Audit Committee Breakfast Briefing

17 October 2023

IAASA
Irish Auditing & Accounting Supervisory Authority

1. Welcome & Introduction

Kevin Prendergast

Chief Executive

IAASA
Irish Auditing & Accounting Supervisory Authority

Disclaimer

Disclaimer

The views expressed by the IAASA speakers are our own and do not necessarily reflect the views of the Authority, Board or the staff of IAASA

The view expressed views expressed by the guest speakers here today are their own personal views and do not necessarily reflect the views of their respective boards or organisations.

This presentation, extracts or sections thereof may not be published or distributed to any third party without the express permission of IAASA

This event will be recorded to be uploaded to IAASA's website

Audience Participation

Physical Attendees

Type SLI.DO in address bar of browser

Passcode: **IAASAACBriefing2023**

Virtual Attendees

SLI.DO

- Access built into Virtual Platform – see right hand sidebar
- Respond to the questions posed for each session
- Ask your own questions

Slido questions

Pre-event questions

- what are you hoping to gain from today's discussions?
- In the past 12 months how would you rate your committee’s/boards preparations on sustainability reporting?

Agenda

1.	Welcome & Introduction	8:30-8:40
2.	Regulatory Update	8:40-9:10
3.	EC Developments Q&A	9:10-09:40
4.	Sustainability Reporting Case Study	09:40-10:10
	Break	10:10-10:30
5.	Audit committee panel session	10:30-11:20
6.	Cybersecurity update	11:20-11:50
7.	Closing comments	11:50-12:00

Slido questions

- What is the key emerging topic that audit committees have had to deal with in 2023?

2. Regulatory Update

Maurice Barrett

Senior Manager

Financial Reporting Supervision

Barry Murphy

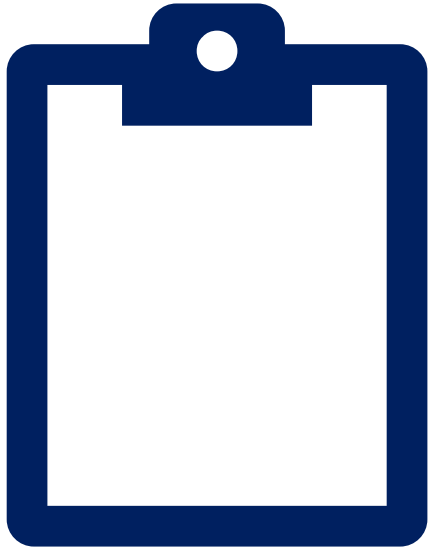
Senior Inspector

Audit Quality

IAASA

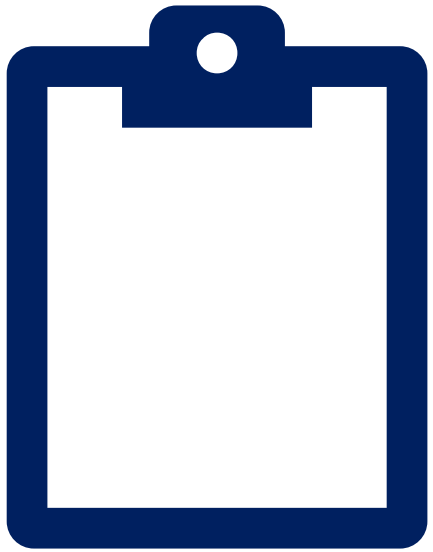
Irish Auditing & Accounting Supervisory Authority

Agenda – Part 1



- AQU update
- 2022 key findings arising
- 2023 inspection areas
- CSRD update

Agenda – Part 2



- FRSU update
- Topical financial reporting issues
- IAASA 2023 Observations document
- ESMA 2023 Common Enforcement Priorities

