respond to internal and external digital factors; and</li><li>• indicate how developed the company's data and digital transformation strategy is and whether there are any associated KPIs.</li></ul>	<ul style="list-style-type: none"><li>• set out how technology and digital support the future business model and the actions and investments the company has made;</li><li>• provide specific details of digital transformation trends; and</li><li>• provide a consistent narrative throughout the report (or are included in a report from the Chief Technology Officer (CTO)) with clear links to other strategic areas and related decisions.</li></ul>








# Governance

<b>Investors want (where relevant) disclosures that:</b> 	<b>Audit committees should consider whether the disclosures clearly communicate:</b> 	<b>Reporting and risk disclosure teams should consider:</b>	
		<b>Core disclosures that:</b> 	<b>Enhanced disclosures that:</b> 
<ul style="list-style-type: none"> <li>• detail the governance structures, culture and processes the company has in place to support digital security and strategy;</li> <li>• link the governance of digital transformation and security risks to strategy and risk appetite;</li> <li>• show how the board, and its committees, have oversight of these risks. This may also include who within the company has ownership of specific risks, and the access they have to senior leaders;</li> <li>• explain what a company has done to foster a digital security (or cybersecurity) culture; and</li> <li>• outline the relevant skills of the board and any assurance obtained.</li> </ul>	<ul style="list-style-type: none"> <li>• who the risk owners or responsible officers are and how they contribute to 'senior-level' discussions;</li> <li>• what steps (including recruitment and training) are being taken to determine whether the appropriate skills exist within the board and company (and whether these steps are fit for purpose); and</li> <li>• what role internal audit and the audit committee play in relation to digital security and strategy risks.</li> </ul>	<ul style="list-style-type: none"> <li>• cross refer to strategic drivers or business model within the audit and risk committee section;</li> <li>• explain board and committee structure and the make-up of a digital committee if in place; and</li> <li>• reference surveys, cyber-related training and other activities conducted during the period.</li> </ul>	<ul style="list-style-type: none"> <li>• provide CTO (or equivalent) reports on opportunities and threats;</li> <li>• set out issues that the board and committees have considered, name owners of specific risks and detail how these tie to specific oversight committees and the role of the CTO (or equivalent); and</li> <li>• detail development of a cyber and digital culture within the organisation, including monitoring and targets.</li> </ul>



# Risks

<b>Investors want (where relevant) disclosures that:</b> 	<b>Audit committees should consider whether the disclosures clearly communicate:</b> 	<b>Reporting and risk disclosure teams should consider:</b>	
		<b>Core disclosures that:</b> 	<b>Enhanced disclosures that:</b> 
<ul style="list-style-type: none"> <li>• link the digital security and strategy risks to strategic objectives and risk appetite;</li> <li>• consider the actions and activities taken to mitigate risk and how risks have evolved;</li> <li>• provide information about the risk and mitigations at the right level of granularity; and</li> <li>• connect digital security and strategy with disclosures on viability and resilience.</li> </ul>	<ul style="list-style-type: none"> <li>• whether a rigorous risk identification process has been undertaken;</li> <li>• what the company considers to be the optimal level of risk;</li> <li>• how the company's digital security strategy is communicated throughout the organisation and supply chain and how this is reviewed/monitored;</li> <li>• that the company/board understand the threat landscape, company vulnerabilities, risk appetite, mitigating actions and effectiveness; and</li> <li>• the extent to which there is reliance on third parties.</li> </ul>	<ul style="list-style-type: none"> <li>• cross refer to strategic objectives and risk appetite and indicate the owner of each risk;</li> <li>• provide detail of frameworks, mitigations and actions;</li> <li>• set out the elements that are reflective across the group or highlight specific areas of the business that are impacted; and</li> <li>• set out the impacts of digital transformation and data within the prospects assessment, assumptions and in the context of stress testing.</li> </ul>	<ul style="list-style-type: none"> <li>• provide more detail on the oversight process, identify associated opportunities and provide clear and specific links to viability and resilience scenarios;</li> <li>• provide risk actions and mitigations at a granular level relevant to the business (e.g. product, segment, operation or geography) or consider the wider value chain (customers, suppliers etc.); and</li> <li>• provide more detail of 'cyber scenarios' (e.g. length of disruption, cost, division, regulatory response) considered and/or of connected scenarios.</li> </ul>

<b>Investors want (where relevant) disclosures that:</b> 	<b>Audit committees should consider whether the disclosures clearly communicate:</b> 	<b>Reporting and risk disclosure teams should consider:</b>	
		<b>Core disclosures that:</b> 	<b>Enhanced disclosures that:</b> 
<ul style="list-style-type: none"> <li>highlight the impacts of events (internal and external) and the actions and activities that respond to these.</li> </ul> <p>Specifically where the company has been the subject of a cyber incident, provide information about:</p> <ul style="list-style-type: none"> <li>the incident and its immediate impacts;</li> <li>mitigating actions taken and their objective and effectiveness;</li> <li>the work of the board to facilitate recovery from the incident;</li> <li>the quantified financial impact of the incident; and</li> <li>any improvements and amendments made, or to be made, in response to the incident.</li> </ul>	<ul style="list-style-type: none"> <li>whether the incident response plans had functioned adequately;</li> <li>whether incident escalation channels had been adequately established and functioned effectively to inform key decision makers about the incident in a timely manner;</li> <li>whether the incident (or type of incident) had been anticipated in some form (or had the event not been foreseen at all); and</li> <li>how accurately cyber-related risks had been considered in the company's various scenario analyses.</li> </ul>	<ul style="list-style-type: none"> <li>provide information about the nature of the incident and its immediate impacts (subject to interaction with other reporting and regulatory requirements); and</li> <li>explain the shorter term mitigations and actions taken to restore operations and reduce customer impacts.</li> </ul>	<ul style="list-style-type: none"> <li>provide detail of response to the issue by internal audit, the board and its committees in understanding the issue, managing the incident, assessing the effectiveness of remediation work conducted and learning lessons for the future.</li> <li>quantify the estimated financial impact (if material) of the incident and impacts on future capital expenditures.</li> <li>explain how learnings and changes have fed through to the net and gross risk and longer-term viability and resilience.</li> </ul>



# Strategy

## Helping investors understand

## Extract

The context for digital security and strategy and its importance to a company's broader strategy, business model and ability to generate value

[IAG](#); [Experian](#)

How external trends associated with digital security and strategy are integrated into the company's approach

[IAG](#); [Experian](#)

How digital security and strategy disclosure links to the company's broader strategy

[BAE Systems](#)



### What is useful?

IAG has included a report from the Chief Information Officer which clearly explains the current and future digital and technology-based strategy in the context of the company's markets and stakeholders.

Reporting 'directly from the CIO' further illustrates the company's commitment to technology and digitisation in achieving its strategic objectives.

# Driving towards technology excellence

## IAGTech



John Gibbs  
Chief Information Officer

**"In 2021, we completed the work on our new IT/Digital operating model and are focused on driving continuous improvements to our ways of working, including creating an environment where our technology professionals can thrive."**

### Overview

Our new IAG Tech operating model is now live, with improvements to the products and services we offer the business; increased efficiency and effectiveness of our value streams and processes; adoption of modern methods and tools; a leaner organisation structure; clearer roles and accountabilities, and improved governance with enhanced reporting. This has resulted in new capabilities being delivered faster and more regularly due to the adoption of agile methodologies. We also saw reductions in the number of incidents affecting our customers and a decrease in the time to restore services. Progress was hampered though, by our need to support the business in responding to COVID-19, for example reducing investments to preserve cash. However,

we have maintained our focus on increasing the maturity of our cyber security capabilities, including strengthening our Security Operations Centre and the start of a new Group-wide identity and access management solution.

### Our people

We have launched a new IAG Tech website as part of our strategy to create a thriving technology community that attracts and retains the very best talent. We now have over 1,500 active members of our guilds sharing best practice and knowledge, supported by a learning academy that is developing our future digital leaders. We also welcomed our second intake of graduates and apprentices.

Our Digital Factory is rapidly deploying Robotic Process Automation and Low Code Solutions to automate processes and help our employees, for example, chatbots that can answer questions on our Ground Operations Manual. This automation is being accelerated through a Digital Champions network that identifies the opportunities and seeks to exploit this technology.

We continue to modernise our internal systems, for example, the upgrade of our call centre technology for British Airways in UK and Hong Kong. We are improving decision-making through use of artificial intelligence, machine learning, data analytics and dashboards including the deployment of a digital boardroom for our IAG GBS management team.

### Our customers

We introduced a wide variety of solutions to assist with travel in a COVID-19 world including automating the validation of customers' travel documentation, pre-ordering of onboard food and drink, and biometric boarding.

Our omni-channel strategy saw the introduction of voice recognition, chatbots and WhatsApp used by our Iberia customers. In parallel, enhancements have been made to all .com platforms including dynamic pricing capability for fares and ancillaries. We increased self-service capabilities such as introducing disruption management onto airport kiosks. We also

introduced new distribution channels for our travel agent partners.

We have supported partnership launches and the delivery of the Global Loyalty Platform for Aer Lingus, Iberia and Vueling, providing a more customised and better experience for our customers.

We migrated Vueling onto our Salesforce platform which enabled us to deploy chatbots to handle routine tasks and answer many of our customer's questions. This resulted in a 60 per cent reduction in back office workload and improved customer satisfaction to over 90 per cent.

### Our planet

Our fifth Hangar 51 innovation accelerator platform explored how new technologies can help us meet our sustainability commitments, and improve operational efficiency, performance, safety, and customer experience.

Many of our technology investments also contribute to our sustainability plan. This included investments in network, aircraft and operational planning systems to reduce the environmental footprint of our flights; the introduction of pre-ordering of food and drink onboard that has reduced waste; and the launch of three data centre migration programmes that will move all of our systems onto new infrastructure hosted in the cloud, providing enhanced resilience, performance and an 80 per cent lower CO<sub>2</sub> footprint for our technology.

### Looking forward

We have three main priorities in 2022, in our pursuit of Technology Excellence. We will accelerate the delivery of the new technology capabilities required to support the Group's transformation, including making significant progress on our data centre migration and replacing obsolescence. We will continue to embed and improve the IAG Tech operating model. We will continue to develop a culture where we value the diversity across our technology professionals, ensure that everyone feels included and is treated equally, and that we have a thriving and supportive community with a strong sense of belonging.

### What is useful?

Experian details how data, digital and cyber trends are developing and feeding directly into the strategy, risks and opportunities for the business over the short, medium and long-term.

This disclosure sets the tone for the rest of the report. The company then includes detailed disclosure on the processes, approaches and actions it is taking in these areas (see next page).

#### Proliferation of data

##### Trend

As the world moves increasingly online, the amount of data available is growing at an extraordinary pace. Of all current data, 90% has been created in the last two years, and 127 new devices connect to the internet every second. As well as the increased amount available, it is becoming cheaper for businesses to store, manage and analyse data. However, these businesses need to understand the many data sources available to them in order to improve decision-making.

New data sources, made available through open banking in the UK and USA, and positive data in Brazil, are giving organisations access to rich, up-to-date information. However, to optimise opportunities in these challenging times, businesses need to embrace advanced analytics tools, capable of connecting disparate datasets and making the information more usable.

##### Our response

We develop solutions to offer sophisticated platforms to help clients take advantage of data proliferation. For example, Ascend Intelligence Services uses AI and machine learning to support continuous improvement of strategic models for clients. This frees up data-scientist time from model building and monitoring activities, it means data can be integrated into models faster, and produces an endpoint that can be utilised by PowerCurve and Experian One. It can also offer real-time market insights, benchmarking and health monitoring.

We are evolving our analytics portfolio in response to client demand for a shift towards cloud-based products. We are investing in a roadmap of innovation to evolve from a largely on-premise software business towards a cloud-first, digital-first, API-enabled and scalable platform business. This transformation is well underway and began with our investments to unify and standardise our product suites, easing the process of scaling these globally.

For example, PowerCurve migration to the cloud provides an adaptable platform that enables decisions to be designed to client needs and combines rich data and advanced analytics to drive decisions at scale. The modular design offers agility, and our continual augmentation of machine learning into the platform can bring greater connectivity to the businesses we serve, with frictionless experiences for their consumers.



#### Advances in automation and technology

##### Trend

Businesses in all industries are looking to AI and machine learning to automate processes in order to operate more efficiently, and secure productivity gains. New technologies are revolutionising industries, and businesses are investing to remain competitive, with over 95% of Fortune 1000 organisations stating they are investing in big data and AI.

Automation can personalise customer experiences, make online transactions simpler, automate logistics and optimise business decisions, allowing companies to generate significant efficiencies and redeploy their staff to do jobs which require a higher level of human input.

##### Our response

We are transforming our technology stack to a modern, resilient, scalable and secure cloud-based architecture to accelerate product delivery to clients. Investment in the best technology is critical to the way we ingest, store and secure data, as well as to the way we develop and deliver our products. It is one of the critical factors in how we can maintain and extend competitive advantage. Technology enables us to link Experian and third-party data assets to create innovative products.

In addition, we use technology to enhance our own processes, which has improved productivity. It has allowed us to reduce our conventional cost base and release funds for investment in new opportunities, such as further innovation. For example, we continue to invest in our RPA (Robotic Process Automation) capability and have automated 377 of our key processes, equating to more than 350 years of manual activity time saved since project inception.



**95%**  
of Fortune 1000  
organisations state they are  
investing in big data and AI



#### A changing regulatory environment

##### Trend

Regulators are becoming increasingly more active in protecting consumer data and privacy rights, and there are now significant financial and reputational consequences for non-compliance. Cybercrime is also increasing, and there is much greater scrutiny of data protection.

As data custodians, businesses have a responsibility to safeguard consumer privacy. We believe we can help our clients and consumers meet their responsibilities in this more demanding environment.

Regulators are opening up banking and other data-rich industries, encouraging consumers to ensure they get the best possible deal.

##### Our response

We work with regulators to ensure we comply fully with all new regulations, and engage in public debate to ensure policy-makers take into account our views and those of our industry. We develop new services to help our clients remain compliant with regulations that affect them.

Protecting consumer privacy and information security is extremely important to us. We have programmes that evaluate every product and service to ensure we strike the right balance between consumers' privacy expectations and the economic benefit to both consumers and clients. Furthermore, we are channelling investment into our multi-layered and extensive information security programme to manage and protect against cyber security risks, by continually upgrading our security infrastructure in an ever-changing environment.

Accurate data is fundamental to our reputation and business success. We constantly strive to increase the accuracy of our data in a competitive market, to ensure customers can have confidence in the services we provide.



Treating data with respect

Security

Accuracy

Privacy

Transparency

Data is the lifeblood of our business. So ensuring we collect, store and manage data safely and appropriately is fundamental to our ongoing success. It's important our clients and customers know we take our responsibilities very seriously when it comes to managing data securely, ensuring privacy measures are managed effectively, the data we hold is accurate and we are open and transparent about the data we hold and the way it is processed.

Security Safeguarding data

We hold vast amounts of data on people and businesses. The loss or inappropriate use of data and systems could result in material loss of business, substantial legal liability, regulatory enforcement actions and significant harm to our reputation.

Our approach

We continually enhance our security infrastructure, practices and culture across the business through our SecurityFirst programme. We invest heavily in cyber security and have specialist teams, state-of-the-art technology and rigorous due diligence procedures to deal with potential threats.

Our security approach has three tiers: applying tools and processes to prevent threats from entering our environment; detecting if a threat enters our environment; and mitigating any threats by minimising the potential for information to be extracted from our environment.

We have controls in place to check for compliance and constantly scan for potential threats, with several layers of protection for our data assets (see diagram below). Our perimeter deflects tens of thousands of attempts every day.

Our Global Security Operations Centre works around the clock to identify suspicious or malicious activity, with teams in Malaysia, the UK and the USA, as well as automated tools and AI. If they identify a threat, our incident response team steps in to eliminate it with support from in-house forensic data specialists and external experts if required.

We gather intelligence to help our security teams stay ahead of evolving cyber threats. This year, we expanded our interaction with law enforcement authorities and others in our industry to help give each other early warnings of high-potential cyber security threats. We also share our knowledge to help other businesses and consumers keep their data safe. Our annual Data Breach Industry Forecast for 2021 highlighted areas that have become increasingly vulnerable to cyber attack in the COVID-19 era. Predicted threats include vaccination misinformation and disruption, hackers holding home devices for ransom, and exploitation of 'track and trace' apps to gain access to personal user information.

