GDPR & Corporate Governance

The Role of Internal Audit and Risk Management One Year after Implementation

Live Webinar #4 – Thursday 5 December 2019

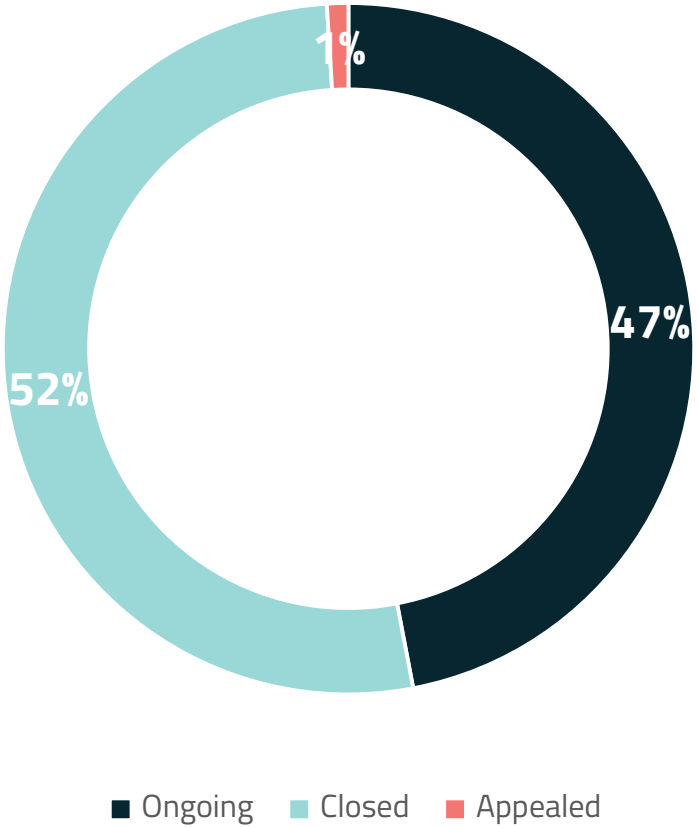
FERMA

ECIIA

GDPR : **where do we stand?**

Framework :

- **27th April 2016** : Adoption
- **6th May 2018** : Application
- **May 2020**: Public evaluation report by the Commission in May 2020 and transmitted to the European parliament and to the Council
- **2020** : E-PRIVACY
- **April 2019 :** European Data Protection Board report: COOPERATION – CONSISTENCY – STANDARDISED for Supervisory Authorities
- **July 2019 – European Commission** Communication taking stock of one year application of the GDPR
- **June 2019** - **European Commission** report of the multi-stakeholder group



Total 206326

Complaints
94622

Data breach notifications
64684

Other
47020

SAs from 11 EEA countries imposed a total of €55.955,671 in fines

GDPR : **where do we stand?**

A joint project carried out between ECIIA and FERMA, with the support of 5 IIA national Institutes and 11 national risk management associations.