AQU update

Inspection Cycles

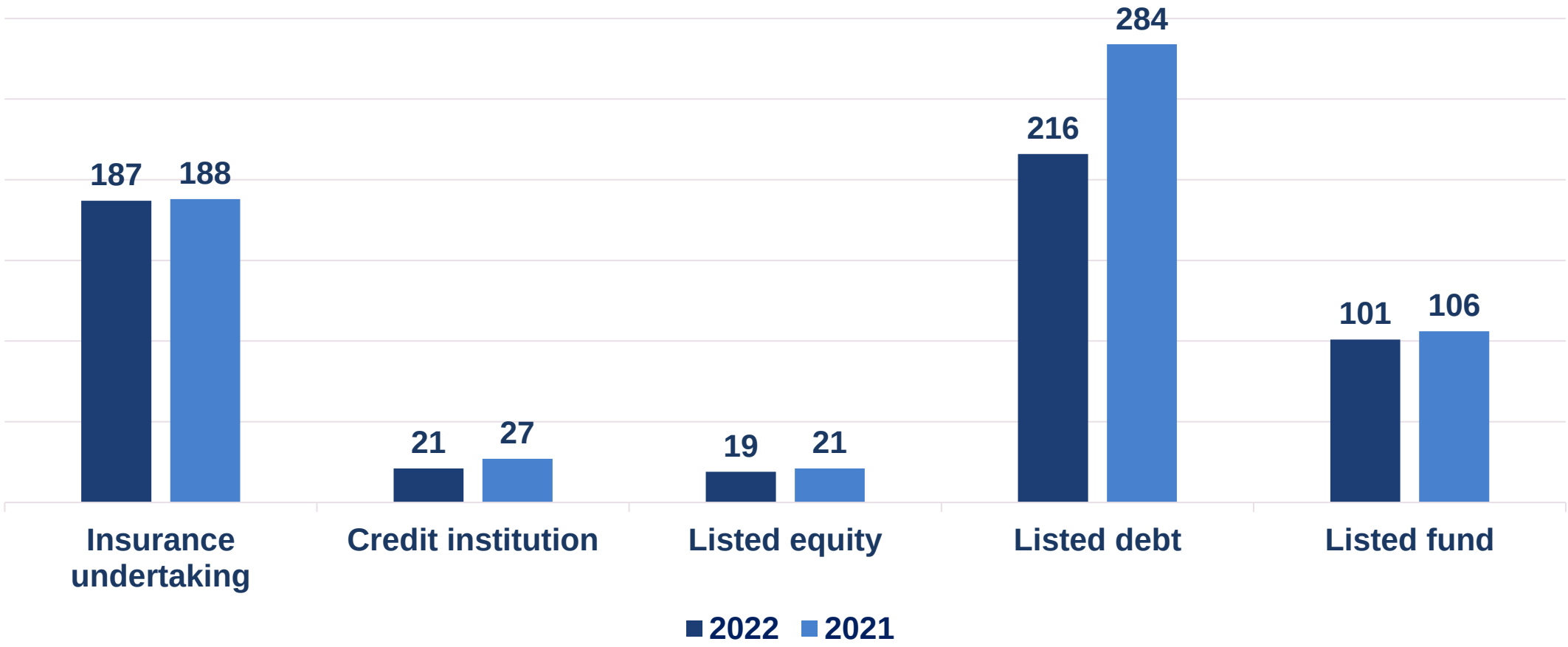
Number of PIE audit firms: 7

Risk selection model

Audit inspections

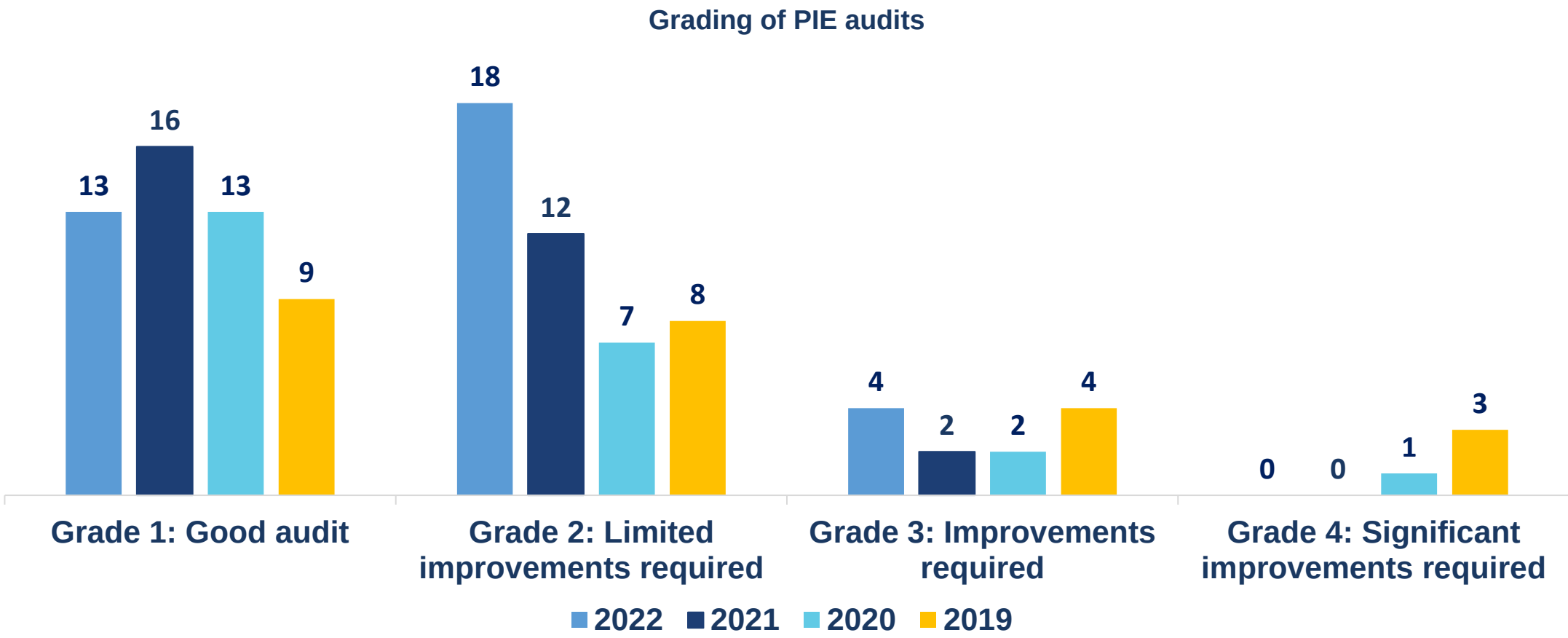
- Hybrid inspection model
- ISQM 1
- Audit Committee discussion