This year, COVID-19 led to almost our entire workforce moving to homeworking and we took steps to provide employees with secure remote connections to our systems. Most data breaches involve some human interaction, often something as simple as clicking a link in an email. Our email and web browsing controls protect against this kind of malware, and our security training also encourages people to think carefully about what they are clicking on.

Our Development, Security and Operations (DevSecOps) teams work together to build security considerations into our products throughout their lifecycle, from start to finish. We use a range of processes, including manual penetration testing, to discover, detect and remediate any potential security risks at every stage of product development – from concept to coding, build, quality assurance and production.

We conduct regular risk assessments and vulnerability checks, and our operations are subject to external cyber security audits every year. Simulated exercises and a global data breach plan prepare our cyber security teams and senior leaders to respond rapidly in the event of a breach.

Protecting our perimeter

We have a defence-in-depth approach to protecting our critical data assets, which provides multiple layers of control and protection.

- Perimeter scanning**  
Scanning the perimeter for open access and scanning applications for regulatory compliance
- Firewall**  
Blocks unauthorised access while permitting outward communication
- Intrusion Prevention System (IPS)**  
Examines network traffic flows to detect and prevent vulnerability exploitation
- Web Application Firewall (WAF)**  
Filters, monitors, and blocks HTTP traffic to and from web applications
- Realtime Application Self Protection (RASP)**  
Detects and blocks computer attacks by taking advantage of information from inside the running software



Security governance

The Chief Information Security Officer has overall responsibility for Experian's global security strategy and the Global Security Office (GSO) sets relevant policies and standards. The Security and Continuity Steering Committee – which includes the Chief Executive Officer, Chief Financial Officer, Chief Operating Officer and Chief Information Officer – oversees our approach to keeping data secure and protecting consumer information. It reviews key metrics on security tools, compliance and training completion rates every month. The Audit Committee also receives progress reports at each of its meetings.

We have a comprehensive Global Security Policy and controls based on the internationally recognised ISO 27001 standard. Our robust information security programme builds on industry-recognised procedures, including the US National Institute of Standards and Technology (NIST) framework. We seek and receive third-party assurance through ISO 27001 certifications of key business areas and systems, as well as other recognised external accreditations of our security programmes. For example, we hold a Cyber Essentials Certification and perform risk assessments against our critical and external-facing applications annually.

Security, Audit and Risk teams work together to continually improve our assurance capabilities and test the effectiveness of our controls. Our Three Lines of Defence model for risk management (see page 73) includes review by Global Internal Audit and oversight from the Board. Any potential policy breaches are thoroughly investigated and we take disciplinary action where appropriate.

The GSO conducts due diligence to identify any potential risks before an acquisition, followed by an in-depth post-acquisition security assessment that is reviewed by Global Internal Audit.

When it is necessary to provide third parties with access to our data and systems, the GSO ensures we provide access in line with our information security requirements. We extend stringent standards on information security to our suppliers and partners through the terms of our contracts. All third parties are risk assessed. Of our nearly 13,000 active third parties, 1,674 have been identified as significant or high risk and all of these have undergone more in-depth assurance by the GSO.

Security requirements are tiered based on this risk assessment, and can include increased controls for higher-risk third parties. We monitor compliance through our third-party risk management framework and third parties identified as significant or high risk are added to the GSO's continuous monitoring programme which alerts us to any material changes to trigger follow-up action if needed.

Our information security culture

At Experian, information security is everyone's responsibility. We set out clear requirements for employees and business units in our Security Risk Management and Governance Policy. We invest significant time and resources in training and awareness on information security through our SecurityFirst programme.

Our strong information security culture starts from the top of the business. Senior leaders are highly engaged and continually reinforce the message that security is the personal responsibility of everyone working with us.

All our employees and any contractors who have access to our systems must complete mandatory annual training on information security and data protection. We track training completion rates weekly and provide a monthly dashboard to the Security and Continuity Steering Committee.

More than 250 training courses are available for people across the business to find out more about keeping information safe across various web, mobile and desktop platforms, applications and software. We provide additional in-depth training for people working in higher-risk roles, such as product and software development.

We continually refresh our training to stay up to date with evolving risks and circumstances. This year, we focused on risks associated with working from home and made sure employees understood how to secure their home network, for example by using filtering software and strong passwords. We adapted our regular awareness campaigns to continue providing employees with frequent updates on important topics, such as email protection and phishing.

Our Global Information Values

Wherever we operate, we are committed to five core Global Information Values:

1. Balance
2. Accuracy
3. Security
4. Integrity
5. Communication



250+

training courses are available for people across the business to find out more about keeping information safe.

Scan me to find out more about Experian's commitment to its Global Information Values.



**BAE Systems  
Annual Report 2021, p12  
and p14**

**What is useful?**

BAE Systems explains how digital strategy and security risks and opportunities are considered in the context of the company's broader strategy (including acquisition activity).

We completed two new acquisitions in 2021, both in the UK, firstly a small technology bolt-on which enhances our data and digital capabilities, and secondly In-Space Missions, a company that designs, builds and operates satellites and satellite systems, enabling us to combine BAE Systems' experience in highly secure satellite communications with In-Space Missions' full lifecycle satellite capability. We also announced we had entered into a definitive agreement to acquire Bohemia Interactive Simulations, a leading developer of advanced military simulation and training software, headquartered in the US.

### Our vision

To be the premier international defence, aerospace and security company

### Our mission

To provide a vital advantage to help our customers to protect what really matters

## Our strategy

	Progress during the year	Outlook
<div style="background-color: #e67e22; color: white; padding: 5px; width: 20px; margin: 0 auto; font-weight: bold;">1</div> <p style="margin: 0;"><b>Sustain and grow our defence business</b></p>	<ul style="list-style-type: none"> <li>– Defence sales grew by 3%</li> <li>– 2021 orders ahead of expectation</li> <li>– Number of major long-term programmes continued to grow</li> <li>– Increased self-funded R&amp;D</li> </ul>	<ul style="list-style-type: none"> <li>– Strong order backlog and long-term programme positions</li> <li>– Defence spending increasing in many of our major markets</li> <li>– Good opportunity pipeline in all our sectors</li> <li>– Geopolitical and macro risks still remain</li> </ul>
<div style="background-color: #e67e22; color: white; padding: 5px; width: 20px; margin: 0 auto; font-weight: bold;">2</div> <p style="margin: 0;"><b>Continue to grow our business in adjacent markets</b></p>	<ul style="list-style-type: none"> <li>– Work continued on key controls and avionics development programmes including 777X</li> <li>– BAE Systems' clean propulsion systems continued to expand its product offerings and markets</li> <li>– Hydrogen Fuel cell partnerships and EVTOL investments announced</li> <li>– Acquisition of In-Space Missions</li> </ul>	<ul style="list-style-type: none"> <li>– Our clean propulsion systems technology is well placed as demand for low and zero emission technology grows</li> <li>– Commercial aerospace recovery is expected in the coming years</li> <li>– Cyber security and digital technology opportunities with allied governments</li> <li>– Investment in space capabilities to drive revenue growth in this domain</li> </ul>
<div style="background-color: #e67e22; color: white; padding: 5px; width: 20px; margin: 0 auto; font-weight: bold;">3</div> <p style="margin: 0;"><b>Develop and expand our international business</b></p>	<ul style="list-style-type: none"> <li>– Qatar programme moving into aircraft delivery and support</li> <li>– A number of significant export awards for MBDA</li> <li>– CV90 awards in several markets</li> <li>– Continued to widen reach and relationships in targeted markets especially in Asia-Pacific</li> </ul>	<ul style="list-style-type: none"> <li>– Strong bid pipeline in Europe, Asia-Pacific and Middle East supported by increasing defence budgets in many key markets</li> <li>– Opportunities to develop in new markets driven by threat environment and ability to export from UK, US, Australia and Sweden</li> <li>– MBDA remains well positioned across Air, Land and Sea</li> </ul>
<div style="background-color: #e67e22; color: white; padding: 5px; width: 20px; margin: 0 auto; font-weight: bold;">4</div> <p style="margin: 0;"><b>Inspire and develop a diverse workforce to drive success</b></p>	<ul style="list-style-type: none"> <li>– Progression of employee value proposition to drive recruitment marketing strategy</li> <li>– Recruited a record 1,373 apprentices and graduates in the UK</li> <li>– Established new gender diversity metrics, embedded our ambitions into process, practices, policies, systems and training</li> <li>– Implemented talent management framework across all levels and relaunched leadership and learning programmes online</li> </ul>	<ul style="list-style-type: none"> <li>– Build stronger employee experience aligned to organisation culture and sustainability ambitions</li> <li>– Progress gender diversity goals and develop stronger ethnicity ambitions</li> <li>– Evolve recruitment transformation programme to focus on critical skills of the future</li> <li>– Develop workplace climate to build stronger culture of agility and inclusiveness, strengthening our commitment to mental health, safety and wellbeing</li> </ul>
<div style="background-color: #e67e22; color: white; padding: 5px; width: 20px; margin: 0 auto; font-weight: bold;">5</div> <p style="margin: 0;"><b>Enhance financial performance and deliver sustainable growth in shareholder value</b></p>	<ul style="list-style-type: none"> <li>– Strong set of financial results delivering order intake, sales, EBIT, EPS and free cash flow growth</li> <li>– Dividend increased for 17th year in a row</li> <li>– £500m share buyback announced in July 2021 and completed in February 2022</li> </ul>	<ul style="list-style-type: none"> <li>– Strong order backlog and established positions on long-term programmes provide a strong platform to deliver mid-term growth</li> <li>– Focus on improving cash conversion and margin expansion</li> <li>– Delivery on rolling three-year cash targets enables strategic flexibility to deliver a broad and balanced capital allocation policy and enhanced shareholder returns</li> </ul>
<div style="background-color: #e67e22; color: white; padding: 5px; width: 20px; margin: 0 auto; font-weight: bold;">6</div> <p style="margin: 0;"><b>Advance and integrate our sustainability agenda</b></p>	<ul style="list-style-type: none"> <li>– UN Race to Zero and 2030 net zero ambitions</li> <li>– Record UK apprentice hiring programme and continued investment in STEM and early careers</li> <li>– SASB submission and the introduction of disclosures in line with TCFD recommendations</li> <li>– Ongoing focus on safety and wellbeing and accredited as real living wage UK employer</li> </ul>	<ul style="list-style-type: none"> <li>– Develop 2030 net zero roadmap and mature TCFD disclosures</li> <li>– Progress ESG agenda and increase our visibility and impact</li> <li>– Use external benchmarks to set targets and metrics and drive improvements and ambitions</li> <li>– Engage employees and key stakeholders to set ESG priorities and drive integrated approach</li> </ul>

### What is useful?

The report from the Innovation and Technology Committee further highlights the importance of the topics within the company and to external stakeholders.

## Innovation and Technology Committee report



**Ewan Kirk**  
Chair of the Innovation and  
Technology Committee

### Members

Ewan Kirk (Chair)  
Nick Anderson  
Dame Carolyn Fairbairn  
Nicole Piasecki

### Dear Shareholders

I am delighted to present the first report of the Innovation and Technology Committee. The Committee was established by the Board in July 2021. We held our inaugural meeting in October wherein we discussed the innovation and technology landscape in the Company's principal markets (excluding the US).

In this report, I will give you an overview of the Committee's remit and in the years to come, I will provide updates on Committee activities and an overview of our discussions.

### Role of the Committee

The Committee's purpose is to promote the success of the Company through the effective oversight of the application of science, engineering and technology, and the successful exploitation of its intellectual property and know-how in pursuit of its business and commercial goals.

Through closer engagement with senior executives, we will support and enhance the Company's ability to meet its strategic objectives, and assure ourselves that there are in place; an appropriate culture, infrastructure, collaborative practices and activities that stimulate innovation.

We will do so by:

- reviewing the allocation and prioritisation of R&D funding;
- overseeing of Company processes to identify, develop and exploit technology and intellectual property; and
- maintaining strategic oversight and awareness of STEM developments, as applicable to the Company.

To support us in the developing of our understanding of the Group's technology landscape, we will regularly visit global sites, meeting with employees and managers, and discussing central and sectoral opportunities.

### Membership

The Committee is comprised of four non-executive director members; Nick Anderson, Dame Carolyn Fairbairn, Nicole Piasecki and myself. More details of membership and attendance at meetings can be found on page 124. The Committee is supported by members of the senior executive team; the Chief Executive, Group Finance Director, Chief Technology Officer and Group General Counsel are all standing attendees.

### National security

In recognition of national security considerations, the Committee focuses principally on the UK business. Much of the intellectual property and know-how owned by the Company is subject to national security laws and regulations, as a result, our site visits and discussions of such technologies are undertaken in accordance with the national security requirements of the UK and other nations.

In particular, the Committee is cognisant of and observes the requirements of BAE Systems, Inc.'s Special Security Agreement.

**Ewan Kirk**  
Chair of the Innovation  
and Technology Committee



# Governance

## Helping investors understand

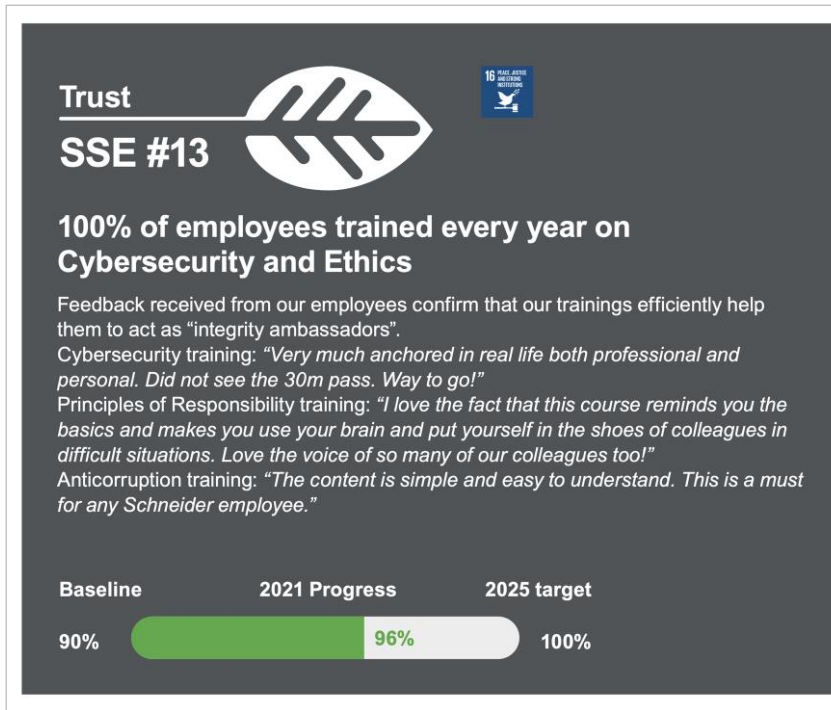
## Extract

The links between the governance of digital transformation and security risks to strategy and risk appetite	<a href="#">Schneider Electric</a> ; <a href="#">Landsec</a> ; <a href="#">UBS</a>
How the board and its committees have oversight of these risks. This may also include who within the company has ownership of specific risks, and the access they have to senior leaders	<a href="#">Flutter Entertainment</a> ; <a href="#">Reach</a> ; <a href="#">London Stock Exchange Group</a> ; <a href="#">RELX</a> ; <a href="#">Admiral Group</a> ; <a href="#">NatWest Group</a> ; <a href="#">Ocado Group</a>
What the company has done to foster a digital security (or cybersecurity) culture	<a href="#">Schneider Electric</a> ; <a href="#">Admiral Group</a>
The relevant skills of the board and any assurance obtained	<a href="#">Flutter Entertainment</a> ; <a href="#">RELX</a> ; <a href="#">NatWest Group</a> ; <a href="#">Admiral Group</a>

**Schneider Electric  
Universal Registration  
Document 2021, p38 and  
p97**

**What is useful?**

Schneider Electric has taken a holistic approach to cybersecurity and has embedded it into its wider 'trust charter'. The trust charter is used to set expectations around the overall company culture. The company has used a case study and key metrics to help demonstrate how its approach to trust is embedded into the company.