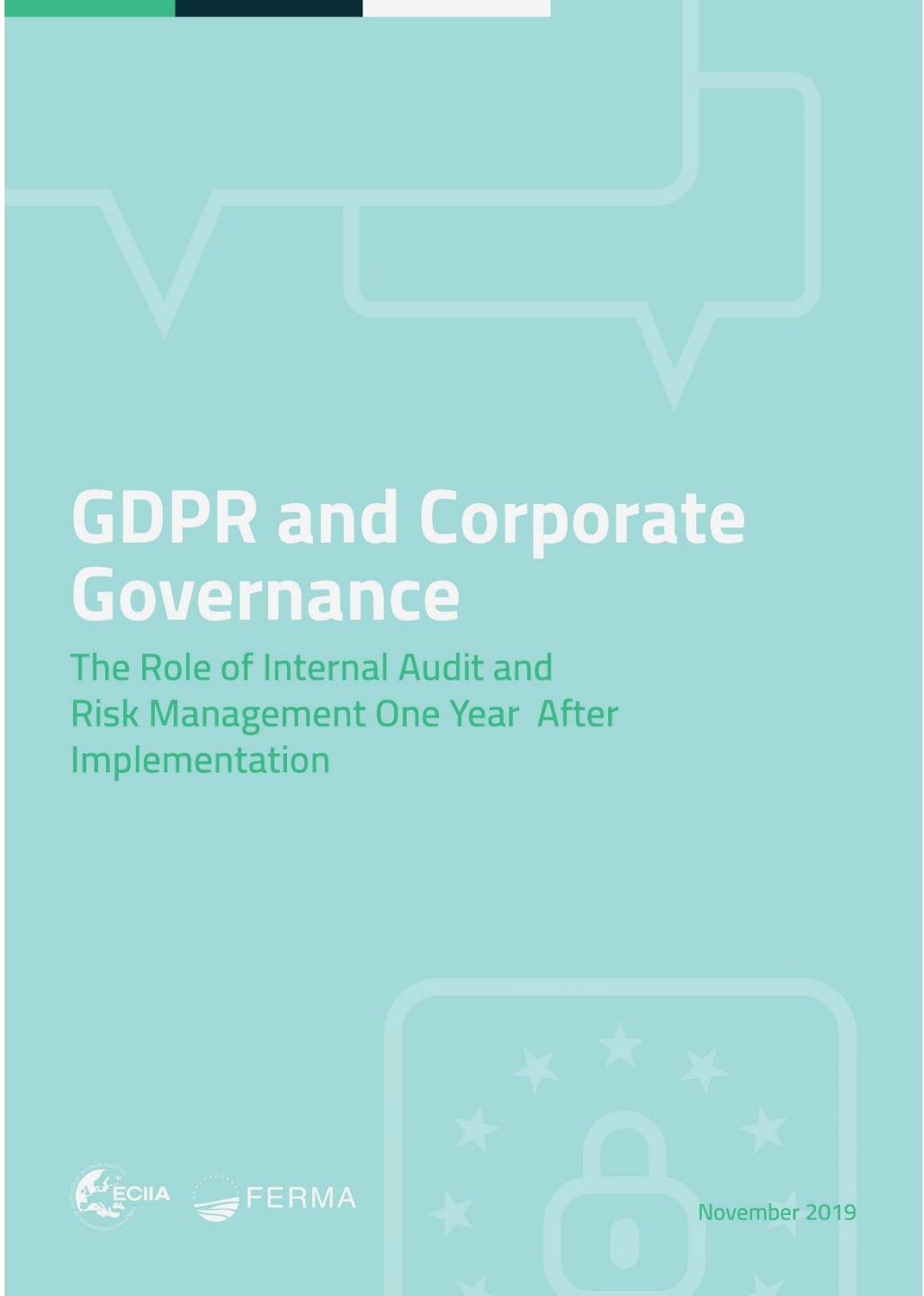
Our ambitious objectives were to:

- **Collect** "best practices" and key challenges related to GDPR from a large panel of practitioners.
- **Promote** good governance and internal audit and risk management alongside the GDPR.
- **Provide** facts and tangibles to be used as an advocacy tool for the new GDPR guidelines.

Up to 19
Questions in total

346
respondents

25
Interviewees



GDPR : **expert's introduction**

Lene Ritz

Chief Risk Officer & Team leader
Energinet (Denmark)