PIE Population



Audit inspections – grading

Individual Audit Inspections: 1 → 4 Grading



2023 audit inspection areas

- Audit Evidence Areas – specific to audit
- Management override of controls
- Communication with TCWG
- Related Parties
- Subsequent Events
- Opening Balances/Initial audit engagements
- Financial Statement review
- EQC Review

ESRSs

- Delegated Act adopted on 31 July 2023
- Significant changes made to the EFRAG version of the standards including:
  - change to timing of phasing in, meaning only companies with more than 750 employees have to comply in 2024
  - for three years from the date of implementation by any company, the standards allow that disclosures can be left out, once an explanation is provided. This is to allow companies a further three years to develop systems to gather the information
  - all data points are now subject to materiality. Certain data points were designated as mandatory by EFRAG, they have now all been subjected to materiality assessment

Transposition into Irish law – status and expectations

- Policy decisions have been finalised and announced
- Policy intention is to provide as much flexibility as permitted in the Directive
- Commercially sensitive data can be omitted
- Sustainability assurance service provider can be different to your statutory auditor
- Independent assurance service providers will not be permitted initially but will be further considered in 2024

Sustainability enforcement regime

IAASA remit will expand to:

- Reviews of reporting for issuers (same issuers as for accounting enforcement)
- Inspection of sustainability assurance for public interest entities
- Oversight of the licensing, quality assurance, CPD and disciplinary regimes for all sustainability assurance service providers
- Adoption of assurance standard (until EC adopts a standard)
- Enforcement powers in relation to all of the above

AQU Key Messages

AQU thematics/insight series

- Materiality
- Communications with TCWG
- Disclosures
- ISQM 1 observations

Financial reporting update – agenda

1. Topical financial reporting issues

2. IAASA 2023 *Observations* paper

3. ESMA 2023 Common Enforcement Priorities (ECEPs)

Some topical financial reporting issues – current year matters

TOPIC	OCCURENCES
Transparency Directive Regulations	8
IAS 36 *Impairment of Assets*	7
IFRS 7 & IFRS 9 – banking	5
IFRS 8 *Operating Segments*	5
Alternative performance measures (APMs)	4
European Single Electronic Format (ESEF)	4
Climate risks & ESG	3

Some topical financial reporting issues – expected 2023 matters

- IFRS 17 *Insurance Contracts*
- IAS 1 – ~~significant~~ material accounting policies
- IAS 8 – definition of accounting estimate
- Amendments to IAS 12 – Pillar II – endorsement status?

IAASA 2023 ***Observations*** paper

Published 3 October 2023

UNCERTAINTY	AREAS OF FOCUS	
Easing growth momentum amid declining inflation and robust labour market	Macro-economic impacts	Financial instruments – IFRS 7 *Financial Instruments: Disclosures* & IFRS 9 *Financial Instruments*
Inflation with domestic price increases at their highest level in 38 years	Fair value measurement and disclosures	IFRS 8 *Operating Segments*
High inflation has led to tighter monetary policies	Transparency Directive Regulations	Alternative performance measures (APMs)
Uncertainty affects us all	IAS 36 *Impairment of Assets*	European single electronic format (ESEF)
		Amendments to IFRSs

ESMA 2023 Common Enforcement Priorities (ECEPs)