**Trust Charter, Schneider Electric's Code of Conduct**

In 2021, Schneider Electric evolved its Principles of Responsibility to the Trust Charter, acting as the Group's Code of Conduct and demonstrating its commitment to ethics, safety, sustainability, quality, and cybersecurity. Schneider Electric believes that trust is a foundational value. It is earned. It serves as a compass, showing the true north in an ever more complex world and Schneider Electric considers it to be core to its environment, sustainability, and governance commitments.

Trust powers all Schneider Electric's interactions with stakeholders and all relationships with customers, shareholders, employees, and the communities they serve, in a meaningful, inclusive and positive way.



**2021 highlights**

**96%**

employees trained on Cybersecurity and Ethics.

**81%**

of our employees are confident to report unethical conduct.

**26%**

of confirmed cases raised via the Trust Line lead to actions.



Ethisphere Institute – One of the 2021 World's Most Ethical Companies.

**Schneider Electric  
Universal Registration  
Document 2021, p41**

**What is useful?**

The company further builds on the cyber culture disclosure and demonstrates through its disclosure that it considers cybersecurity risk beyond the company boundary, i.e. suppliers, contractors and communities.

These risk considerations then connect with the company’s detailed exploration of risks, mitigations and opportunities.

**Schneider 2021 Vigilance risk matrix**

- Very high risk
- High risk
- Medium risk
- Low risk

	Schneider Electric sites						Suppliers						Contractors		Communities	
Offices	Travelers, sales forces	Factories low voltage and electronics	Factories medium voltage	Project centers	Field services	Travels and hospitality	Transportation and shipping	Raw materials	Metal transformation and treatment	Plastics	Batteries	Other components	On Schneider Electric sites	Off site and projects execution	Around Schneider Electric sites	Around customers project sites

Offer safety and cybersecurity	Offer safety			●	●	●	●		●	●	●	●	●		●	
	Cybersecurity and data privacy	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●

**Company insight: Schneider Electric SE**

During a discussion with Schneider Electric to understand more about their approach to ‘cybersecurity disclosure’ they identified some key considerations:

1. The more disclosure, the better – rather than focus on just what is required, report the maximum allowable by the company’s policies
2. Be proactive, not reactive – integrate cyber, digital and data risks into the broader enterprise risk management framework and try to anticipate regulations before they are implemented – this allows systems, processes and reporting to be ahead of the game
3. Own the narrative – this can only be achieved if you report and make information visible to your community. If not reported directly by the company, information may be obtained through other channels, potentially resulting in an alternative narrative being presented to the market and other stakeholders
4. Consider the company’s importance and role in the value chain especially for critical infrastructure – report information that allows others to fully understand the company and its cybersecurity posture



**What is useful?**

These risk considerations then connect with the company's detailed exploration of risks, mitigations and opportunities.

Risk description and impact	Policies	Main actions and 2021 performance	Opportunity created
<b>Cybersecurity and data privacy</b>			
<b>Business disruption</b>			
<b>Industrial activities</b> Risk of a malicious exploitation or intrusion into the infrastructures of Schneider Electric production and distribution centers <ul style="list-style-type: none"> <li>• Impacts on productivity, data privacy, operations</li> <li>• Financial cost, and loss of confidence from stakeholders</li> </ul>	Directive Site Protection  Data center, IT Room and Network Enclosure Security Policy  IT Disaster Recovery Plan for Business Continuity Policy  Network Security Policy  Acceptable Use of Assets Policy  Security testing for products and systems	<ul style="list-style-type: none"> <li>• 200+ Cybersecurity leaders appointed and trained</li> <li>• Operational Technologies (OT) workers security awareness deployed</li> <li>• Access level defined, granted, and checked as per the profile/need</li> <li>• Endpoints inventory and protection</li> <li>• Topography of OT network, OT monitoring and threat detection, security policy compliance, incident response process</li> <li>• IT/OT network segmentation secured industrial Personal Computer (PCs), secure remote access, backup restore for PCs and Programmable Logic Controller (PLCs)</li> </ul>	Improved supply chain resilience  Greater confidence of our customers and partners into our supply chain and products  Market access to critical infrastructures/customers  Advanced discussions with authorities and greater collaboration on safety and security
<b>Human resources (HR) and employee collaboration</b> Risks of HR systems disruption or HR data leakage <ul style="list-style-type: none"> <li>• Impact on business continuity, legal compliance and overall reputation</li> </ul>	Acceptable Use of Assets Policy  Crown Jewel Security Policy  Digital Certification Policy  Email Security Policy  Personnel Management Security Policy  Third-Party Security Policy  User Access Management Policy	<ul style="list-style-type: none"> <li>• Cybersecurity Charter shared and signed by all employees and contractors</li> <li>• All employees trained every year on Cybersecurity and Ethics; dedicated mandatory training for high-value asset administrators</li> <li>• Monthly phishing campaigns</li> <li>• Data protection and cleanup yearly campaign</li> <li>• Yearly access audits on all HR applications</li> <li>• Data Protection Impact Assessments for high-risk applications</li> <li>• External pen tests performed on all high-value asset applications</li> <li>• Background verification checks in accordance with relevant laws and regulations</li> </ul>	Attractiveness of Schneider Electric for prospective candidates aligned with Trust Charter commitments
<b>Compliance</b>			
<b>Data privacy, retention &amp; residency</b> <ul style="list-style-type: none"> <li>• Risk of compromise, modification or exfiltration of data from Schneider Electric's data systems</li> <li>• Representing a non-compliance to data protection regulations and laws as well as business purpose leading to potential penalties</li> <li>• Non-compliance to data protection regulations leads to potential fines</li> </ul>	Data Privacy Policy  Data Classification Policy  Global Data Retention  Record Creation  Backup and Recovery Policy  Log Management & Monitoring Policy  Acceptable Use of Assets Policy  Digital Certification Policy	<ul style="list-style-type: none"> <li>• Mandatory Cybersecurity &amp; Data Privacy annual training sessions</li> <li>• Data privacy champions appointed</li> <li>• Annual review of all policies</li> <li>• Data Retention implemented by area</li> <li>• Sensitivity label feature enabled on Microsoft Office 365 Suite for all employees</li> </ul>	Increase sentiment of trust for our customers, partners and larger community  Prove alignment to regulations and devotion to ESG requirements

Risk description and impact	Policies	Main actions and 2021 performance	Opportunity created
<b>Cybersecurity and data privacy (continued)</b>			
<b>Damage to customers assets</b>			
<b>Field services operations &amp; remote customer support</b> Risk of malware distribution into the production environment of a customer through compromised Field Service end-point or on-site activities <ul style="list-style-type: none"> <li>• Impact on customer assets and production</li> <li>• Reputational impact</li> </ul>	Cyber Badge Principles  Third-Party Security Principles  Network Security Policy  Malicious Software Policy	<ul style="list-style-type: none"> <li>• Cybersecurity contact identified, ad hoc and periodic assessments for strategic ones</li> </ul> For our customer-facing employees: <ul style="list-style-type: none"> <li>• Deployment of Cyber Badges across 20,000+ customer-facing employees.</li> <li>• Compliance monitoring of Cyber Badge deployment</li> </ul> For our customer-facing suppliers: <ul style="list-style-type: none"> <li>• Consistent Cybersecurity and Privacy Terms &amp; Conditions developed for all suppliers</li> </ul>	Increase sentiment of trust for our customers, partners and larger community <ul style="list-style-type: none"> <li>• Absolute requirement</li> <li>• Global Action Plan</li> </ul>
<b>Customer staging and project commissioning</b> Risk of compromised customer assets having an impact at site level, as a result of a failure in the control environment of Schneider Electric <ul style="list-style-type: none"> <li>• Reputational Impact</li> <li>• Repairment cost</li> </ul>	Security Principles  Cybersecurity Policy for Products & Systems  Network Security Policy  Malicious Software Security Policy  Source Code Security Policy	<ul style="list-style-type: none"> <li>• Deployment of an end-to-end Project Supply Chain Security methodology</li> <li>• Datamining for preparing recommendations</li> </ul>	Greater confidence of our customers in our products  Market access to critical infrastructures  Advanced discussions with authorities and greater collaboration on safety and security  Fulfillment of contract requirement opening the door for additional or further opportunities.  On-time with tendering process
<b>IP theft and loss</b>			
<b>R&amp;D repositories and source code compromise</b> <ul style="list-style-type: none"> <li>• Compromise, deterioration or exfiltration of R&amp;D repositories and source code</li> <li>• Jeopardizing Intellectual Property availability, integrity and confidentiality</li> </ul>	Source Code Security Policy  Cybersecurity Policy for Products and Systems  Information Security Charter  Sensitive Source Code Security and Confidentiality Affidavit	<ul style="list-style-type: none"> <li>• Site security controls compliance, training and awareness deployed</li> <li>• Assets inventory, topography of R&amp;D sites</li> <li>• Protection against vulnerabilities or malware</li> <li>• Pen tests conducted</li> <li>• Least Privileged Access Control, Disaster Recovery Plan, Network Segmentation, Port Management, and Protocol Hardening applied</li> <li>• Source code reality checks conducted on code content, code engineering, governance, etc.</li> <li>• Threat detection of signals on the surface web, the dark web, social media etc. to spot cracked software, Source Code and IP exposed etc.</li> </ul>	Effective visibility for risk management and proper actionable outcomes  Perceived as a trusted partner  Reducing risk through advance detection of exposure of sensitive code or potentially compromised or modified applications which could facilitate criminal activity or customer compromise

### What is useful?

Landsec clearly identifies Key Risk Indicators (KRIs) and their impact on the company's strategic objectives. The existing and planned mitigating activities are outlined.

## 6 Information security and cyber threat

EXECUTIVE RESPONSIBLE | BARRY HOFFMAN

**Data loss or disruption to the corporate systems and building management systems resulting in a negative reputational, operational, regulatory (including GDPR) or financial impact.**

### EXAMPLE KRIs

- › Speed of threat and vulnerability detection
- › Speed of vulnerability resolution
- › Number of data loss events
- › Disaster recovery – system availability
- › Building management cyber security risk
- › Cyber security and GDPR training

### MITIGATION

- › We have an IT Operations team and Privacy & Compliance Officer who monitor information security and privacy risk and cyber threat
- › All of our colleagues complete mandatory cyber security and GDPR training
- › Our IT security management policy sets out our standards for security and penetration testing, vulnerability and patch management, data disposal and access control
- › We complete a quarterly assessment that key IT controls are operating effectively
- › All third-party IT providers must complete an information security vendor assessment which is reviewed and approved by the cyber security officer
- › We work closely with our IT service partners to manage risk and improve technical standards
- › Our development brief clearly defines the required technical IT standards for all building systems
- › Our move to put all corporate systems in the cloud has improved the resilience of our disaster recovery and business continuity plans
- › We have an effective vulnerability management system, including an annual rolling penetration testing programme across our IT estate.
- › All our properties have business continuity and crisis management plans in place, which are tested at least annually
- › We are rolling out a programme of improvements to our site building cyber defences based on the NIST framework

### CHANGE IN YEAR | NO CHANGE

The level of this risk has not changed, reflecting that, while companies continue to be subject to an increasing number of attempted cyber attacks, we have continued to develop and invest in the maturity of our mitigation controls.

### OPPORTUNITY

We continue to work with our service partners and strategic suppliers to examine our industry's standards, in particular for building systems. We consider new technologies so we can take advantage of the latest innovations and opportunities and enhance our reputation as a trusted and responsible partner.

### What is useful?

Responsibility for the risk area is clearly presented by the company and the importance to the audit committee's discussions and focus during the period is highlighted.

## Introduction from the Chairman of the Audit Committee

NICHOLAS CADBURY  
CHAIRMAN OF THE AUDIT COMMITTEE



### COMMITTEE MEMBERS

- › Nicholas Cadbury (Chairman)
- › Madeleine Cosgrave
- › Stacey Rauch

### HIGHLIGHTS

- › Continued focus on integrity of reporting process
- › Rigorous assessment of risk management and internal controls
- › Review of impact of Covid-19 on the business

### KEY RESPONSIBILITIES

- › Reliability of the financial statements and internal controls
- › Effective risk identification and management
- › Overall transparency and financial governance

### NUMBER OF MEETINGS AND ATTENDANCE

- › Four scheduled meetings
- › 100% attendance from all members

### DEAR SHAREHOLDER

Throughout the financial year, the Audit Committee continued its focus on the financial statements and the integrity of the reporting process, oversight of risk management and internal controls and addressing the ongoing impact of the pandemic on the Group's risk profile, performance and recovery.

### RISK

The Committee used the risks contained in the Group's risk register (set out on pages 71-75 of this Annual Report) as a basis for its activity during the year. On behalf of the Board, the Committee manages the process by which risks are identified, prioritised and managed.

There are two areas of key risk that the Committee has monitored over the year that I would like to note due to their importance: cyber security and fire management. A risk management strategy has been established to identify and prioritise cyber security risks to improve cyber standards and practices across all our assets. Fire safety management is also being closely monitored by the Committee to ensure the correct measures are in place and risk management processes are being updated regularly.

A global pandemic was not something most companies had identified as a principal risk prior to 2020. The disruption caused by Covid-19 has illustrated how going forward we need to ensure that disruption risk is embedded into all our principal risks as appropriate. I am, however, reassured by Landsec's response to the pandemic which highlights how well embedded risk management is, the effectiveness of the business resilience plan and how capable the business is in responding to a crisis.

### FINANCIAL STATEMENTS

The Group's financial statements are of critical importance to investors and the Committee monitors the integrity of the Group's reporting process and financial management. It scrutinises the full and half-yearly financial statements before proposing them to the Board for approval. The Committee reviews in detail the work of the external auditor and external valuer and any significant financial judgements and estimates made by management to ensure that it is satisfied with the outcome.

The Financial Reporting Council (FRC) reviewed our 2020 Annual Report and Accounts and we were pleased that, based on its review, there were no questions or queries that it wished to raise nor any significant findings. It was very useful, however, to receive some suggestions from the FRC as to how we could improve our

**What is useful?**

UBS identifies cybersecurity and information security as a risk. The company not only identifies the direct manager of the risk but also the 'independent' party responsible for overseeing the risk.

	Risk managed by	Independent oversight by
Non-financial risks		
<p><b>Operational risk:</b> the risk resulting from inadequate or failed internal processes, people or systems, or from external causes (deliberate, accidental or natural), that have an impact (either financial or non-financial) on UBS, its clients or the markets in which it operates. Events may be direct financial losses or indirect, in the form of revenue forgone as a result of business suspension. They may also result in damage to our reputation and to our franchise that has longer-term financial consequences.</p> <p><b>Legal risk:</b> the financial or reputational implications resulting from the risk of: (i) being held liable for a breach of applicable laws, rules or regulations; (ii) being held liable for a breach of contractual or other legal obligations; (iii) an inability or failure to enforce or protect contractual rights or non-contractual rights sufficiently to protect UBS's interests, including the risk of being party to a claim in respect of any of the above (and the risk of loss of attorney-client privilege in the context of any such claim); (iv) a failure to adequately develop, supervise and resource legal teams or adequately supervise external legal counsel advising on business legal risk and other matters; and (v) a failure to adequately manage any potential, threatened and commenced litigation and legal proceedings, including civil, criminal, arbitration and regulatory proceedings, and / or litigation risk or any dispute or investigation that may lead to litigation or threat of any litigation.</p> <p><b>Employment risk:</b> the risk incurred by the firm by not adhering to the applicable employment law, regulatory requirements and human resources practices, as well as our own internal standards. Such risk is managed by business management, with independent overview by Human Resources.</p> <p><b>Cybersecurity and information security risk:</b> the risk of a malicious internal or external act leading to a material impact on confidentiality, integrity or availability of UBS data or information systems. Cyberattacks are manifestations of a cyber threat into an act of aggression or criminal activity causing financial, regulatory or reputational harm or loss.</p>	<p>Business management</p>	<p>Group Compliance, Regulatory &amp; Governance (GCRG)</p> <p>Legal</p> <p>Human Resources</p>
	<p>Business management and Chief Digital and Information Office (CDIO)</p>	<p>GCRG</p>

### What is useful?

Flutter explains how the board considered cyber risks and security during the period. Furthermore, details are provided regarding which frameworks have been adopted, applied and monitored across the group.