Ralf Herold

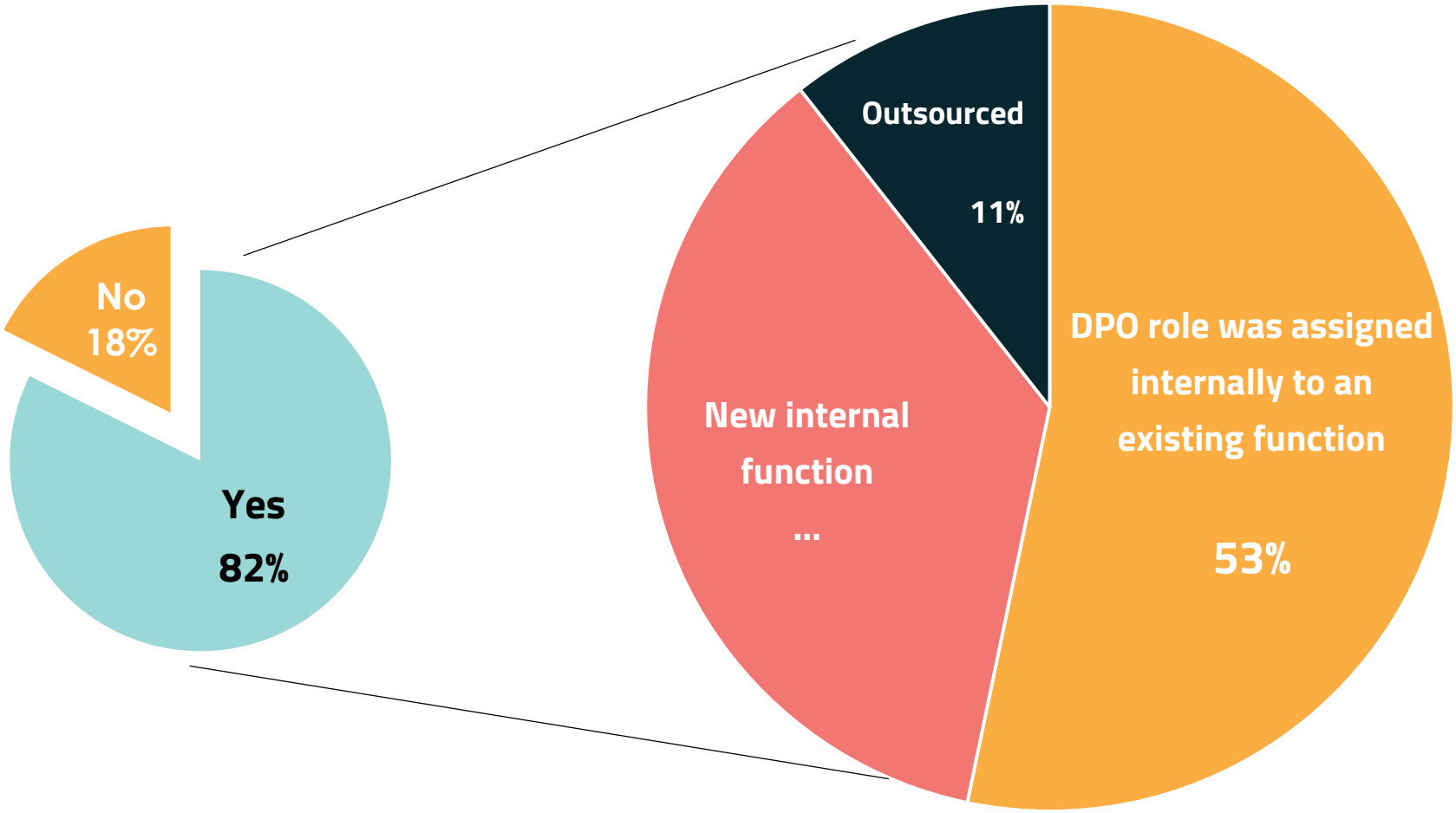
SVP Corporate Audit
BASF (Germany)

GDPR : **Polling question #1**

Do you have a DPO internally or as outsourced function ?

- Internally – new function
- Internally – existing function
- Outsourced
- Other

Do you have a DPO internally or as outsourced function ?