ESMA 2023 Common Enforcement Priorities (ECEPs) – expected late October 2023

- **Climate-related matters**
  - consistency between financial statements and non-financial information
  - existence of impairment triggers arising from climate-related matters
  - disclosures surrounding green-financing
- **Macro-economic impacts**
  - increase in interest rates and impact on (re-)financing
  - fair value measurements and disclosure
- **Alternative performance measures** – ESMA APM Guidelines
- **European Single Electronic Format** (ESEF)
- **Sustainability reporting**

Useful links

Audit inspections	Financial reporting
IAASA.ie	*Observations* paper
Quality Assurance Reports 2022	Enforcement Decisions
Annual Audit Programme & Activity Report	Annual Activity Report
Thematics and Observations	Information Notes
	ESMA 2023 Common Enforcement Priorities

3. EC Developments Q&A

Sven Gentner

Head of Unit, DG FISMA, European Commission

IAASA
Irish Auditing & Accounting Supervisory Authority

4. Sustainability Reporting Case Study – Musgrave Group plc

Andrew Keating
CFO, Musgrave Group
Michael Kelleher
Director of Finance, Musgrave Group

IAASA
Irish Auditing & Accounting Supervisory Authority

Slido

- What is your understanding of value chains from a sustainability perspective?
- What is your understanding of the double materiality concept?
- For issuers implementing the sustainability standards in 2024 & 2025, what are the most significant challenges ahead of them

IAASA Audit Committee Briefing 2023

Musgrave

BREAK

The briefing will recommence at 10.30

IAASA
Irish Auditing & Accounting Supervisory Authority

6. Audit committee panel session

Panel Session

IAASA
Irish Auditing & Accounting Supervisory Authority

Slido

- What is the biggest challenge for your organisation in implementation of the sustainability standards?
- Does your board/committee receive adequate training to perform their respective roles?
- Are positions on audit committees an attractive proposition?
- Is cybersecurity an active topic your board’s/committees’ agenda?

Overview

- Sustainability reporting preparations
- Audit Committee training
- Cyber risk

6. Audit committee panel session

Panel Session

Questions?

6. Cybersecurity

Dr Caroline McGroary

Ass. Professor Accounting, DCU

IAASA
Irish Auditing & Accounting Supervisory Authority

Slido

- What do you believe are the major challenges facing management/boards when navigating the cybersecurity landscape? (Tick all that apply)
- Do you believe you have received the appropriate cybersecurity training to allow you to appropriately understand and navigate a cyber-attack?

Cybersecurity: The Role of the Accounting Profession

Irish Auditing and Accounting Supervisory Authority (IAASA)

Audit Committee Briefing 2023
17 October 2023

Dr. Caroline McGroary

Dublin City University

DCU
Ollscoil Chathair Bhaile Átha Cliath
Dublin City University

Dr. Caroline McGroary

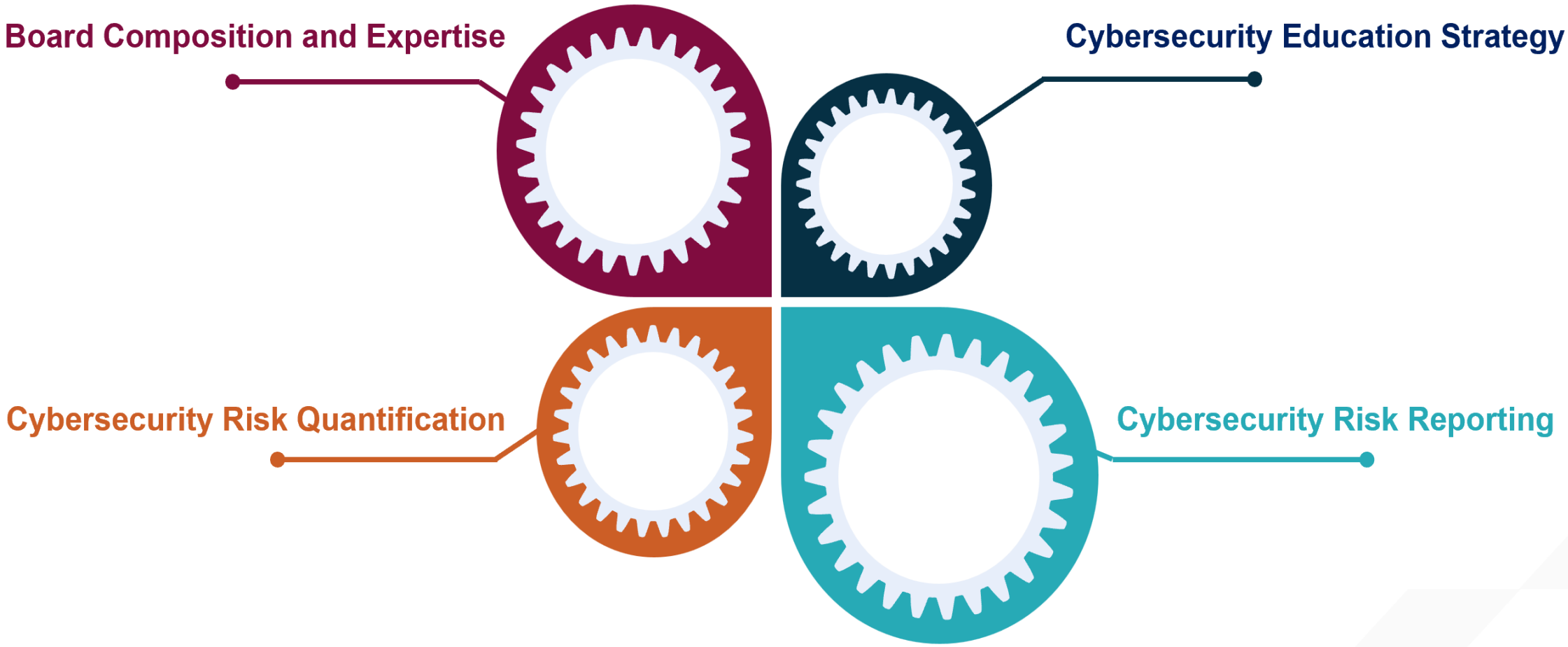
Chartered Accountant, Fulbright Scholar, Lecturer in Accounting