The company has clearly reported what plans are in place to enhance the board's knowledge and expertise including the appointment of an external advisor.

## Governance in Action



### Cyber Security Toolkit for Boards

Cyber threats continue to be a feature of operating digital businesses and the Board is acutely aware of these risks. Therefore, time continued to be spent in 2020 discussing and monitoring cyber risks and security, and the progress in mitigating these risks and preventing any possible attacks or related material adverse incidents, including:

- approval of the Global Cyber Security Policy which sets out the set of cyber security requirements across the Group;
- regular review of access controls;
- review of security standards such as ISO27001: 2013, PCI and NIST held across the Group;
- approach to testing products and services in the same way that hackers would;

- defensive measures, procedures and teams in place to protect from malicious distributed denial of service (DDOS) attacks;
- processes in place to ensure security is built in to product development;
- tools and processes in place to ensure the Group is protected against insider threat including data leakage; and
- an emphasis on employee awareness, education and testing.

To further strengthen the Board's knowledge and expertise on cyber security, Templar Executives were appointed as cyber security advisors of the Board to provide a structured advisory programme over 18 months based on the UK National Cyber Security Centre ("NCSC") Cyber Security Toolkit for Boards.

The advisory programme is structured into three stages. The first stage completed in September included one-to-one discussions with each Board member to establish current levels of understanding of cyber security risks to the Group. The second stage includes four separate Board training sessions covering different aspects of cyber security and introducing elements of the NCSC toolkit. The Board has completed one session to date, with three additional sessions to be scheduled during the first half of 2021. The third stage will include one-to-one follow up sessions with selected Board members and will be scheduled to take place during 2021.

The Committee will monitor the effectiveness of the cyber security advisory programme throughout 2021.

## Governance in action – cyber security

The Board is aware of the increase in cyber threats for any business, but particularly one whose strategy is focused on increasing its digital presence. Throughout the year, the Board has overseen and spent time discussing Reach's cyber security programme, whose objectives are to:

- mitigate any immediate material risks identified;
- build a capability to detect a cyber-breach rapidly and limit the spread and impact;
- build a best practice cyber security function; and
- embed security by design alongside data protection in all projects including all elements of the strategy.

External cyber security experts were engaged to assist in delivering the programme while the Group simultaneously established a new operating model. The Group has adopted the NIST Cybersecurity Framework to provide a policy and controls framework which can be used to assess our ability to prevent, detect and respond to cyber attacks.

During 2021, significant investment has been made in building a cyber centre of excellence, a Group-wide cyber awareness programme and technologies to support an enhanced 365-day, 24-hour monitoring service.

The Board receives a quarterly update on current cyber security readiness and maturity, using a dashboard of the independent key metrics and the associated trend for each metric, including penetration and vulnerability testing results.

	The challenge facing the industry	The opportunities for Reach	How is Reach responding?
<b>Data privacy and cyber security</b>	<ul style="list-style-type: none"> <li>• Cyber attacks are a constant threat across all digital businesses</li> <li>• Data privacy rules are constantly in flux with changes from technology platforms, with Apple and Google both changing their third-party data policies</li> </ul>	<ul style="list-style-type: none"> <li>• As digital marketing moves away from third-party cookies, relevant, latent first-party data will become more important</li> <li>• Contextual targeting is also developing in importance as marketing operators move away from third-party cookies</li> <li>• Progressive, trusted partners will be key to brands who want to be at the forefront of targeted campaigns</li> </ul>	<ul style="list-style-type: none"> <li>• Full cyber security programme developed with assistance of external experts</li> <li>• Reach has launched brand safety and contextual targeting tool Mantis</li> <li>• Reach PLUS+ advertising products offer brands the opportunity to access relevant, targeted data sets based on recent media consumption and geography</li> <li>• Reach appointed departmental data champions to ensure data privacy is a priority throughout the organisation</li> </ul>
<b>Regulatory response to technology platforms</b>	<ul style="list-style-type: none"> <li>• Digital audiences are delivered via leading technology platforms – and publishers have little leverage to negotiate attractive terms and to secure transparency over algorithm changes and the overall value driven by publisher content</li> </ul>	<ul style="list-style-type: none"> <li>• Global platforms are enabling a wider audience for Reach's content</li> <li>• Reach has a scale audience, enabling it to develop diverse revenue streams</li> <li>• Governments are seeking increased competition in the digital sector and want to rebalance the relationship between platforms and publishers</li> </ul>	<ul style="list-style-type: none"> <li>• Continuing to invest in award-winning journalism to build audience trust</li> <li>• Driving registrations to build a closer direct relationship with our customers</li> <li>• Launching new Live regional sites to reach an even bigger audience of local and national readers – further increasing the data-gathering opportunities</li> <li>• Developing new products, e.g. InYourArea, to capture new revenue opportunities, including hyper-local advertising streams</li> <li>• Securing some revenue payments from certain platforms and seeking to maximise the potential of these relationships on both an audience and advertising basis</li> </ul>



**Our people need to reflect the communities we serve, and the culture of leadership throughout the business needs to reflect the behaviours needed to develop strategic thinking, coaching, learning and development.**

## Reach

Annual Report 2021, [p21](#) and [p77](#)

### What is useful?

Reach illustrates the importance of digital, and therefore cybersecurity, to the company and its strategy.

The company reports the objectives of its cybersecurity programme, investments made into the area and outlines updates provided to the board.

Furthermore, the challenges facing the industry in the area are provided in the context of opportunities identified and how Reach is responding to these challenges and identified opportunities.

### What is useful?

The LSE Group provides a clear depiction of how technology, cyber and resilience feature in the company's governance framework.

#### Information and cyber security threats

Executive Lead: Chief Information Officer

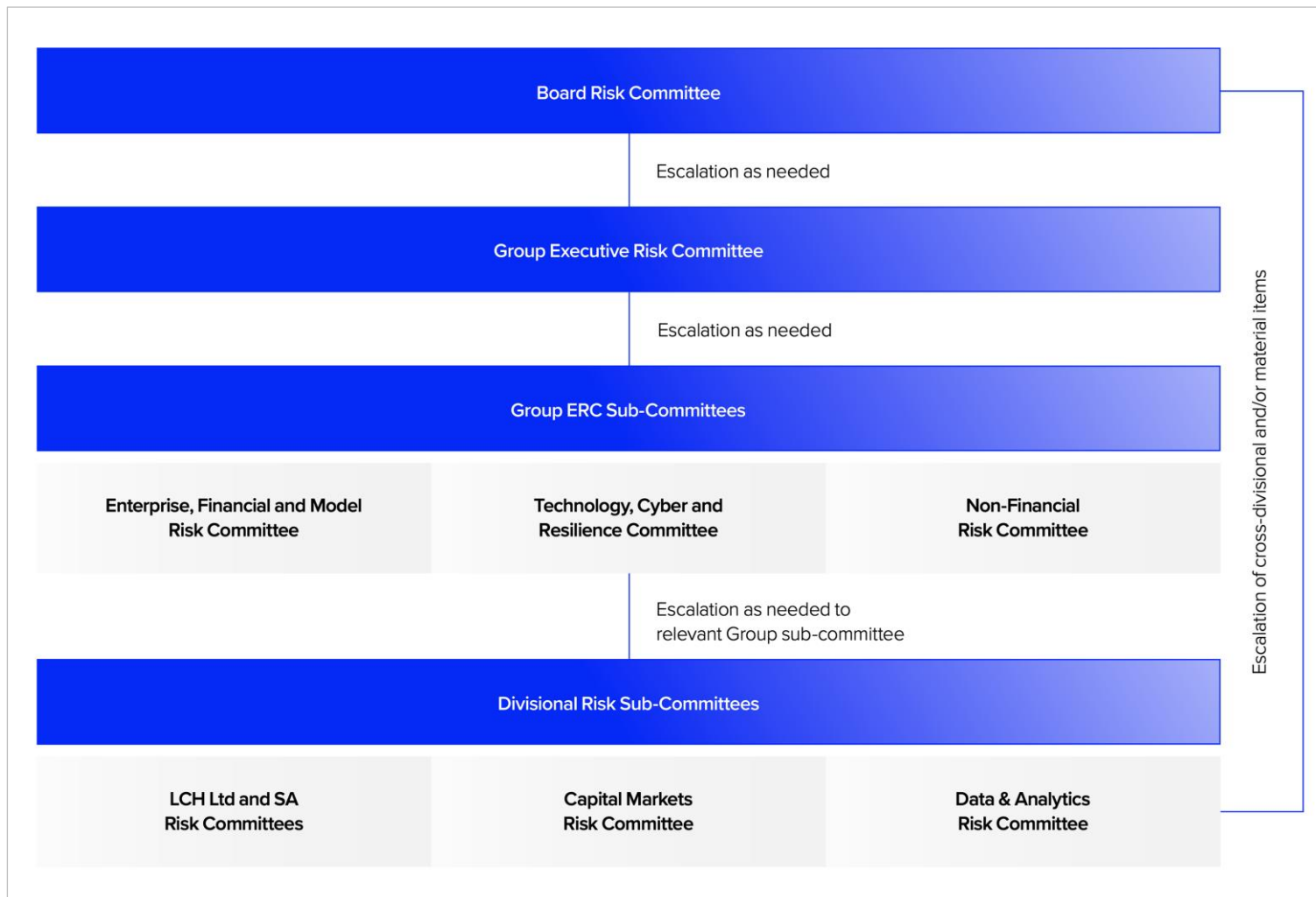
As a global Financial Markets Infrastructure (FMI) and data provider, LSEG is exposed to cyber risk. Significant cyber events continue to be observed in the financial sector and in the broader economy that demonstrate the motivation and sophistication of cyber adversaries and the impact they can have on the victim organisation. LSEG is the sum of its networks, users and devices. It consists of an eco-system of trusted vendors and business partners with a workforce that is increasingly dynamic in terms of how, when and where they are authorised to gain access to our technology environment and digital assets. In addition to the direct impact on ourselves, our role as an FMI provider underscores the systemic impact a cyber event would have on the UK financial sector and the global markets that we serve. Cyber risk does not respect and is not bound by organisational perimeters and high profile external cyber events reinforce this inter-connectivity and inter-dependency and highlight the exposure to risks arising outside of a firm's own control environment. We must acknowledge, to remain competitive in this era of digitalisation and open platforms, that cyber risk cannot be eliminated, however, it can be managed to a level of risk that we are prepared to take as a cost of doing business.

We continue to make significant investments in cyber security and have a dedicated Cyber Security function led by our Chief Information Security Officer (CISO) which is focused on protecting and defending LSEG against cyber-attacks. Due to the increasing sophistication of cyber adversaries and the techniques that they use, we proactively collect and evaluate threat intelligence. We recognise that the prevention of cyber attacks may not always be possible and our focus and priority is on remaining resilient to withstand cyber-attacks with minimal disruption to our business. Our approach to cyber security aligns to industry frameworks such as the National Institute of Standards and Technology (NIST) and we will continue to invest and advance our cyber defence, detection and response and recovery capabilities. Our Group operates a three lines of defence framework and we have a dedicated Cyber Risk function within Group Risk providing independent oversight and challenge. Our Internal Audit function performs independent assurance on our cyber controls.

## London Stock Exchange Group Annual Report 2021, [p52](#)

### What is useful?

The LSE Group provides a clear depiction of how technology, cyber and resilience feature in the company's governance framework.





### What is useful?

The group also provides insight into its assessment of risks arising from its business model and emerging technologies and how it intends to mitigate them. The executive lead is also identified.

#### Emerging technology

Executive Lead: Chief Information Officer, Divisional Group Heads

Structural market changes, new business models and advances in cloud, artificial intelligence (AI) and distributed ledger technology (DLT) could lower entry barriers, increase competitive pressures and change the markets we serve. This could negatively impact the performance of our core business and disrupt our commercial models. This risk spans the business, and the pace of change in business models, technology advances and market entrants continues to accelerate.

Cloud providers are expanding their capabilities from storage to a wide range of data management and analytics solutions. They also enable a whole new ecosystem of providers, including new market entrants, which can now take advantage of cloud providers' customer bases and fast development cycle. This can also drive new end-user data consumption models such as renting data.

The increased use of AI internally and among customers brings with it associated risks such as inherent bias, automated decision-making and data management. It will also introduce new challenges for cyber security defence and detective mechanisms.

As technology and regulatory clarity improves, aggressive competitor activity in DLT could increase risk of disruption. DLT presents potential disruptive risk to parts of our business, as it may result in a reduced need for centralised intermediaries, thereby bypassing some of the services we offer.

The Group actively monitors new technological developments and the pace of change, developing robust innovation strategies to mitigate the risk resulting from emerging technology. The Group, including through our Strategy function, actively scans for potential investment opportunities in emerging technology and has a dedicated innovation function with subject matter expertise in specific technology domain areas. The Group partners with advisers and builds Proof of Concepts to test new hypotheses and, by collaborating with our customers, can identify and quickly react to changing consumption preferences.

Regulators are actively exploring the application of new frameworks to manage the development of innovative financial services technologies. We expect these to be important for maintaining resilience and stability in the market while enabling innovation with emerging technology. The Group participates in relevant industry and academic forums, partnering closely with Regulators.

The Group continues to maintain systems and controls to mitigate the risk resulting from emerging technology. Risk arising from the Group's use of Cloud, AI and DLT is identified, assessed, managed and reported through the risk framework. We align with industry best practices and guidance when considering increased use of AI and DLT.

**RELX**  
**Annual Report 2021, p48,**

**What is useful?**

RELX's reporting clearly illustrates the steps taken to address cybersecurity throughout the company (specifically relating to board awareness and skills) and the approach taken by its suppliers.

The Board evaluation identified several specific topics for additional focus by the Board in 2022, including product and market competition, further understanding the views of the Company's suppliers in their dealings with RELX and the key cyber security risks facing the Company. These topics will be further addressed as part of the Board's 2022 programme.

- Reviewed RELX's data protection systems and processes to mitigate against cyber security risks, including a comprehensive presentation on cyber security from the Group Head of Information Assurance and Data Protection, covering the industry threat landscape, its implications to RELX and the mapping of RELX's cyber security programme to address those risks; a detailed review of the key performance indicators for the cyber security programme; and both company-wide and operating division-specific initiatives for 2021

**Vijay Raghavan**  
 Director, RELX  
 Technology Forum and  
 Chief Technology Officer,  
 Risk

Joined in 2002. Appointed to current position in 2019.

Previously Vice President of Technology, LexisNexis Insurance Solutions. Prior technology executive positions at ChoicePoint, Paragon Solutions, Primus Knowledge Solutions, and McKesson. Holds a bachelor's degree in electrical and electronics engineering from the Birla Institute of Technology and Science, Pilani, completed an advanced management program for executives at MIT Sloan School of Management, and is completing a master's degree in cybersecurity from the Georgia Institute of Technology.

2021 OBJECTIVES	Achievement
Security – SDG 16 (Peace, Justice and Strong Institutions): Continue to implement controls to increase resilience to user-based attacks such as phishing and ransomware; introduce a Great Phishing Challenge for internal and external stakeholders	<ul style="list-style-type: none"> <li>Monthly phishing simulations with results outperforming industry benchmarks; Fraud Awareness Week and Cyber Security Month activities to engage colleagues on data privacy and security</li> </ul>
Privacy – SDG 16 (Peace, Justice and Strong Institutions): Conduct a 2021 privacy quality review on compliance with EU and other requirements for cross-border data transfers	<ul style="list-style-type: none"> <li>Completed privacy quality review focused on the effectiveness of safeguards intended to mitigate the risk of non-compliance with the European Commission requirements for the cross-border transfer of personal data originating in the European Economic Area</li> </ul>

**Admiral Group  
Annual Report 2021, p58,  
p87 and p133**

**What is useful?**

Admiral provides insight into the information relayed to the board regarding information security and cyber risk and indicates that these areas received a greater level of attention from the board and risk committee during the period.

Further, the company highlights the actions taken to enhance the culture of cyber risk resilience throughout the group.

**Cyber risk**

Having been highlighted as an area of focus within the 2020 Board evaluation, the Board, as well as the Group Risk Committee, increased its oversight of cyber risk in 2021. It received updates on information security and cyber risk, technology updates generally and also held a crisis management session based on IT security and lessons learned to date. Given the increasing sophistication of cyber-attacks in the external environment, the Board intends to maintain its focus on improving cyber security defences and reviewing the Group's response plan to a cyber-attack.