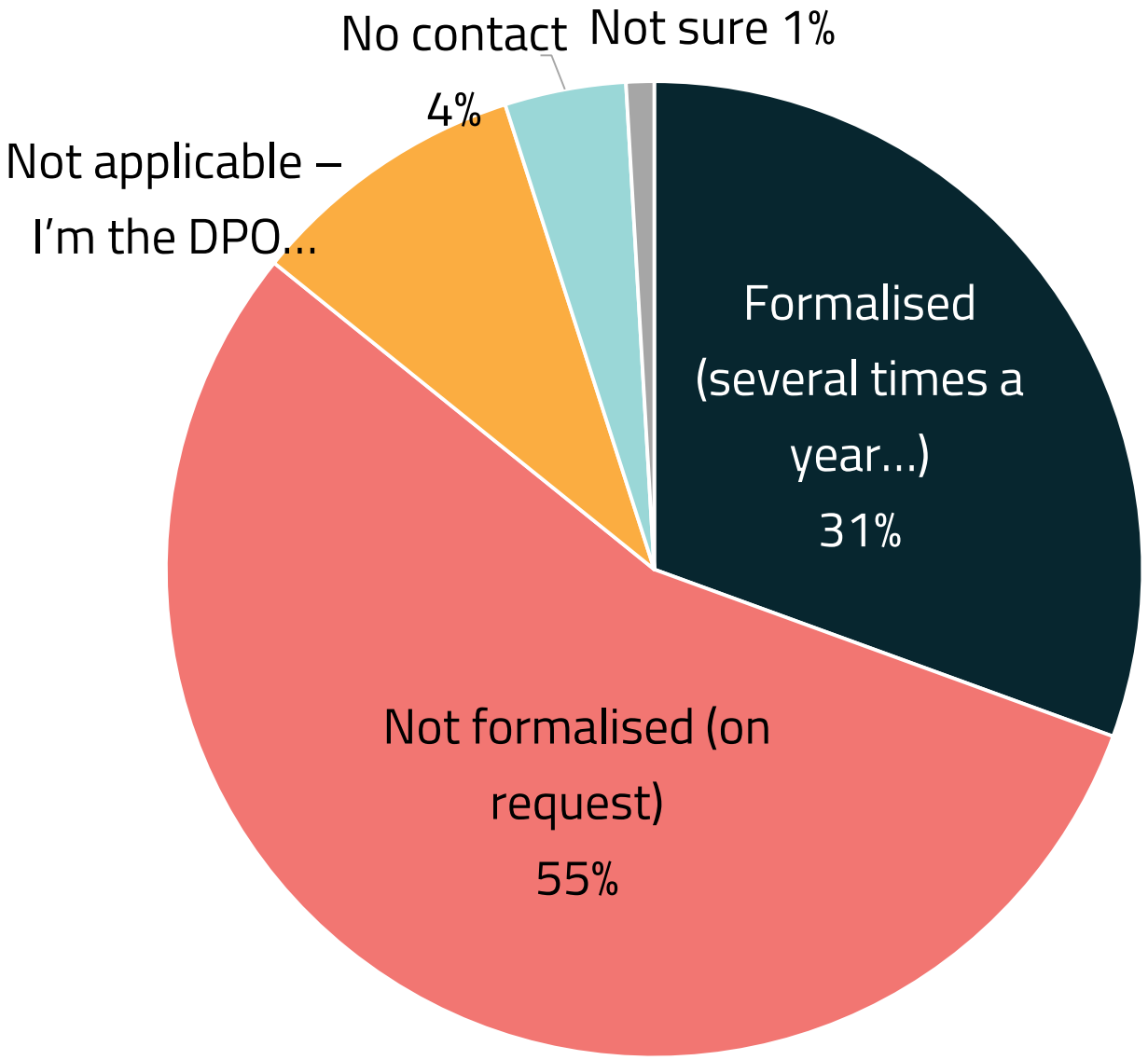
1. Legal - Compliance : **54%**
2. IT - IS : **15%**
3. Risk Management : **11%**
4. Operations - Finance : **10%**

GDPR : **Polling question #2**

What is your level of interaction with the DPO ?

- Formalised
- Not Formalised
- No contact
- Not applicable

What is your level of interaction with the DPO ?