About

- Chartered Accountant, FCA
- Ass. Professor of Accounting, Finance and Business Strategy, Dublin City University, Ireland and Saudi Arabia
- PhD in Professional Accounting Education
- Fulbright Scholar in Cybersecurity, Boston College, USA, 2022

caroline.mcgroary@dcu.ie // https://www.linkedin.com/in/carolinemcgroary/

Cybersecurity Risk Management



Cybersecurity Risk Management

Board Composition and Expertise

- Competing demands: cyber risk v's other business risks
- On agenda of boards: Driven by regulators, customers and investors
- Increased CISO/CIO representation on the board: need clear communication strategy
- CFO/Finance Director has an important intermediary role to play between IT and the Board

Cybersecurity Risk Management

Cybersecurity Education Strategy

- Enterprise-wide specialised training required e.g. Finance team high risk
- Simulated exercises e.g. incident response training (including testing backups)
- Key Relationships e.g. An Garda Síochána, Third-party consultants

Cybersecurity Risk Management

Cybersecurity Risk Quantification

- Need to better understand how to quantify cyber risk e.g. cyber risk assessment score
- Inventory of assets e.g. rebuild costs, disposal of IT assets, intangible assets (brand)
- Cyber insurance: Increasing premiums, changing policy cover
- Policy for incident response e.g. ransomware payments, access to bitcoin
- Potential lawsuits

Governance Considerations

Cybersecurity Risk Reporting

- ESG or ESGC Reporting
- Lack of consistency in current reporting
- American Institute of Certified Public Accountants (AICPA) Framework
- U.S. Securities and Exchange Commission (SEC) Regulations
- National Institute of Standards and Technology (NIST) Cybersecurity Framework
- Directive on the security of Network and Information Systems (NIS2)