**Information security**

Admiral's Group information security team, Infosec, aligns its practices to internationally recognised information security and cyber risk management frameworks and infosec risks are managed in line with the Group Enterprise Risk Management Policy. Information security policies are in place to ensure that all employees understand their responsibilities when it comes to information security, and we provide all employees and contractors with regular training.

In 2021, Infosec teams regularly engaged with colleagues to strengthen the Group's information security practices and build a resilient cyber risk culture in the new world of hybrid working. Information security risk assessments were carried out regularly across the Group and the results are monitored, managed, and reported via the appropriate governance forum, based upon the materiality of the risk.

**> Board oversight, training and escalation**

The Board continues to receive updates from management on the treatment of existing customers and on ensuring fair outcomes throughout the customer journey. Customer and employee feedback is fed into Board discussions which ultimately shapes strategic decision making, such as plans related to digital investment and future diversification. The Board also receives annual feedback on the Conduct Risk framework through the Group Risk Committee.

During 2021, the Board spent significant time on understanding the likely market response and operational impact of the implementation of the FCA's pricing remedies, which aims to:

- Ensure that renewing home and motor insurance consumers are quoted prices that are no more than they would be quoted as a new customer through the same channel.
- Make it simpler for customers to stop automatic renewals if they wish to do so.

- Enhance the FCA's product governance rules to ensure that insurers deliver fair value on all their insurance products.

The Board also received updates on (i) the progress to deliver the technology and digital strategies, which have a direct impact on the improvements made to customer journeys, and (ii) information security and cyber risk, including crisis management, both from a customer and reputational impact perspective.

### What is useful?

NatWest clearly lays out the potential risk posed due to cyber-related threats as part of its market trends and environment analysis and its response to ensure minimum interruption to stakeholders.

The area is fundamental to the company and its strategy (and related risk environment), as evidenced by specific mention in the group's external auditor's report.

### Cyber threats

#### Overview

Cyberattacks pose a constant risk to our operations, both in relation to our own digital estate and indirectly with regards to our supply chain. Cybercrime continues to evolve rapidly. Attacks may be from individuals or highly organised criminal groups intent on stealing money or sensitive data, or potentially holding organisations to ransom.

#### Our response

We continue to invest significant resources in the development and evolution of cybersecurity controls, deploy rigorous due diligence with regards to third parties and work to protect and educate our colleagues and customers on fraud and scam activity. To provide continuity of service for customers with minimal disruption, we monitor and assess a diverse and evolving array of threats, both external and internal, as well as developing, strengthening or adapting existing control capability to be able to absorb and adapt to such disruptions.

### Auditor's responsibilities for the audit of the financial statements

Our objectives are to obtain reasonable assurance about whether the financial statements as a whole are free from material misstatement, whether due to fraud or error, and to issue an auditor's report that includes our opinion. Reasonable assurance is a high level of assurance, but is not a guarantee that an audit conducted in accordance with ISAs (UK) will always detect a material misstatement when it exists. Misstatements can arise from fraud or error and are considered material if, individually or in the aggregate, they could reasonably be expected to influence the economic decisions of users taken on the basis of these financial statements.

### Explanation as to what extent the audit was considered capable of detecting irregularities, including fraud

Irregularities, including fraud, are instances of non-compliance with laws and regulations. We design procedures in line with our responsibilities, outlined below, to detect irregularities, including fraud. The risk of not detecting a material misstatement due to fraud is higher than the risk of not detecting one resulting from error, as fraud may involve deliberate concealment by, for example, forgery or intentional misrepresentations, or through collusion. The extent to which our procedures are capable of detecting irregularities, including fraud is detailed below.

However, the primary responsibility for the prevention and detection of fraud rests with both those charged with governance of the company and management.

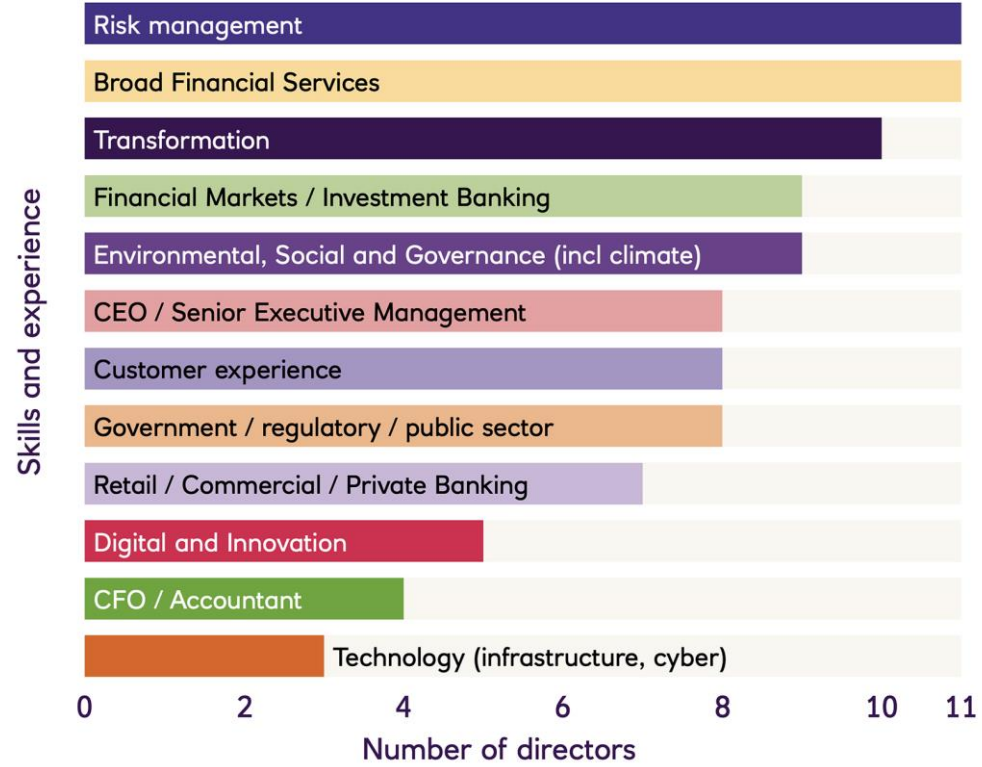
- We obtained an understanding of the legal and regulatory frameworks that are applicable to the Group and determined that the most significant are the regulations, licence conditions and supervisory requirements of the Prudential Regulation Authority (PRA) and the Financial Conduct Authority (FCA); Companies Act 2006; and the Sarbanes Oxley Act (SOX).
- We understood how the Group is complying with those frameworks by making inquiries of management, internal audit and those responsible for legal and compliance matters. We also reviewed correspondence between the Group and regulatory bodies; reviewed minutes of the Board and Risk Committees; and gained an understanding of the Group's governance framework.
- We assessed the susceptibility of the Group's financial statements to material misstatement, including how fraud might occur by considering the controls established to address risks identified to prevent or detect fraud. We also identified the risks of fraud in our key audit matters as described above and identified areas that we considered when performing our fraud procedures, such as cybersecurity, the impact of remote working, implementation of new government supported lending products, and the appropriateness of sources used when performing confirmation testing on accounts such as cash, loans and securities.
- Based on this understanding we designed our audit procedures to identify non-compliance with such laws and regulations. Our procedures involved inquiries of legal counsel, executive management, and internal audit. We also tested controls and performed procedures to respond to the fraud risks as identified in our key audit matters. These procedures were performed by both the primary team and component teams with oversight from the primary team.
- The Group operates in the banking industry which is a highly regulated environment. As such, the Senior Statutory Auditor considered the experience and expertise of the engagement team to ensure that the team had the appropriate competence and capabilities, involving specialists where appropriate.

A further description of our responsibilities for the audit of the financial statements is located on the Financial Reporting Council's website at <https://www.frc.org.uk/auditorsresponsibilities>. This description forms part of our auditor's report.

**What is useful?**

NatWest demonstrates its commitment to digital, data and related innovation through its board appointments (skills).

## Board skills and experience



**What is useful?**  
NatWest further demonstrates its commitment to digital, data and related innovation by explaining the context further through a dedicated committee and report in the annual report.

## Report of the Technology and Innovation Committee

Letter from Yasmin Jetha  
Chairman of the Technology and  
Innovation Committee

### Dear Shareholder,

I am delighted to present my second report as Chairman of the Technology and Innovation Committee (the Committee or TIC).

### Role and responsibilities

TIC is responsible for supporting the Board by overseeing, monitoring, and challenging the actions being taken by management in relation to technology and innovation. In doing so, the Committee also gives due consideration to NatWest Group's purpose.

Authority is delegated to TIC by the Board and a regular report of the Committee's activities is provided to the Board. The terms of reference are available at natwestgroup.com. These are reviewed annually and approved by the Board.

### Principal activity during 2021

During 2021, the Committee has played an important role in helping to support and challenge management plans to use technology and innovation as part of its journey to become a relationship bank for a digital world. TIC focused on the principal themes of digitising the core, future ready, innovation, partnerships and ventures, and emerging threats and opportunities. As agreed, as part of the 2020 Committee evaluation, it deliberately focused on a smaller number of deep dives into specific aspects of each theme, including competitor position and link to purpose. Key highlights included:

### Digitising the core

The Committee received a number of spotlight sessions on the development of existing technology, architecture, and processes to enhance customer experience and maintain the health and resilience of IT systems.

The Committee considered management programmes designed to automate pioneer customer journeys, including Account Opening and Pay a Bill or Person, which impact 70 to 80% of customer interactions and the majority of the customer base. The Committee considered how the activity would improve customer experience, reduce cost, and utilise One Bank capabilities to drive a consistent approach. Committee discussions focused on digitising the front to back architecture; the use of digital journeys in branch and telephony channels; the benefits from immediate decisioning; and from simplifying the product offering and supporting processes and technology.

"The Committee has played an important role in helping to support and challenge management plans to use technology and innovation as part of its journey to become a relationship bank for a digital world."

The Committee also discussed how predictive analytics, including machine learning, was being used within the Retail and Private Banking businesses, primarily to assist with identification of potential customer needs and plans to extend the use of such techniques to the Commercial Banking business.

TIC also considered how Open Finance was changing the sector and the changes required to core systems and architecture. The Committee noted the increased use of Application Programming Interfaces (APIs) to improve the NatWest Group's internal architecture, maximise re-use of assets and to improve customer experience. In addition, the external consumption and monetisation of bank produced APIs in conjunction with partners was also considered. The Committee discussed potential opportunities presented by the development of FreeAgent (integrated lending for NatWest Group customers based on cashflow forecasts), Payit (Open Banking payments offering), and data sharing to support new SME customers onboarding.

The Committee received an update regarding changes in the use of technology by the Risk function. TIC discussed technology and data transformation underway, including the use of robotic process automation and workflow tools; movement of risk engines to a cloud-based solution; data transformation; and use of 'Software as A Service' applications for solutions. The Committee discussed and challenged how proposed changes to the logical data architecture could improve regulatory reporting and noted that approach reduced complexity via data consolidation and assigning end to end ownership for such data.

The update on the use of technology and innovation as part of NatWest Group's security and cyber defences, included the evolution of the threats faced by NatWest Group; the strength of NatWest Group's defences against such attacks to date; and the continuous innovation approach being implemented. Mr James Lyne, Head of Research and Development at the SANS Institute and member of NatWest Group's Technology Advisory Board provided an external perspective on how NatWest Group compared to competitors and challenges being faced by the industry.

### Future ready

The Committee considered a number of actions being taken within the organisation to transform data and technology capabilities and deploy forward-looking technology.

TIC received an update on how new technology was empowering colleagues to adapt to a digital future by providing modern software, such as Workday, which had seen high adoption rates. Implementation of Ask Archie, NatWest Group's chatbot, and accelerated adoption of tools such as Microsoft Office 365 and Zoom as a result of COVID-19 were also considered. The Committee discussed and challenged the mindset and behaviour changes needed to embrace adoption, the technology challenges posed by legacy technology platforms, and contention between tools which were managed via One Bank design oversight.

The Committee discussed the manner in which potential acquisitions would be considered from a technology and innovation perspective. Discussion focussed on external threats, lessons learned from prior acquisitions and potential targets.

### Innovation & partnerships and ventures

Being powered by innovations and partnerships is a key part of NatWest Group's strategy.

TIC considered an update on the framework and approach to partnership working from a technology and innovation perspective. This was supported by certain deep dives on existing strategic relationships. TIC also discussed the potential income threat from payments disruption and potential opportunities to address this threat.

The Committee received updates regarding key Venture's initiatives, including Tyl and Rapidcash. In relation to Tyl, the Committee noted that it extended beyond helping businesses to receive payments by helping customers to run and grow their business as well as giving back to the community. The Committee discussed and challenged growth plans and how the business was proposed to be scaled following reduced growth, partly as a result of COVID-19. The competitive environment, emergence of non-traditional payment providers, and the potential to make greater use of merchant acquiring data to help customers and drive further development was also considered.

Regarding Rapidcash, TIC noted the transition of the business into Commercial Banking as a market leading product with the potential to disrupt the asset finance market by resolving issues such as long onboarding times, links to customers' accounting software packages to provide 'always on' lending and use of an invisible trust account to resolve customer pain points.

### Emerging threats and opportunities

TIC considered the potential threats and opportunities presented by big technology companies, including innovation from China-based technology companies. The Committee noted the collaborative approach taken by management to deepen relationships beyond supplier relationships into partnership working to solve customer needs.

The Committee discussed the evolution of digital currencies, exploration of central bank digital currencies and growth of tokenised assets and the potential threats and opportunities presented. It was agreed that this would continue to be monitored.

### Membership and meetings

The Committee is comprised of three non-executive director members, Frank Dangeard, Patrick Flynn, and me. More details of membership and attendance at meetings can be found on page 103 of the Corporate governance report.

The Committee is supported by management and the Group CEO, Group CFO, Chief Administration Officer, Chief Risk Officer, Director of Innovation, Director of Strategy & Corporate Development and Chief Technology Officer are all standing attendees.

External insights were also provided through the updates provided by management.

The Committee held four scheduled meetings during 2021.

### Performance evaluation

The annual review of the effectiveness of the Board and its Committees, including TIC, was facilitated by Independent Board Evaluation, a specialist board evaluation consultancy. Throughout the year the Committee acted in accordance with its terms of reference and, overall, the review concluded that the Committee operated effectively, and had responded to prior feedback regarding focus on a smaller number of spotlight items.

The review suggested that, given the importance of technology and innovation, the Committee could arrange its work in a way that would be more accessible to all Board members. As a result, it was agreed that appropriate agenda topics would be opened to all Board Directors in future and that consideration would be given to reducing the number of Committee meetings held taking into account the sessions opened up to the full Board in future years.

The outcomes of the evaluation have been reported to the Board and the Committee will track progress during 2022.

### Conclusion

I am delighted to chair this Committee as it continues to support the Board in an area core to NatWest Group's purpose to champion potential, helping people, families, and businesses to thrive.

Together with my fellow directors, we will retain our focus on monitoring the future technology and innovation landscape and its impact on NatWest Group in order to ensure continued resilience and help NatWest Group become a relationship bank in a digital world. The Committee will continue to shape opportunities arising from management's response to both threats and opportunities that align with NatWest Group's purpose.

I want to take the opportunity to thank the Committee members and attendees for their continued commitment during 2021.

Yasmin Jetha  
Chairman of the Technology and Innovation Committee  
17 February 2022

## Ocado Group Annual Report 2021, [p121](#) and [p131](#)

### What is useful?

Ocado details the areas of focus for board development over the period including the new chair's induction programme. Specifics relating to the internal and external providers of these trainings are reported.

## Rick Haythornthwaite's Induction Programme

Due to the restrictions placed on physical meetings because of Covid-19, the majority of the Chair's induction programme was delivered virtually. The programme was structured to provide the information needed to engage in Board meetings in the same way as for other Non-Executive Directors joining the Board, and was then further expanded to develop the oversight required as Chair. Rick underwent the same first-day onboarding experience, as undergone by all new Ocado joiners. In addition to time spent with Senior Management to understand areas of focus, time was spent with Lord Rose in the four months prior to his retirement to gain his insights as Chair.