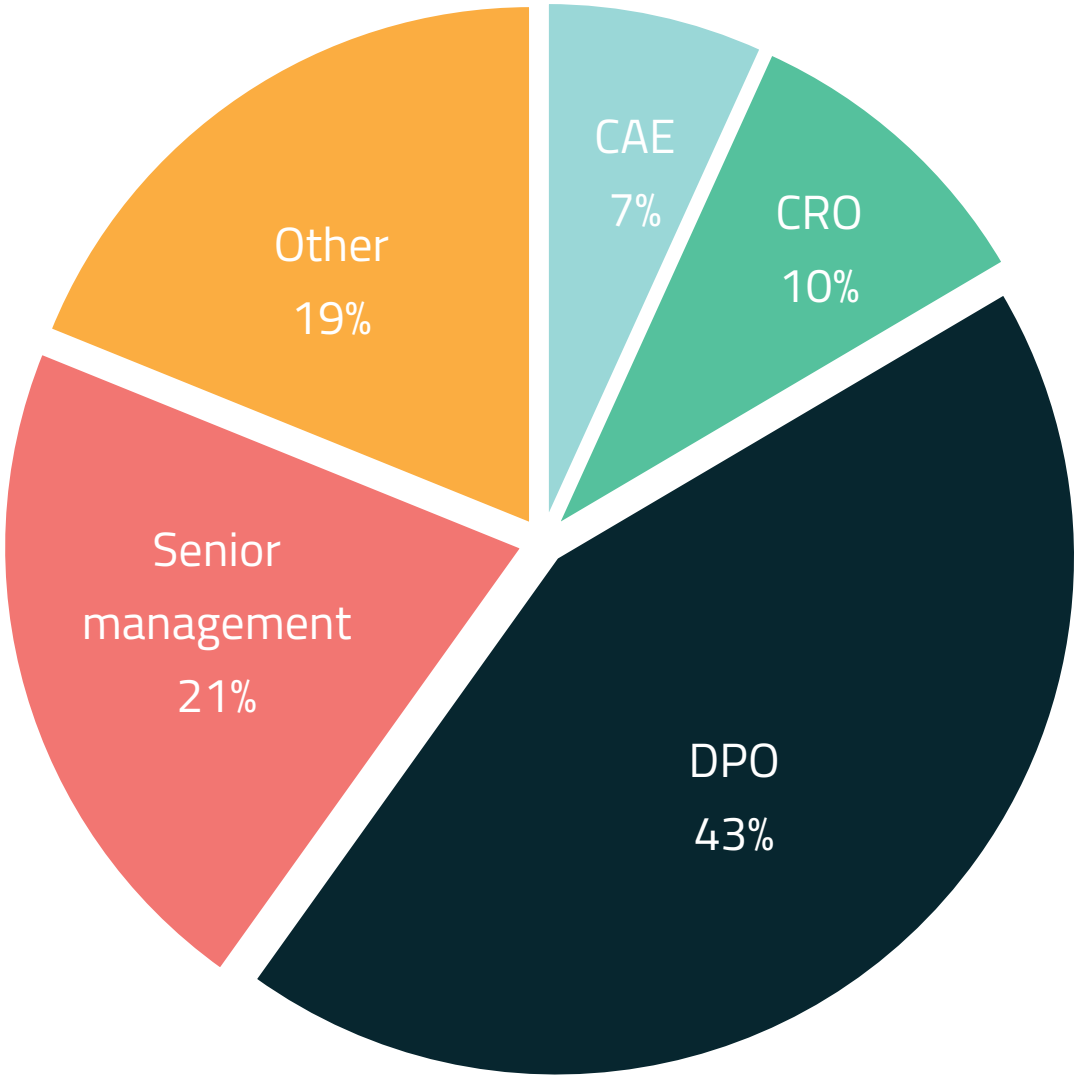
86% in contact

GDPR : **Polling question #3**

In your organisation, who is in charge of reporting to the Board about data privacy matters including GDPR ?

- DPO
- Senior Management
- CRO
- CAE
- Other

Who is in charge of reporting to the Board about data privacy matters including GDPR?