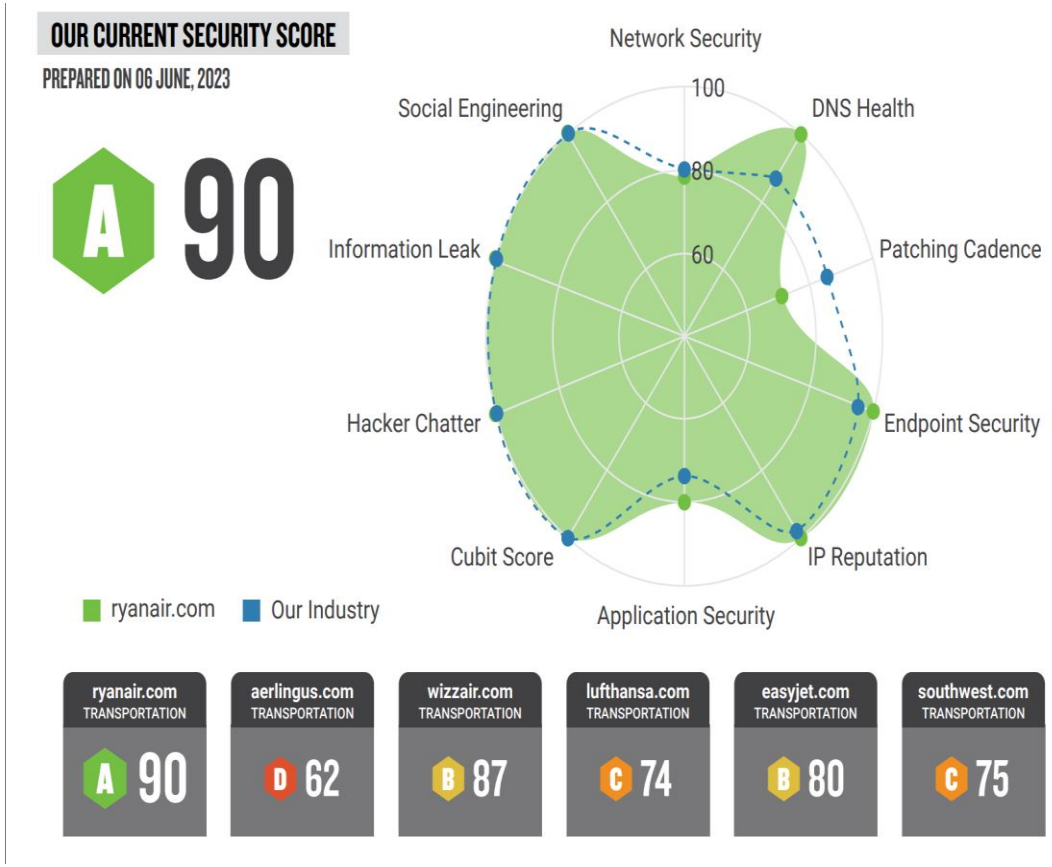
Cybersecurity Reporting: Ryanair

Company Description: Ryanair Holdings plc is Europe's largest airline group and parent company of Ryanair, Ryanair UK, Buzz, Lauda and Malta Air.

Cyber security is a key focus area in which the Group invests heavily in and in FY23 we doubled the size of our 24/7 security team.

We have an incident response agreement with Cyber Security firm, Madiant, to provide additional cyber security support. During the year we also successfully completed the EU Network and Information Systems (NIS) Directive Audit and the Civil Aviation Authority's (CAA) Cyber Security CAF Audit.

We are proactive in our Cyber Security tests. We frequently conduct simulated phishing tests with our people, with those failing the test required to undergo additional training. Cyber Security assessments are also done during the onboarding of new suppliers.



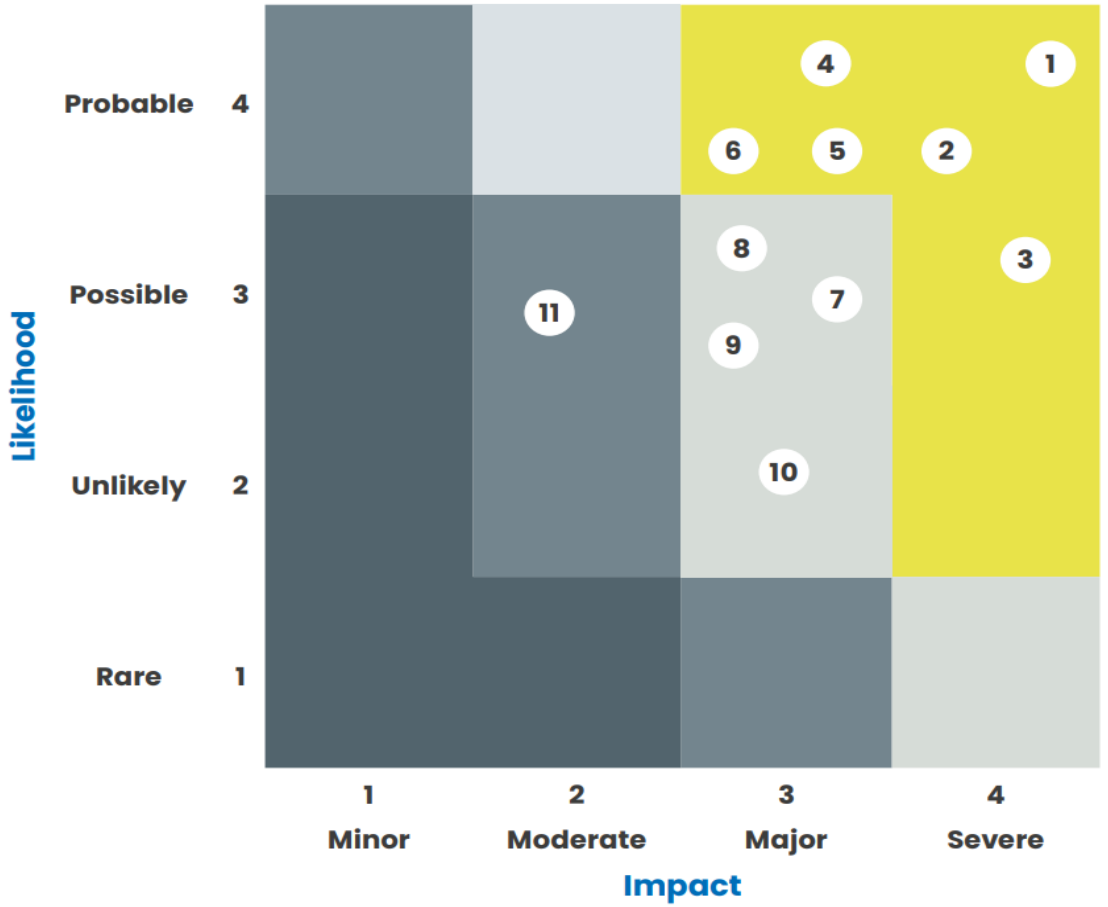
Source: [Ryanair Sustainability Report 2023]