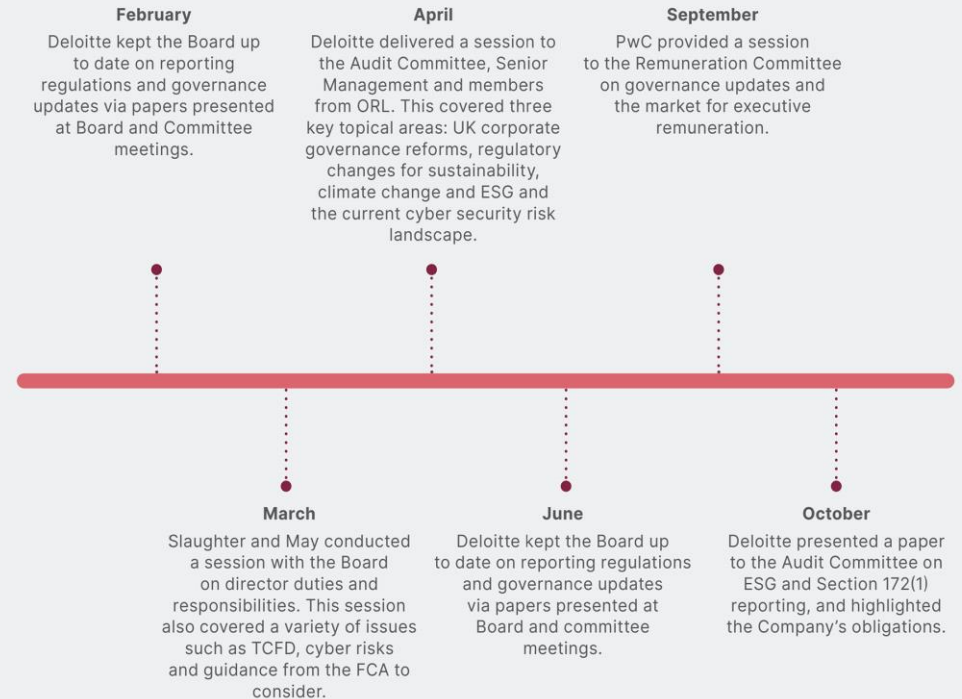
### Areas covered in the Chair's induction programme

Areas of focus	Description	Delivered by
<b>Strategy</b>	• Strategic Priorities	CEO
	• Impressions on strategy from newly incumbent CFO	CEO, Ocado Solutions; COO; CEO; Ocado Technology; CFO
	• Introduction to each of Ocado's operating segments and business areas	Head of Corporate Development
<b>Culture</b>	• People Priorities	Chief People Officer
	• Ocado's approach to remuneration	Chief People Officer
	• Client services	MD, Client Services
<b>Corporate Governance</b>	• Ocado's governance framework	Group General Counsel and Company Secretary
	• Stakeholder engagement	Chief Compliance Officer
		Communications Director
<b>Financial Performance</b>	• Ocado's financial position	CFO and CFO reports
<b>Risk</b>	• Information Technology and Cyber Risk	Chief Information Security Officer

As permitted, operational and site visits were also put into place. These included site visits to CFC Erith and CFC Bristol and meeting with operational employees, a logistics and driver experience, and a technology workshop with the senior Ocado Technology team, Rick also joined a visit to Sweden with one of our partners, Kroger, to look at our latest generation of hardware design.

## Board Development

During the year, the Board members enhanced their professional development with the following training and development opportunities.



### What is useful?

Ocado specifies cyber-related risks in its s172 statement disclosure and provides detail regarding the nature of the risk, mitigation, movement over the period, tolerance (or appetite), related horizon-scanning, owner and how it ties to the company's ESG materiality considerations.

## Cybersecurity and Data

### What is the risk

We risk the loss of critical assets and sensitive information as a result of a cyber attack, insider threat, or a data breach. This could result in business disruption, reputational damage, significant fines or the loss of confidential business information.

### How we manage it

- Structuring IT systems to operate reliably and securely.
- Testing by third party.
- Overseeing an information security governance programme by the Information Security Committee.
- Monitoring security issues and responding to security incidents by a dedicated information security team.
- No customer payment card data is held in Ocado Group's databases.
- Overseeing the Group's privacy compliance programme by the Data Protection Officer.
- Planning Cyber incident contingency.

### Movement:



### Target tolerance:

Minimal – We are extremely conservative in selecting options that impact this risk. We will only accept options that come with a limited possibility of failure.

### Emerging threats:

Cyber risk is constantly evolving, driven by technology advances and developments in the geopolitical environment. We anticipate continued risk from existing sources and incrementally from areas such as supply chain, an increasingly remote workforce, the use of AI and machine learning.

### Owner:

CEO Ocado Technology

### ESG materiality reference:

● Cybersecurity; Data Privacy Management

### Strategy reference:



## S172(1)(e): Maintaining high standard of business conduct

### Board activity and principal decisions

Considered the composition and effectiveness of the Board, including the appointment of Nadia Shouraboura and Rick Haythornthwaite.

Reviewed and approved Corporate Statements.

Undertook annual review of the principal and emerging risks of the Group and consideration of risk appetite.

Reviewed and validated the effectiveness of the Group's systems of internal controls and risk management framework.

Reviewed reports on specific risk areas across the business including the cyber security control environment, ongoing material litigation, and health and safety measures introduced in response to Covid-19.

Reviewed and approved the Group's full-year 2019/20 and half-year 2021 results, as well as the quarterly results, regulatory announcements and the Group's Viability Statement and Going Concern status.

Reviewed and approved the refreshed Group Code of Conduct, the new global Conflicts of Interest Policy and the updated Whistleblowing Policy.

Strategic Pillars:

Stakeholders:





# Risk

## Helping investors understand

## Extract

The links between the digital security and strategy risks, strategic objectives and risk appetite

[Derwent](#); [Pennon Group](#);  
[Legal & General Group](#)

The actions and activities taken to mitigate risk and how risks have evolved

[Chesnara](#); [Next](#); [Ocado Group](#)

The risk and mitigations at the right level of granularity

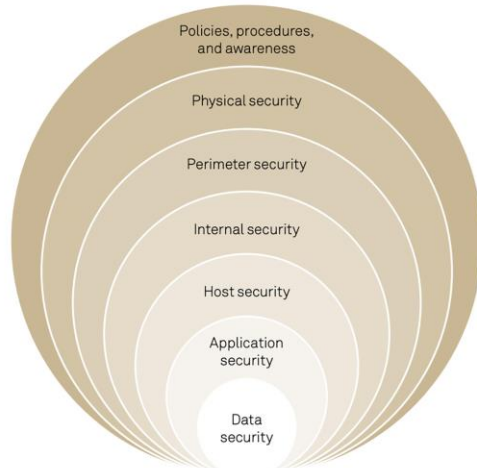
[Convatec Group](#)

## RISK COMMITTEE REPORT CONTINUED

### Cyber security

Our cyber security controls have been strengthened considerably in recent years in response to the increasing threat this poses to businesses, and it remains an area that we keep under continuous review. We adopt a layered approach to cyber security which provides multiple opportunities for threats to be identified before they can cause harm.

Our layered security approach consists of the following:



We recognise that ransomware has been identified by the National Cyber Security Centre as the most immediate threat to UK businesses. In addition to our layered security approach, we maintain a 'ransomware security incident response playbook'. During 2022, we will perform a detailed review of our ransomware playbook and will update our Business Continuity Plan to incorporate ransomware as a potential scenario for disaster recovery. Additionally, during Q1 2022, an independent review of our controls in respect to ransomware will be conducted.

Our Digital Innovation & Technology (DIT) team tested the effectiveness of our ongoing security awareness programme in 2021 by sending fake phishing emails to staff in November and monitored their response. Any staff member who clicked on the links contained in the test emails, or entered their credentials, was provided with further training on the dangers and tips on how to identify phishing emails. Each year, all staff participate in mandatory information security training and, throughout the month of October, the DIT team promoted Cybersecurity Awareness Month by sharing cyber security themed tips and guidance.

Our cyber security procedures are subject to regular independent reviews and tests. In December 2021, IT Governance conducted a cyber security health check consisting of a review of our information security governance framework, an internal/external vulnerability scan and an employee questionnaire to gauge cyber awareness levels. The Committee receives updates on the outcome of these tests/assessments and monitors the implementation of any arising recommendations.

The Committee reviews a dashboard of key risk indicators at each meeting which includes information security and cyber risk-related KPIs. During 2021, there were 131,319 (2020: 109,735) attempted attacks on our systems, none of which were successful and 99.97% (2020: 99.96%) of the attempts were stopped before they reached the intended targets, with the remaining attempts immediately being reported to our DIT team – this highlights the robustness of our cyber security posture and awareness campaigns.

### Cyber Essentials accreditation

As part of our ongoing commitment to cyber security, on 30 July 2021 our Cyber Essentials accreditation was renewed, having passed an external security scan of all internet-facing services and an assessment of technical and operational controls.

Cyber Essentials is a government-backed, industry-supported scheme which helps guard against the most common cyber threats and demonstrates to stakeholders our commitment to cyber security.



### Information security

We have robust procedures in place to safeguard the security and privacy of information entrusted to us. This ensures that we:

- maintain the confidentiality, integrity and availability of data and safeguard the privacy of our customers and employees, to ensure that the business retains their trust and confidence;
- protect the Group's intellectual property rights, financial interests and competitive edge;
- maintain our reputation and brand value; and
- comply with applicable legal and regulatory requirements.

We operate a data protection steering committee, which is comprised of Data Protection Champions from each department and meets on a monthly basis. In August 2021, the Committee was provided with an update on the work performed by the data protection steering committee, which included mandatory refresher training to all employees on protecting personal data.

[Compliance training page 161](#) →

## Derwent Annual Report 2021, [p162](#)

### What is useful?

Derwent provides context of how cyber risk connects to its operations and business model. The company considers the changing environment and describes the key aspects of its approach.

### What is useful?

The relevance to the company's business model is also clear in the detailed risk section. This is achieved through splitting the risks between internal operational risk and customer/product risk, providing a direct link to strategic objectives, business model and KPIs and detailing the mitigations for each risk. The company also provides details of executive responsibility and where internal audit review of the cyber issue was obtained.

#### 5A. CYBER ATTACK ON OUR IT SYSTEMS

The Group may be subject to a cyber attack that results in it being unable to use its information systems and/or losing data. Such an attack could severely restrict the ability of the Group to operate, lead to an increase in costs and/or require a significant diversion of management time.

**Movement during 2021:** Increased



This risk has been heightened during the Covid-19 pandemic, as cyber-criminals seek to exploit the disruption caused by employees working from home. In response, we identified the key IT risks arising from homeworking and implemented additional controls.

**Executive responsibility:** Damian Wisniewski

- The Group's Business Continuity Plan is regularly reviewed and tested.
- Independent internal and external penetration/vulnerability tests are regularly conducted to assess the effectiveness of the Group's security.
- Multi-Factor Authentication exists for remote access to our systems.
- Incident response and remediation processes are in place, which are regularly reviewed and tested.
- The Group's data is regularly backed up and replicated off-site.
- Our IT systems are protected by anti-virus software, security anomaly detection and firewalls that are frequently updated.
- Frequent staff awareness and training programmes.
- Security measures are regularly reviewed by the DIT department.
- The Group has been awarded the 'Cyber Essentials' accreditation which demonstrates our commitment to cyber security.

#### 5B. CYBER ATTACK ON OUR BUILDINGS

The Group is exposed to cyber attacks on its properties which may result in data breaches or significant disruption to IT-enabled tenant services. A major cyber attack against the Group or its properties could negatively impact the Group's business, reputation and operating results.

**Movement during 2021:** Unchanged but likely to increase as our buildings become more 'intelligent'



**Executive responsibility:** David Silverman

- Each building has incident management procedures which are regularly reviewed and tested.
- Physical segregation between the building's core IT infrastructure and tenants' corporate IT networks.
- Physical segregation of IT infrastructure between buildings across the portfolio.
- Inclusion of Building Managers in all cyber security awareness training and phishing simulations.

##### Strategic objectives

1. 2. 3. 4. 5.

##### Business model

Could potentially impact on all aspects of our business model

##### KPIs

- Total shareholder return

- Monitored our secure internet gateway and cloud managed malware protection for malicious activity during home/office working.
- Provided additional employee awareness training on social media and remote working security best practice.
- Monitored our Data Leak Prevention system for any indications of personal data breaches.
- Remediated any key findings from the last security penetration test and commissioned another independent internal/external test.
- Conducted a simulated 'phishing' exercise as part of the ongoing security awareness programme.
- Completed a business continuity test and full disaster recovery test.
- On 30 July 2021, our Cyber Essentials accreditation was renewed, having passed an external security scan of all internet-facing services and an assessment of technical and operational controls.
- IT Governance conducted a cyber security health check which consisted of a review of our information security governance framework, an internal/external vulnerability scan and employee questionnaire (see page 162).

- Implement the recommendations arising from RSM's internal audit of our IT controls and the cyber security health check performed by IT Governance.
- Perform a detailed review of our 'ransomware security incident response playbook' (see page 162).
- Implement further security controls to enhance our layered defence model.
- Enhancing cloud security and anomaly detection for remote workers.
- Enhancing our security patching and mobile device management capabilities to support a hybrid working model.

##### Strategic objectives

1. 2. 3. 4. 5.

##### Business model

Could potentially impact on all aspects of our business model

##### KPIs

- Could impact on any Group KPIs

- Engaged with a portfolio IT partner to provide additional support for ICT infrastructure and cyber security assessments.
- Conducted security reviews on network designs for any new buildings, or refurbishments.
- Ensured that cyber security remains a key consideration in the delivery of intelligent buildings and digital initiatives.
- Continued to collaborate with the IoT Security Foundation and other industry stakeholders on the development of a set of intelligent buildings security guidance documents.
- Sent phishing simulation tests to Building Managers.
- Completed mandatory security awareness training for all staff, including Building Managers.

- Further develop our IT governance framework, security monitoring and security incident response procedures.
- Implement further security controls to enhance our layered defence model.
- Collaborate with our portfolio IT partner on mitigating any cyber risks identified following cyber security assessments.

**What is useful?**

Pennon details its risk appetite relating to technology and security risk. The company also explains actions taken during the period to mitigate these risks and what frameworks have been used as part of the risk management process.

**P: Inadequate technological security results in a breach of the Group's assets, systems and data**

*Long-term priorities*

**1** Failure of our technology security, due to inadequate internal processes or external cyber threats, could result in the business being unable to operate effectively and the corruption or loss of data. This could have a detrimental impact on our customers and result in financial penalties and reputational damage to the Group.

During the period of COVID-19 external cyber threats have continued to increase in both volume and sophistication.

While there has been an increase in remote working, which has introduced additional capacity challenges, IT systems have remained resilient and the Group has maintained a strong preventative and detective information security framework, aligned to guidance issued by the National Cyber Security Centre. South West Water also continues to hold the ISO27001 accreditation.

South West Water has also completed a number of actions during the year as part of the roadmap to meet the requirements of the Network and Information Systems (NIS) directive, with activities aligned to priorities identified by the Drinking Water Inspectorate.

Disaster recovery plans are in place for corporate and operational technology and are subject to regular review.



The Group seeks to minimise technology and security risk to the lowest possible level without detrimentally impacting on the Group's operations.

### What is useful?

Legal & General explains the impact of digital security risks on multiple stakeholders and any actions taken to mitigate these risks.

### Understanding the risks

Providing protection products means that we have to make assumptions about our customers' life spans, how healthy they will be, and how long they will continue with the policy. We seek to price and underwrite our products to take account of these risks, and use reinsurance to manage significant exposures. In delivering our ambition to be a market leader in the digital provision of insurance, as we develop our digital propositions, we are also exposed to technology risks and cyber risks which if not well controlled may lead to both reputational damage and financial loss.

## Suppliers



### Overview

Proactive interaction with our suppliers and treating our suppliers fairly allows us to drive higher standards and reduce risk in our supply chain whilst benefitting from cost efficiencies and positive environmental outcomes.