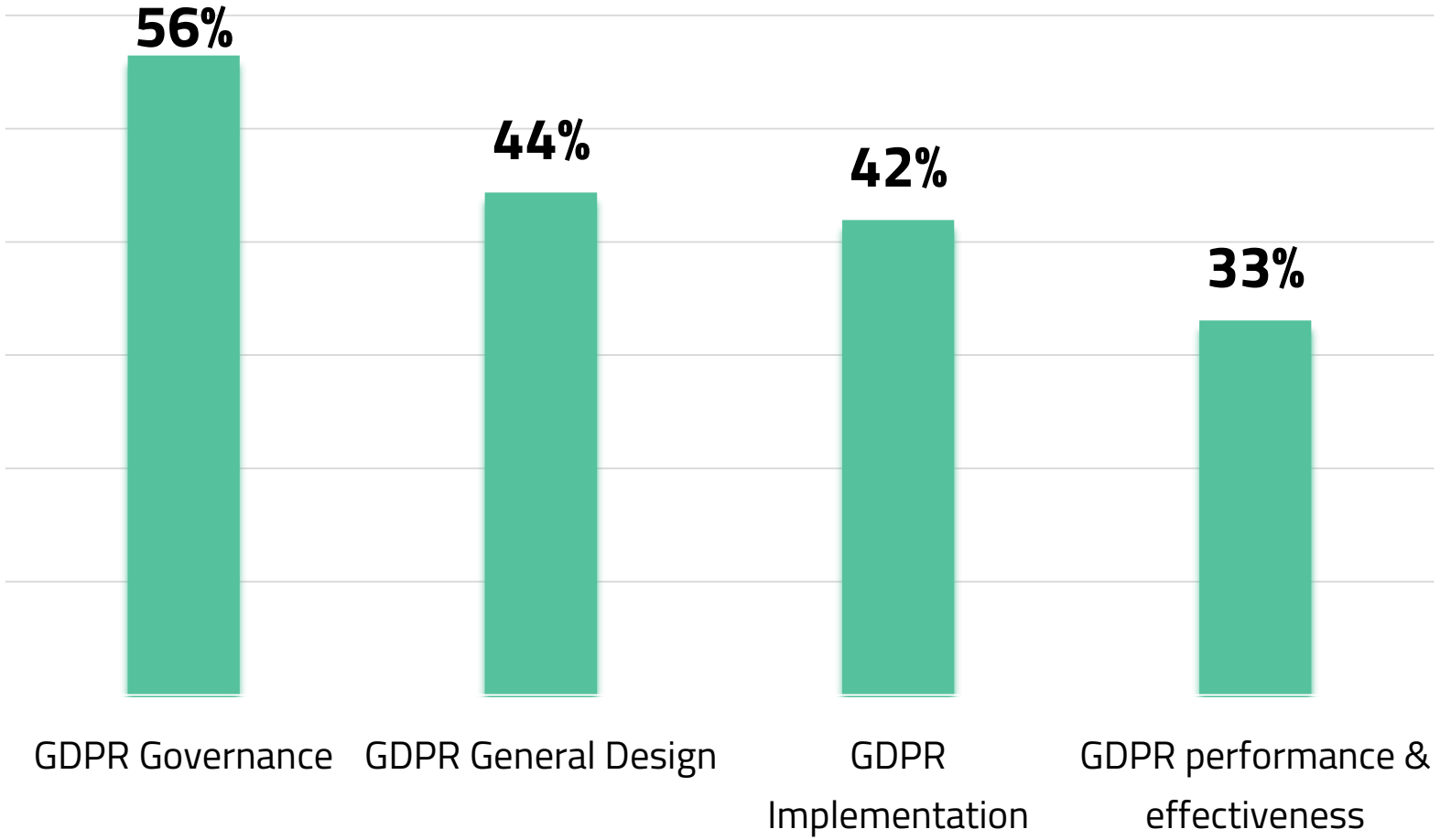


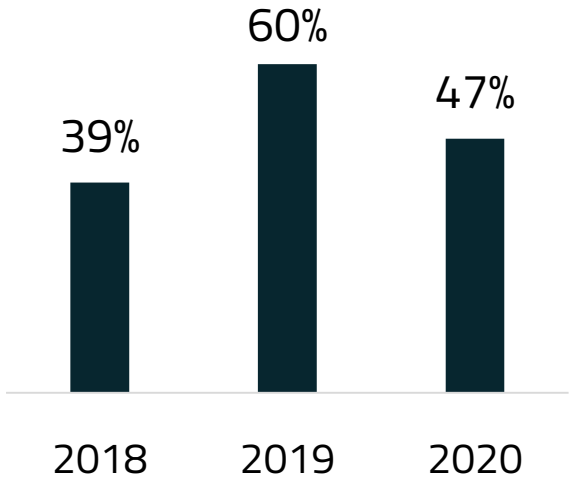
GDPR : **Polling question #4**

Do you foresee that the GDPR related engagements will become recurring audits in your audit plan ?

- Yes
- No
- I do not know

What elements of GDPR do you plan to (or currently) audit?