Cybersecurity Reporting: Grafton Group

Company Description: Grafton is the largest DIY, Home and Garden retailer in Ireland, trading from 35 stores nationally and online under the Woodie's brand.

Group's principal risks

1. Macro Economics
2. Cyber Security and Data Protection
3. Acquisitions and Integration of New Businesses
4. Supply Chain
5. Colleagues – Retention, Recruitment, Succession, Diversity, Wellbeing
6. Competition
7. IT Systems Implementation
8. Health and Safety
9. Sustainability and Climate Change
10. Internal Controls and Fraud
11. Pandemic Risk



Source: [Grafton Group Annual Report 2022]

Cybersecurity Reporting: Grafton Group

Cyber security and data protection

Risk movement

Strategic links

Risk description

Increased levels of cybercrime represent a threat to the Group's businesses and may lead to business disruption or loss of data. The Group is exposed to the risk of external parties gaining access to Group systems and deliberately disrupting its business. This includes the risk of ransom demands, a material loss of revenue and profitability while systems are being restored, stolen information or fraudulent acts.

Theft or leakage of data relating to employees, business partners or customers may result in a regulatory breach and could impact the reputation of the Group.

Mitigation

The Group has a number of IT security controls in place including gateway firewalls, intrusion prevention systems and anti malware software. The Group has a suite of information security policies, which are communicated to colleagues, through mandatory online training and regular security awareness campaigns.

Regular IT audits are carried out in the Group's businesses to test these controls. The Group has put in place a Security Incident Management Plan and each business has their own cyber incident response and backup plans which are regularly rehearsed.

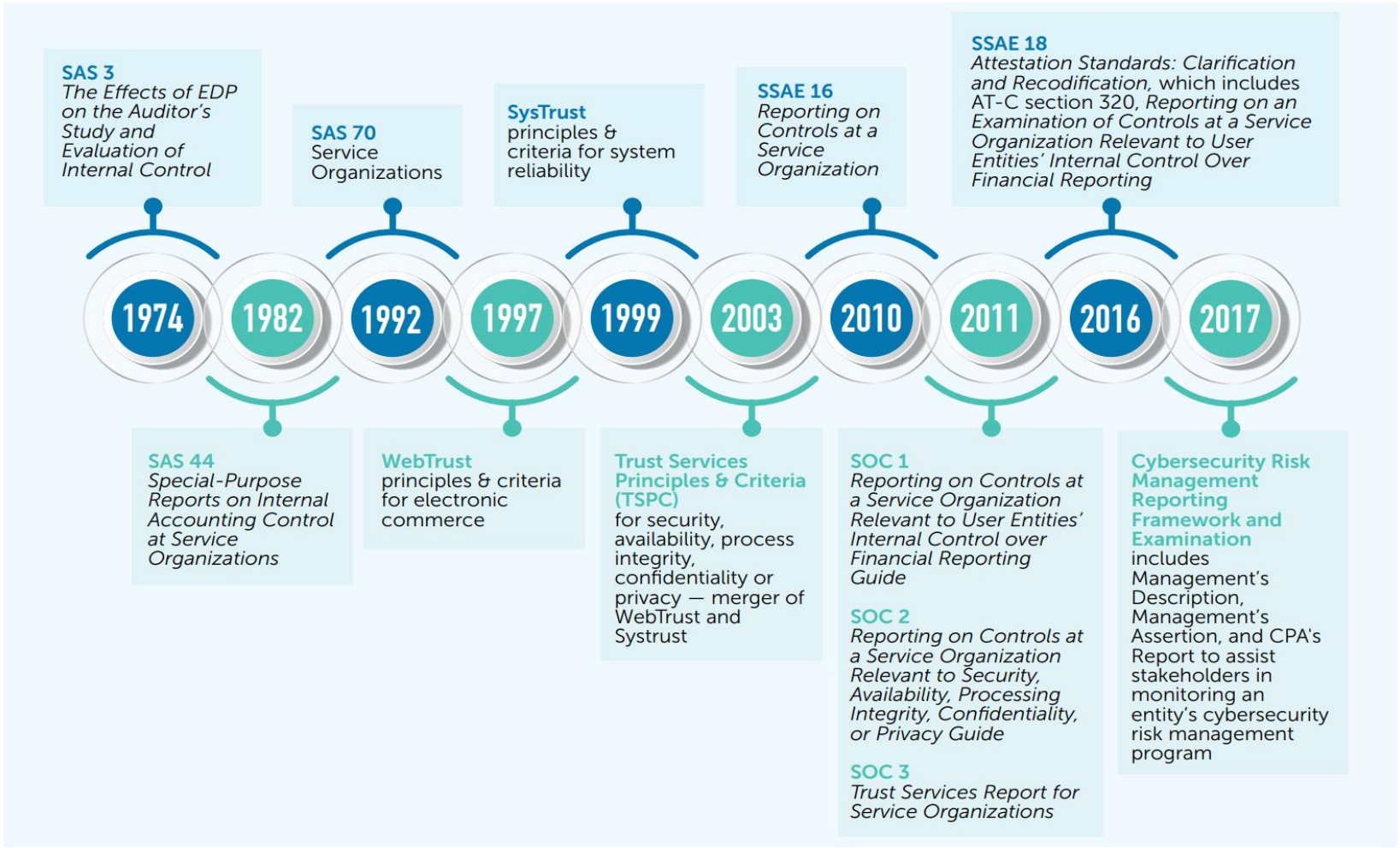
Following a review of the Group's cyber security maturity by third party specialists in 2021, a programme of initiatives was commenced in 2022 to further reduce cyber risk. This has been overseen by the Group's Information Security Steering Committee through the monitoring of quarterly assessments by IT teams which have been verified by Group Internal Audit.