### Engagement

#### Continuing engagement

- The Legal & General Resources Limited Board, our main contracting entity for suppliers, receives a procurement update at each Board meeting, including an update on material procurements, relationships with suppliers and associated performance. The Group Board has sight of the minutes of each of these Board meetings and any issues are escalated to the Group Board where necessary.
- In accordance with the Group Board matters reserved, any expenditure in relation to a supplier in excess of an amount determined by the group from time to time is put to the Board for consideration and approval, as required.
- The Group Chief Financial Officer and the Legal & General Resources Board continued to receive updates regarding any supplier performance issues associated with Covid-19, including the continued work undertaken with suppliers to mitigate any risks.
- Lesley Knox is the Group Board sponsor for modern slavery and drives this agenda through her membership of the Modern Slavery and Human Rights Committee.

#### Additional current year engagement

- The Executive Risk Committee, Group Risk Committee and Group Technology Committee received reports relating to cyber security and supplier governance throughout the year.
- The Legal & General Resources Board and Group Environmental Committee were updated throughout the year on the progress of topics such as supplier diversity and modern slavery as well as the environment.
- Outputs from a current review of potential supply chain risks due to logistics delays, price increases and shortages will be presented to senior management during 2022.
- Throughout the year the Modern Slavery and Humans Rights Committee has been progressing risk assessments for the balance of our supply chain and has incorporated these results into our Financial Watchlist for material suppliers. See page 50 for information on our sustainable supply chain.

### Outcomes

- This year we joined the Supplier Diversity Council UK to take a lead role in progressing this important topic and help shape the principles and toolkits needed. The Council meets regularly with the objective of raising awareness, sharing knowledge and looking at ways of helping to drive greater opportunity for small and diverse firms.
- We also enhanced our Sustainable Sourcing Principles Statement in November 2021 to bring greater clarity and detail in the guidance to buyers and supplier managers.
- Group Procurement is continuing to progress its five-year transformation journey. Once finalised, this will include the deployment of e-sourcing and supplier management tools which is anticipated to bring more granular analytics as well as digital sourcing capabilities.
- Following feedback from key stakeholders, our purchase order system continues to be utilised to drive payment efficiencies and cost controls.
- Our senior management team worked in collaboration with Stronger Together to deliver external workshops to over 40 suppliers in relation to human rights and spotting the signs of modern slavery. We have also delivered extensive training to promote awareness of this important topic. For more information on our activities in relation to modern slavery, refer to page 51.

### What is useful?

The group's commitment to technology and related risks (and opportunities) is highlighted by the work of the group's technology committee.

For example, in 2021 the Board received detailed training sessions on technology risk and governance, cyber security and IFRS 17. The Board non-executive directors also visited our business operations in different locations and attended one-to-one briefing sessions with key members of the senior management team on a regular basis over the year.

#### Technology Committee

The Technology Committee was established in January 2018 primarily to provide assurance to the Board on the delivery of the group's programme to implement planned enhancements to the group's IT estate, and to ensure the group was operating within its targeted access management, information security and cyber risk appetite. Following the successful delivery of the 2018 enhancements to the IT estate and significant improvements in the group's IT controls, in July 2020 the Technology Committee decided to focus its attention on more strategic matters. As part of this transition, two executive committees reporting into the Technology Committee were refocused to allow the Technology Committee to place reliance on the IT mechanisms and controls in place at an executive level. In addition, the meetings were lengthened to facilitate more comprehensive strategic discussion. The Technology Committee now focuses primarily on the Company's IT, digital and cyber strategies and their implementation plans and strategic technology opportunities for the group.

Its other responsibilities include:

- overseeing the control environment in place for information technology and cyber security.
- overseeing technology aspects of major change programmes and understanding their strategic contribution and risks.
- reviewing risks relating to IT and cyber security and plans for mitigation or treatment.
- reviewing and approving any proposed technology projects and contracts within its remit of responsibility.
- considering current capability relating to technology, cyber and digital skills and plans to address any gaps.
- considering the adequacy, resilience and performance of suppliers and supply chains for IT and cyber.

The group IT community was at the forefront of the group's Covid-19 response as the group moved to a more agile way of working. The Technology Committee continued to assess the impact of Covid-19 on the group's technology estate and our technology suppliers throughout 2021.

In 2021 the Committee:

- received regular updates from the Technology Executive Committee and the Executive Security Committee.
- reviewed risks relating to cyber security and the cyber-resilience of suppliers.
- Focused on the group's cyber security, information security and access management programmes.
- reviewed and endorsed the organisation and operating model in place for IT and cyber security and subsequently considered its ongoing suitability.
- maintained oversight of the overall resilience of the group's IT systems and reviewed and approved divisional technology transformation programmes.
- maintained oversight of the group's IT, digital and cyber strategies and the corresponding implementation plans.
- received deep dive insights into major IT and cyber programmes across the group.
- received updates on the technological threats and opportunities available to the group.
- received updates on the group's data capabilities and the opportunities this could create.
- received presentations from external speakers to provide an overview of industry trends and potential threats in relation to cyber security.

**What is useful?**

Chesnara’s risk disclosures include both appetite and impacts within the body of the ‘risk table’. The company also details key elements of its mitigations for cyber risk and resilience and highlights the impact of recent events, including COVID-19 and Russia on their digital supply chain.

IT/DATA SECURITY & CYBER RISK

PR7

**DESCRIPTION**

Risk of IT/data security failures or impacts of malicious cyber-crime (including ransomware) on continued operational stability.

**RISK APPETITE**

The group aims to minimise its exposure to this risk, to the extent possible, but acknowledges that it may need to accept some risk as a result of carrying out business.

**POTENTIAL IMPACT**

Cyber risk is a growing risk affecting all companies, particularly those who are custodians of customer data. The most pertinent risk exposure relates to information security (i.e. protecting business sensitive and personal data) and can arise from failure of internal processes and standards, but increasingly companies are becoming exposed to potential malicious cyber-attacks, organisation specific malware designed to exploit vulnerabilities, phishing attacks etc. The extent of Chesnara’s exposure to such threats also includes third party service providers.

The potential impact of this risk includes financial losses, inability to perform critical functions, disruption to policyholder services, loss of sensitive data and corresponding reputational damage or fines.

**KEY CONTROLS**

Chesnara seeks to limit the exposure and potential impacts from IT/ data security failures or cyber-crime by:

- Embedding the Information Security Policy in all key operations and development processes;
- Seeking ongoing specialist external advice, modifications to IT infrastructure and updates as appropriate;
- Delivering regular staff training and attestation to the Information Security Policy;
- Regular employee phishing tests and awareness sessions;
- Ensuring the board encompasses directors with information technology and security knowledge;
- Conducting penetration and vulnerability testing, including third party service providers;
- Executive Committee and board level responsibility for the risk, included dedicated IT security committees with executive membership;
- Having established Chesnara and supplier business continuity plans which are regularly monitored and tested;
- Ensuring Chesnara’s outsourced IT service provider maintains relevant information security standard accreditation (ISO27001); and
- Monitoring network and system security including firewall protection, antivirus and software updates.

In addition, a designated Steering Group provides oversight of the IT estate and Information Security environment including:

- Changes and developments to the IT estate;
- Performance and security monitoring;
- Oversight of Information Security incident management;
- Information Security awareness and training;
- Development of business continuity plans and testing; and
- Overseeing compliance with the Information Security Policy.

**RECENT CHANGES / OUTLOOK**

Chesnara continues to invest in the incremental strengthening of its cyber risk resilience and response options.

No reports of material data breaches.

The move to remote working, as a result of COVID-19, had the potential to increase cyber risk for businesses and therefore various steps were taken to enhance security, processes and controls to protect against this.

It is anticipated that cyber-crime campaigns originating from Russia will increase, with some suppliers already reporting an increase in information security threats which some are saying are state sponsored. Although Chesnara is not considered to be a direct target of any such campaigns, all business units have confirmed that they have increased monitoring and detection/protection controls in relation to the increased threat.

**What is useful?**

Next ties digital security risk to business continuity. The company specifies actions it has taken during the period to mitigate the risk and indicates involvement of the board and audit committee in the process.

**Information security, data protection, business continuity and cyber risk**

The continued availability and integrity of our IT systems is critical to successful trading. Our systems must record and process substantial volumes of data and conduct inventory management accurately and quickly. Continuous enhancement and investment are required to prevent obsolescence and maintain responsiveness.

The threat of unauthorised or malicious attack is an ongoing risk, the nature of which is constantly evolving and becoming increasingly sophisticated. Our brand reputation could be negatively impacted by cyber security breaches.

- We operate an Information Security and Data Privacy Steering Committee. Its main activities include agreement and monitoring of related key risks, activities and incidents. The Committee comprises two executive directors and relevant senior management.
- Significant investment in systems development and security programmes has continued during the year, complemented by in-house dedicated information and physical security resources.
- Systems vulnerability and penetration testing is carried out regularly by both internal and external resources to ensure that data is protected from corruption or unauthorised access or use.
- Critical systems backup facilities and business continuity plans are reviewed and updated regularly.
- Major incident simulations and business continuity tests are carried out periodically.
- IT risks are managed through the application of internal policies and change management procedures, imposing contractual security requirements, service level agreements on third-party suppliers, and IT capacity management.
- All staff and contractors are required to read, accept and comply with the Group’s data protection and information security policies, which are kept under regular review and supported by training.
- Information security and data protection risk exposures are reviewed during the year by both the Audit Committee and the Board; this informs an executive-sponsored programme of continuous improvement.

Link to strategy	
Risk trend	



### What is useful?

Convatec, through use of a case study, outlines how external providers have advised on changes to risk mitigation activities and further embedded the importance and visibility of digital security within the company and its supply chain.

Changes made to supplier selection and management as a result of the supply chain review are clearly explained.

### Case study – cyber security and data privacy risks

At the request of the Committee, independent external experts assessed the Group's cyber and privacy maturity against external benchmarks. This has resulted in the strategic approach to improving the Group's cyber security risk mitigations being modified for best practice. This included accountability for privacy being driven deeper into the organisation, heightened risk visibility across the Group, new security testing capability for the Group's strategic focus on Digital and Software as a Medical Device and role-specific training with higher impact.

The Committee also requested a review of cyber readiness of the Group's main suppliers (including raw materials) that may materially impact the Group's business. There is evidence that cyber maturity is growing across the Group's key supplier base, with the majority either being already certified to security standards or recognising the risk and currently taking action to address it. This review resulted in management adopting risk-based supplier supervision for the highest-risk suppliers, including defining a minimum standard of security capability the Group expects from its suppliers, engaging with relevant suppliers to ensure standards are met and developing contingency measures. An oversight survey is to be conducted during 2022 as part of the cyber security strategy adoption of the National Institute of Standards and Technology ("NIST") Privacy Framework.



# Events

## Helping investors understand

## Extract

The impact of events and incidents	<a href="#">Weir</a>
The company's response to a cyber incident or data security issue	<a href="#">Weir</a>
The impact of geopolitical issues on digital security	<a href="#">Chesnara</a>

**Weir**  
**Q3 trading update and Full**  
**Year Results 2021**  
**presentation, [p5](#)**

**What is useful?**

Weir was subject to a cybersecurity incident in September 2021. The company included initial information in its Q3 update to the market. This was supplemented at year end with more detail in the year end results presentation. The timeline and key outcomes provide users with a quick understanding of the event and its impacts quickly.

**RAPID RESPONSE TO CYBER INCIDENT AND SYSTEMS RESTORATION BROADLY COMPLETE**



**Q3 trading update and cybersecurity incident**

The Weir Group PLC is today accelerating the announcement of its Q3 trading update whilst updating the market on its management of a recent cybersecurity incident



The Group has accelerated the announcement of its Q3 trading update.

“We responded quickly and comprehensively to what was a sophisticated external attack on our business. The robust action to protect our infrastructure and data has led to significant temporary disruption but our teams have responded magnificently to this challenge and have managed to minimise the impact on our customers. We will continue to focus on the safe restoration of all our systems whilst strengthening our future resilience even further.”

*Jon Stanton, Chief Executive of Weir – Q3 trading update*

## Weir Annual Report 2021, [p12](#) and [p16](#)

### What is useful?

The annual report covers the cyber incident in detail. The Chairman's statement notes upfront the issue and some of the board's interaction on the topic. This is then reflected through the Chief Executive's statement which covers the operational impact of the event and the financial review which covers key financial impacts. The incident is also reflected throughout the rest of the report with significant detail of the Audit Committee's role and actions and how the incident has fed through to risks and risk reporting.

CHARLES BERRY  
Chairman



#### A GREAT TEAM THAT GETS EVEN BETTER IN THE FACE OF A CHALLENGE

When presented with something as complex as a cyber attack, its impact on ways of working is felt across the whole organisation. As a board, we knew we needed to be utterly clear on our course of action and completely supportive of our colleagues. We decided, strongly, that we would not engage with the attacker. And for our colleagues, we ensured we were visible.

Adversities such as these are the real tests of a team, and the way the whole organisation came together to face the incident head on has made me incredibly proud. I've also been hugely impressed at the leadership shown by Jon and the Group Executive over the past few months, managing the inevitable tensions between getting systems back up as quickly as possible so we can serve customers, while making absolutely sure of a secure IT environment to protect us in the future. These are good tensions – tensions which have helped us find the best answer and made Weir an even stronger team.

The role of a Board is, of course, to act as the ultimate decision-making body in a company, and the representative of its stakeholders. But the Board also has to walk the talk, must be unwavering and supportive of the team in tough times, and take brave decisions in good times. We have done all of the above this year.

#### ACCOUNTABLE TO OUR COLLEAGUES, LISTENING TO, AND LEARNING FROM THEM

In October, the Board visited colleagues at our Todmorden plant in the UK where we heard first-hand about their experiences as they handled the cyber incident. We saw for ourselves how they had adapted to keep the facility running and our customers' orders moving through.

## CHIEF EXECUTIVE'S STRATEGIC REVIEW

# WE HAVE A CLEAR PURPOSE AND STRATEGY TO DELIVER VALUE FOR ALL OUR STAKEHOLDERS

2021 has been a year of strong execution and significant strategic progress at Weir.

Market trends have been favourable, and order momentum is strong. Economic and external factors have made for a complex operating environment – one in which our resilience has shone through.

At the time of writing, we have seen a rapid escalation of events in Ukraine and Russia. Our first priority is the safety of our impacted colleagues; our thoughts are with them and we are doing all we can to support them.

Reflecting on 2021, I am very pleased that we have delivered a good set of results in our 150th anniversary year. That is down to the phenomenal efforts of our employees who have worked safely and tirelessly to serve our customers, protect our communities and support each other through the ongoing Covid-19 pandemic, and during the last quarter when we also responded to a major cybersecurity incident. This performance demonstrates the strength of our culture and I'd like to thank all my colleagues around the world for their commitment and hard work over the last year.

That dedication is also reflected in a creditable set of safety results. Our total incident rate<sup>9</sup> of 0.45 (2020: 0.41) keeps us among the safest companies in our sector. Another year of life and work through the pandemic was not without its challenges, and I am pleased that we have not wavered on our journey to becoming a zero harm workplace.

#### CELEBRATING OUR 150TH ANNIVERSARY

In 2021, we marked 150 years since brothers James and George Weir, both Scottish engineers, established the Company. Throughout 2021 we celebrated James and George's innovation, agility and passion for seeing things differently and while our celebrations took a different form to what we had originally planned, given restrictions due to the pandemic were still largely in place, we adapted, kept our trademark Weir passion and have many special personal memories as a result.

#### STRONG END MARKETS AND STRATEGIC GROWTH INITIATIVES DRIVES ORDER MOMENTUM

2021 saw the global economy continue to recover supporting strong demand for a wide range of commodities, with nearly all well above incentive prices and several at record levels. Across our main exposures of copper and iron ore, average prices were up c.50% on 2020 and average gold prices remained at multi-year highs. Demand for commodities was supported by the economic recovery in the many sectors that had been impacted by Covid-19, underpinned by global stimulus spending, whereas physical inventory shortages and production constraints meant supply struggled to keep up. Given the strength of commodity prices, customers were almost entirely focused on maximising ore production with volumes and machine utilisation continuing to normalise, reaching pre-Covid levels in Q3 and accelerating further in Q4.

Our mining market order growth was strong across all regions, with the exception of Australia, which saw good growth in the previous year but suffered ore production constraints in 2021. Growth was supported by two large OE orders for high pressure grinding rolls (HPGRs) and electric-powered mine dewatering pumps. Infrastructure markets continued their strong recovery with sand and aggregates markets benefiting from residential housing activity, particularly in North America. We also saw very strong growth in industrial markets with orders up by nearly 50%.