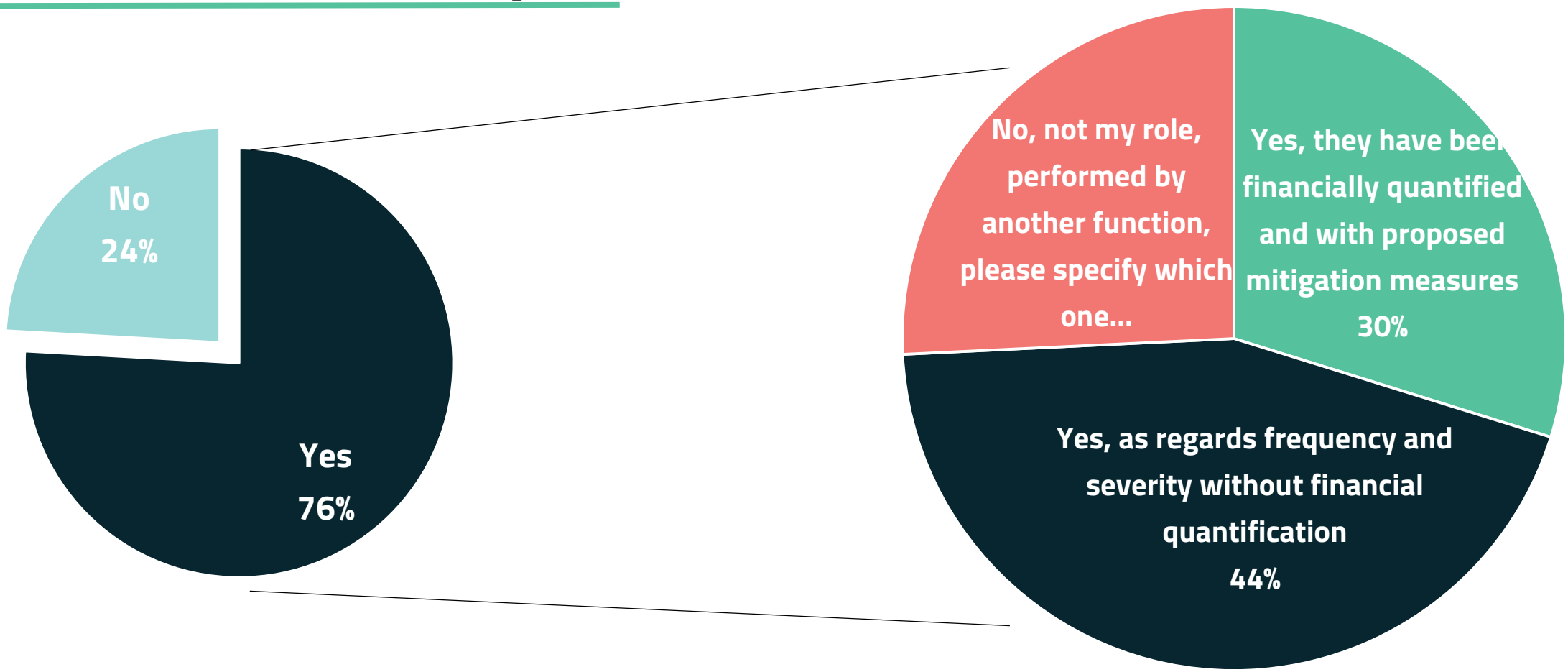
Audit plan trends

GDPR : **Polling question #5**

How do you rate the various risks of GDPR in your organisation ?

- Strategic
- Operational
- Compliance
- Financial
- Reputational

Did you perform an evaluation of the threats arising from the GDPR implementation?



Is Data Protection integrated in your global risk mapping of ERM?

What are the challenges of GDPR implementation in your organisation ?