During 2023 a second review of the cyber security maturity will be conducted to confirm the progress made and identify any further steps that need to be taken to improve the Group's ability to both prevent and reduce the impact of any attack occurring.

A Group-wide programme to implement GDPR was completed in 2018 and compliance activity has now been embedded into business processes, with roles established in each business unit to co-ordinate ongoing activities. This includes ensuring that all new businesses acquired by the Group meet the same group Data Protection standards. The Group continues to evaluate and invest in new technology to maintain and improve its Data Protection management processes and controls.

Source: Grafton Group Annual Report 2022

The Role of the Accounting Profession



Key Takeaways

The Irish Times
https://www.irishtimes.com › special-reports › 2023/08/24

Scale of cybercrime is 'breathtaking'

24 Aug 2023 — According to specialist research firm **Cybersecurity** Ventures, global cybercrime is predicted to cost $8 trillion this year alone.

Financial Times
https://cybersecuritydavos.live.ft.com

Cyber Security: A Leadership priority - Financial Times

Cyber security is a **board-level responsibility** and intrinsically linked to ESG risk. What are the strategic, regulatory and commercial imperatives of ...

Finance Professionals Offer Powerful Defense Against Cybersecurity Threats

The 2022 AFP Payments Fraud and Control Survey found that 71 percent of organizations were victims of payments fraud attacks or attempts...

The Irish Times

Cyber security spending remains high on agenda for Irish companies

Almost half of Irish businesses are planning to increase spending on cyber security this year, as companies keep the issue at the top of the...

Revolutionize Board Engagement With Cyber Risk Quantification

Emerging cyber risk quantification methods are allowing boards to ask “what if” questions if operating conditions change, and to align cyber...

Financial Times

Risk managers warn cyber insurance could become 'unviable product'

Concerns grow over insurers failing to cover big state-backed attacks.

Cybersecurity budgets under pressure at small businesses, new research shows

Companies are set to cut their cybersecurity budgets by up to half in 2023, despite the risk of cyber attacks, a new survey has found.

Most mid-sized businesses lack cybersecurity experts, incident response plans

Mid-sized businesses in US and Canada face cybersecurity challenges, with gaps in toolkits, planning, staffing, training, and insurance.

Cybersecurity Is a Shared Responsibility

Cybersecurity threats and data breaches keep me up at night. The digital world in which we now live in is continuously changing.

Thank you

DCU Ollscoil Chathair Bhaile Átha Cliath Dublin City University

8. Closing Comments

Kevin Prendergast

Chief Executive

IAASA
Irish Auditing & Accounting Supervisory Authority