JON STANTON  
Chief Executive Officer



FINANCIAL REVIEW

WE SAW  
STRONG ORDER  
GROWTH AND  
OPERATING  
MARGIN  
IMPROVEMENT

“  
THE QUALITY OF OUR  
BUSINESS SHONE THROUGH  
WITH REVENUE, OPERATING  
PROFITS AND MARGINS ALL  
SHOWING PROGRESS WHILE  
LEVERAGE REDUCED.  
”

JOHN HEASLEY  
Chief Financial Officer



OVERVIEW

2021 saw us build a record order book while managing the complexity of raw material and freight inflation and a serious cybersecurity incident. Revenue, adjusted operating profits and margins all showed progress on a constant currency basis while leverage reduced to 1.9 times following receipt of the proceeds from the sale of our Oil & Gas Division. The margin progress was especially pleasing as we fully mitigated inflationary pressures and realised initial benefits from our efficiency programme. The strong order growth and margin performance and operational focus means we are well placed to deliver our medium-term growth, margin and cash conversion objectives.

FINANCIAL HIGHLIGHTS

Continuing operations order input increased 22% on a constant currency basis with less Covid-19 related mine site disruption and supportive commodity prices which drove aftermarket (AM) demand. We also saw higher demand for our more sustainable solutions as we started to see our strong original equipment (OE) project pipeline convert, as customers became more confident in the global macroeconomic backdrop and Covid recovery.

Continuing operations revenue increased 2% on a constant currency basis, with Minerals revenue 1% lower on a constant currency basis following the non-repeat of the large Iron Bridge contract last year being offset by positive aftermarket growth and underlying OE activity. ESCO increased 11% on a constant currency basis reflecting a strong recovery in infrastructure markets in North America and Europe and significantly reduced Covid disruptions to mining customer operations. On a reported basis revenue decreased 2%, impacted by a foreign exchange translation headwind of £70m. Overall book-to-bill at 1.14 reflects the phasing of orders and an element of revenue slippage related to the cybersecurity incident, meaning that we enter 2022 with a record order book.

Continuing operations adjusted profit before tax of £249m was in line with prior year, after a translational foreign exchange headwind of £15m and prior year restatement as explained below. Continuing operations adjusting items reduced by £31m to £40m (2020: £71m) and mainly relates to intangibles amortisation in the current year. Statutory profit for the year after tax from total operations of £259m (2020: loss of £155m) reflects the increases in profit from both continuing operations of £22m and discontinued operations of £392m. The latter reflecting the impairment of the Oil & Gas Division in 2020 and subsequent gain on sale in 2021, which includes the recycling of £103m of cumulative net foreign exchange gains from the foreign currency translation reserve to the income statement, which is only accounted for following completion.

Cash generated from operations decreased by £99m to £266m in the year, including a decrease of £27m from discontinued operations, and reflects an increase in trade and other receivables due to back-end loading of revenues at the end of the year as operations recovered from the cybersecurity incident, together with an increase in inventory as operations geared up to execute a record closing order book. Our reported net debt decreased by £279m to £772m (2020: £1,051m) following a free cash inflow of £62m, plus net proceeds of £283m from the sale of the Oil & Gas Division and the Saudi Arabia based Arabian Metals Company (AMCO) joint venture and an associated reduction in lease liabilities due to the Oil & Gas disposal of £65m. These movements are partially offset by consideration paid for the acquisition of Motion Metrics of £68m, the interim dividend of £30m and foreign exchange retranslation of £32m. Net debt to EBITDA on a lender covenant basis was 1.9 times<sup>8</sup> compared to a covenant level of 3.5 times.

AUDIT COMMITTEE REPORT



STEPHEN YOUNG  
Chair of the  
Audit Committee

“  
THE AUDIT COMMITTEE IS PLEASED TO  
CONFIRM THAT INTERNAL CONTROLS  
REMAINED EFFECTIVE DESPITE THE  
CYBERSECURITY INCIDENT.  
”

STEPHEN YOUNG  
Chair of Audit Committee

AUDIT COMMITTEE DURING 2021

MEMBERS

The Committee is comprised entirely of independent Non-Executive Directors whose biographies are set out on pages 86 to 88.



Clare  
Chapman  
Non-Executive  
Director  
Member since:  
30 April 2021

Ebbie Haan  
Non-Executive  
Director  
Member since:  
25 June 2019

Sir  
Jim McDonald  
Non-Executive  
Director  
Member since:  
1 January 2015

Srinivasan  
Venkatakrishnan  
Non-Executive  
Director  
Member since:  
30 April 2021

MAIN ACTIVITIES DURING 2021

- Reviewed and challenged interim and annual financial reporting, including appropriate reporting and presentation of the disposal of the Oil & Gas Division, the financial impacts of the cybersecurity incident and the preliminary fair value accounting in respect of the acquisition of Motion Metrics.
- Reviewed the results of internal audits in the year and agreed the 2022 internal audit strategy and plan; met with the Head of Internal Audit independent of Executive management.
- Approved the PwC external audit plan; reviewed the effectiveness of the external audit; held independent discussions with PwC's Group Engagement Leader, Kenneth Wilson.
- Reviewed the effectiveness of the Group's risk management and internal control frameworks, comprising internal audit, compliance scorecard process, presentations to the Committee from Divisional Finance Directors, the Group Head of Tax, Group Treasurer and the Chief Compliance Officer.
- Reviewed the outputs of specifically scoped workstreams implemented to provide assurance that the internal control framework remained robust following the cyber incident. A special Audit Committee meeting took place in December 2021 to consider the work performed to date.
- Reviewed the approach to incorporate the Task Force on Climate-related Financial Disclosures requirements and the change in respect of Software as a Service, following the IFRS Interpretations Committee (IFRIC) agenda decision in relation to Configuration or Customisation Costs in a Cloud Computing Arrangement.
- External evaluation concluded the Committee was fulfilling its terms of reference effectively, no significant areas of concern.
- The Committee confirmed the external auditor, PwC, remains independent and that non-audit fees are appropriately approved.

AUDIT COMMITTEE MEETING ATTENDANCE

Members	19-Jan 2021	17-Feb- 2021	22-Jul 2021	26-Oct 2021	14-Dec 2021	Total
Stephen Young	✓	✓	✓	✓	✓	100%
Clare Chapman <sup>1</sup>	n/a	n/a	✓	–	✓	67%
Ebbie Haan <sup>2</sup>	✓	–	✓	✓	✓	80%
Barbara Jeremiah <sup>3</sup>	✓	✓	n/a	n/a	n/a	100%
Sir Jim McDonald	✓	✓	✓	✓	✓	100%
Srinivasan Venkatakrishnan <sup>4</sup>	n/a	n/a	✓	✓	✓	100%

Scheduled Scheduled Scheduled Scheduled Unscheduled

1. Clare Chapman joined the Committee on 30 April 2021; Clare was unable to attend in October due to unscheduled but unavoidable business commitments.  
2. Ebbie Haan was unable to attend in February due to unscheduled but unavoidable personal circumstances.  
3. Barbara Jeremiah stepped down from the Committee on 30 April 2021.  
4. Srinivasan Venkatakrishnan joined the Committee on 30 April 2021.

AREAS OF FOCUS 2022

- Ongoing review over cybersecurity control effectiveness.
- Assess readiness for any future implications from the consultation on reforming UK Corporate Governance, audit and reporting, as published by the Department for Business, Energy and Industrial Strategy in March 2021.
- Extended review of the Group risk assurance framework.
- External review of the effectiveness of the Internal Audit function.

INFORMATION SECURITY & CYBER V

Description	Why we think this is important	How we are mitigating this risk	Key changes during 2021
<p>Failure to adequately protect Weir Group from cyber enabled fraud and other information security risks which can lead to operational disruption, reputational damage, regulatory fines and/or financial impacts.</p> <p><b>Impact on strategy</b></p>  <p><b>Risk owner:</b> Chief Information Officer</p>	<p>Weir's global operations are heavily reliant on its IT systems and infrastructure. As the scale, regularity and disruption of cyber-attacks continues to increase we must recognise this risk and take steps to ensure the business is protected against them.</p> <p>In the last eighteen months, the IT Transformation programme has delivered a number of improvements to reduce the impact of cyber incidents on our business.</p> <p>Our Cyber Security Strategy sets out a three-year programme of activities to further improve our cyber defences and controls.</p> <p>One of the key objectives of the cyber security strategy is to increase our resilience and reduce the impact of a cyber incident in addition to the implementation of preventative measures.</p>	<p>We have an IT governance framework which oversees our technology operations. The IS&amp;T Control Board provides assurance and oversight of our security posture across the business and approves policy and control assessments in relation to cyber risk and IT Security.</p> <p>Security incidents are managed by the cyber security operations team, and any significant cyber security incidents are reported to the Group Executive. Internal and external audit activities are also regularly undertaken to provide additional governance around our control environment as well as highlighting opportunities to make further improvements.</p> <p>An annual cyber security education and awareness plan is in place to ensure colleagues are equipped with the knowledge and awareness they need to use technology safely and securely.</p> <p>The implementation of our IT Transformation and the Cyber Security Strategy roadmap are delivering improvements across multiple areas of the business which in turn will help to reduce the impact of any future cyber incidents.</p>	<p>We have invested in operational capabilities and skills to support the monitoring and resolution of cyber security incidents. These improvements include the appointment of a new Cyber Security Ops Director to lead the transformation of our operational cyber security capabilities. We have also partnered with a highly skilled threat hunting team who will look for issues which cybercriminals may be able to exploit. A number of additional control enhancements were also implemented following the cyber security incident in September 2021.</p> <p><b>Risk trend</b></p>  <p>Our Cyber risk underwent a thorough review following the ransomware incident. The principal conclusion was that our developed risk treatment remained the same and was further underpinned by security control enhancements. The completion of these initiatives, and the continued execution of our approved Cyber strategy, will significantly reduce the impact of any future cyber incident and as such the risk is assessed as remaining unchanged from the prior year.</p>

**ATTEMPTED RANSOMWARE INCIDENT**

The attempted ransomware incident in September 2021 was a sophisticated, determined and prolonged assault on our business. Our swift and robust response to the incident protected our infrastructure and data, meaning we were able to continue meeting the needs of our customers throughout.

All Weir systems have now been restored and a number of improvements introduced in direct response to lessons learned from the incident.

Finally, the Committee received presentations from the Group Head of Tax and the Group Treasurer covering Tax and Treasury Strategy and Risk respectively.

**Cybersecurity incident**

In September 2021, the Group was the target of a sophisticated attempted ransomware attack. On detecting the threat, the Group's cybersecurity systems and controls responded quickly and robust action was taken to protect the Group's infrastructure and data. Forensic investigation, in conjunction with cybersecurity experts, produced no evidence that any data had been exfiltrated or encrypted.

As a result of the incident, the Group took the decision to temporarily remove access to Windows-based PC's and to isolate and shut down IT systems, including the Group's core financial reporting systems, while the threat was assessed. In the days following the incident, processes began to safely restore systems and bring applications back online in a progressive manner and in order of business priority. From a financial reporting perspective, this did lead to some temporary disruption to regular procedures and impacted the Group's usual internal reporting procedures for a short period.

The Committee were updated in their scheduled October meeting on the impact of the cybersecurity incident on the finance function. This included a detailed review of the processes impacted and the early mitigating actions taken to minimise impact and/or risk. In addition, this outlined short-term re-planning of specific finance processes to allow focus on system restorations, ensuring effective controls and data integrity were maintained. Such early mitigating actions included an immediate tightening of controls over the Group's bank accounts and related banking procedures.

The incident necessitated some re-prioritisation of tasks for finance teams globally. The decision was taken to cancel the second half 2021 Compliance Scorecard process and to introduce alternative targeted controls assurance workstreams, focusing on providing assurance post system restores that there were no gaps in the recording of transactions as a result of the incident. A number of planned internal audits were also deferred.

The Committee held an additional meeting in December to receive an update in respect of the response to the incident. The Committee were assured that core systems were promptly restored with no loss of data and that there was limited manual processing.

In terms of additional assurance, the Committee were also presented with an overview of planned inventory counts post the incident, providing good levels of coverage in this specific risk area. We also received a report of the findings from Internal Audit's independent review to confirm that the controls implemented by entities to ensure the completeness and accuracy of data processed during the offline period were adequate. Their review covered heightened risk areas such as payments, inventory and revenue recognition. Tests were performed to confirm that transactions on manual lists were transferred to the ERP system accurately. Additionally, sample testing was performed to confirm the existence of transactions recorded offline, and to confirm that they were approved appropriately. Specific balance sheet reconciliations were reviewed with no exceptions noted. Based on their review and findings, Internal Audit were able to conclude that there were no instances of material breakdowns in controls over the key processes reviewed.

Further updates were provided to the Committee in January 2022. Finally, the Committee received an update in February 2022 which included the results from a self-certification exercise introduced in place of the usual six-monthly Compliance Scorecard process. This involved each company Finance Director completing a standard questionnaire and certifying that appropriate balance sheet rigour had been restored.

The results of these specifically scoped assurance workstreams provided the Committee with comfort that the Group's internal control frameworks, including IT processes and controls, remained stable and effective. We have also taken assurance from the work of PwC in this area.

**(iii) Internal audit**

The Committee has a responsibility to monitor the effectiveness of the Group's internal audit function. During the year, the Head of Internal Audit provides me with copies of all internal audit reports, and presents the results of audit visits and progress against the internal audit plan to the Committee, with particular focus on high priority findings and the action plans, including management responses, to address these areas. Private discussions between myself and the Head of Internal Audit are held during the year and at least once a year with the full Committee.

The above activities provide broad coverage of the function and a good sense of the control environment. This also allows us to ensure the function is effective (which includes assessing the independence of the function), adequately resourced and has appropriate standing within the Company. As with last year, due to the Covid-19 pandemic, most internal audits were performed remotely.

As referred to above, a number of planned internal audits were deferred as a result of re-prioritising across the finance function in response to the cybersecurity incident. The total number of completed internal audits was 28 (2020: 26).

During 2021, Internal Audit has been strengthened further, bringing stronger IT and digital skills to the team and helping enable greater use of data analytics in audits. Once again, in 2021, the internal audit team were supported by guest auditors from across the Group, including Group Finance and Group Tax, providing subject matter expertise for the internal audit team and development opportunities for the guest auditors. Audit actions continue to be closed out efficiently and effectively and improvements have been made in automation, of both the audit and the Compliance Scorecard process. In addition, the Committee were updated on the potential impact of the UK Government's white paper issued by the Department for Business, Energy and Industrial Strategy in March 2021, with some preliminary discussion around potential preparatory actions.

One of the main duties of the Committee is to review the Annual Internal Audit Plan and to ensure that internal audit remains focused on providing effective assurance. As part of the Group's risk management procedures, key sources of assurance are mapped against the Group's core processes and this is used to ensure internal audit planning considers wider internal assurance risk indicators. The factors considered when deciding which businesses to audit and the scope of each audit, including consideration of the number of visits to each operating company in the Group on a cyclical basis are, amongst other things, the volatility of end markets, critical system or Senior Management changes in the year, financial results, the timing of the most recent internal audit visit, assessments from other assurance reviews undertaken and whether the business is a recent acquisition. In addition, the emergence of any common themes or trends in the findings of recent internal audits or Compliance Scorecard submissions (see previous section) is taken into consideration. Planning is further assisted by a risk modelling tool for dynamic risk prioritisation of audits.



Financial Reporting Council

Reports and information about the Lab can be found at <https://www.frc.org.uk/Lab>

The FRC does not accept any liability to any party for any loss, damage or costs howsoever arising, whether directly or indirectly, whether in contract, tort or otherwise from any action or decision taken (or not taken) as a result of any person relying on or otherwise using this document or arising from any omission from it.

© The Financial Reporting Council Limited 2022

The Financial Reporting Council Limited is a company limited by guarantee.

Registered in England number 2486368. Registered Office:

8th Floor, 125 London Wall, London EC2Y 5AS

**Financial Reporting Council**

8th Floor  
125 London Wall  
London EC2Y 5AS  
+44 (0)20 7492 230

[www.frc.org.uk](https://www.frc.org.uk)

Follow us on  
 Twitter [@FRCnews](https://twitter.com/FRCnews)  
or  [LinkedIn](https://www.linkedin.com/company/frc).