Top challenges mentioned by respondents in the survey (%)	
1. Uncertainty, complexity	30%
2. Innovation/ R&D	25%
3. Workload, resources	17%
4. Relations – 3rd parties	14%
5. Relations – internal	14%

Questions & Answers

Recommendations

Appendix

1. Lene’s recommendation

2. Ralph’s recommendation

Main recommendations for IA and the European Authorities

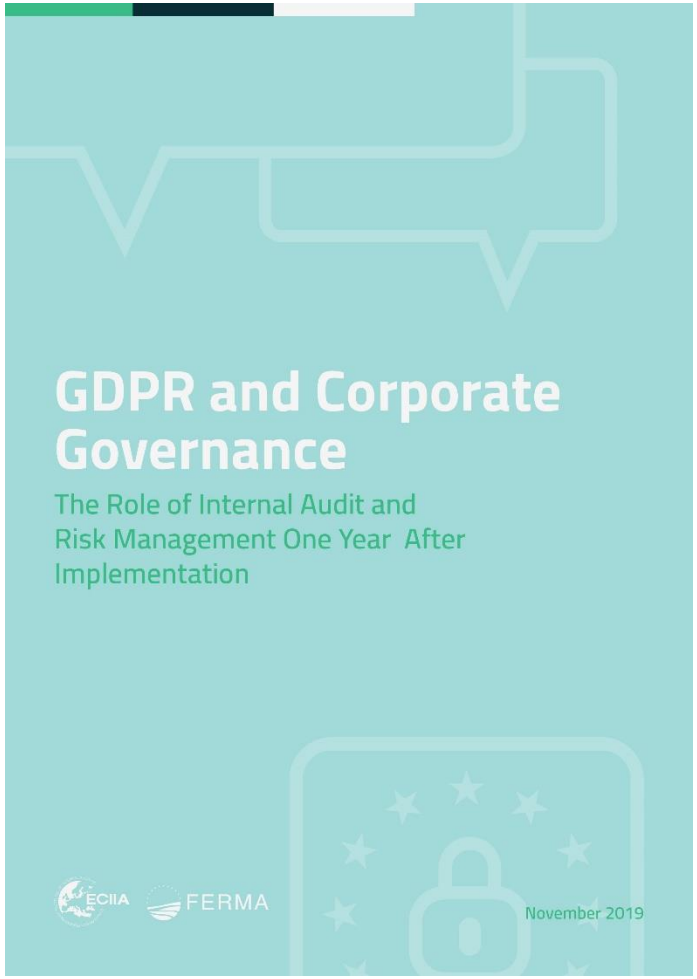
1. Recognize the key role played by corporate governance in ensuring GDPR compliance as well as a certain degree of accountability of organizations about personal data protection.
2. Reduce the uncertainty of how local authorities will deal with GDPR compliance (interpretation of what constitutes “high” risks, amount, format and frequency of the reporting…).
3. Formalize the relationship regarding privacy risks between the DPO, Risk Management and Internal Audit, relying on the three lines of defense model as a starting point.

Main recommendations for RM and the European Authorities

1. Embed data privacy in most of the existing risk maps.
2. Include the understanding of how privacy risks can affect all aspects of the business into their risk assessment, in order to propose credible and documented mitigation measures to the senior management of the organisation
3. The next review of the GDPR by the European Commission in May 2020 should preserve the organisation’s ability to innovate.

Next steps

Final report available on FERMA and ECIIA websites



FERMA and ECIIA to follow up with EU institutions in 2020

Thank you and see you in 2020

- 4 webinars were conducted in 2019 with increasing attendance and high ratings
- FERMA will continue in 2020 to propose new webinars on the most relevant topics for the risk professionals
- Subscribe to our newsletter to stay informed https://www.ferma.eu/contact-us/

About FERMA

The **Federation of European Risk Management Associations (FERMA)** speaks for the risk management profession in Europe.

FERMA acts on its behalf at European level and promotes the risk management profession.

FERMA provides a risk management perspective on European issues and strengthens the profession through a European risk management certification (rimap).

They represent nearly 5,000 professional risk managers active in a wide range of business sectors.

FERMA brings together **21 risk management associations** in **20 European countries**.

About ECIIA

The **European Confederation of Institutes of Internal Auditing (ECIIA)** is the voice of internal audit in Europe.

Our role is to enhance corporate governance through the promotion of the professional practice of internal auditing.

The ECIIA mission is to further the development of good corporate governance and internal audit at the European level, through

- **Knowledge sharing**
- **Developing key relationships**
- **Impacting** the regulatory environment, by dealing with the European Union, its Parliament and the European Authorities.

ECIIA gives voice to **47.000 Internal Auditors** in **34 countries from wider Europe**.