Out of the shadows: CISOs and DPOs in the spotlight!

2022 CISOs' and DPOs' role and responsibilities survey

pwc

clusil/

CNPD

Introduction

Home-based working, companies transitioning to digital workspaces or public cloud, an escalating number of cyberattacks and the growing complexity of information systems, evolving legislation and enforcement, better informed data subjects—these and many other factors have further increased the importance of the roles of **Chief Information Security Officers (CISOs)** and **Data Protection Officers (DPOs)** in the last few years.

PwC Luxembourg, **CLUSIL** (Club de la Sécurité de l'Information – Luxembourg) as well as the **CNPD** (Commission Nationale pour la Protection des Données) have collaborated to create the first edition of the only survey dedicated to CISOs, ISOs, DPOs and privacy experts in Luxembourg. Thanks to this collaboration, the tailored questionnaire enabled us to have a holistic view of these two roles. The answers are, as always, anonymous and details were not shared with the regulator.

With the growing importance of the CISO in mind (incl. Information Security Officer/ ISO) and DPO (incl. DPP (Data Privacy Professionals)), we have collected 90 responses from CISOs (41%) and DPOs (47%) within Luxembourg (the remaining 12% represent respondents with both roles), helping us to identify the typical profile for each role, discover their individual positions within their companies and gain a better understanding of their (potential) collaboration, as we believe, both roles have a lot of common interests when it comes to personal data protection and information security.

41%

of CISOs' respondents

47%

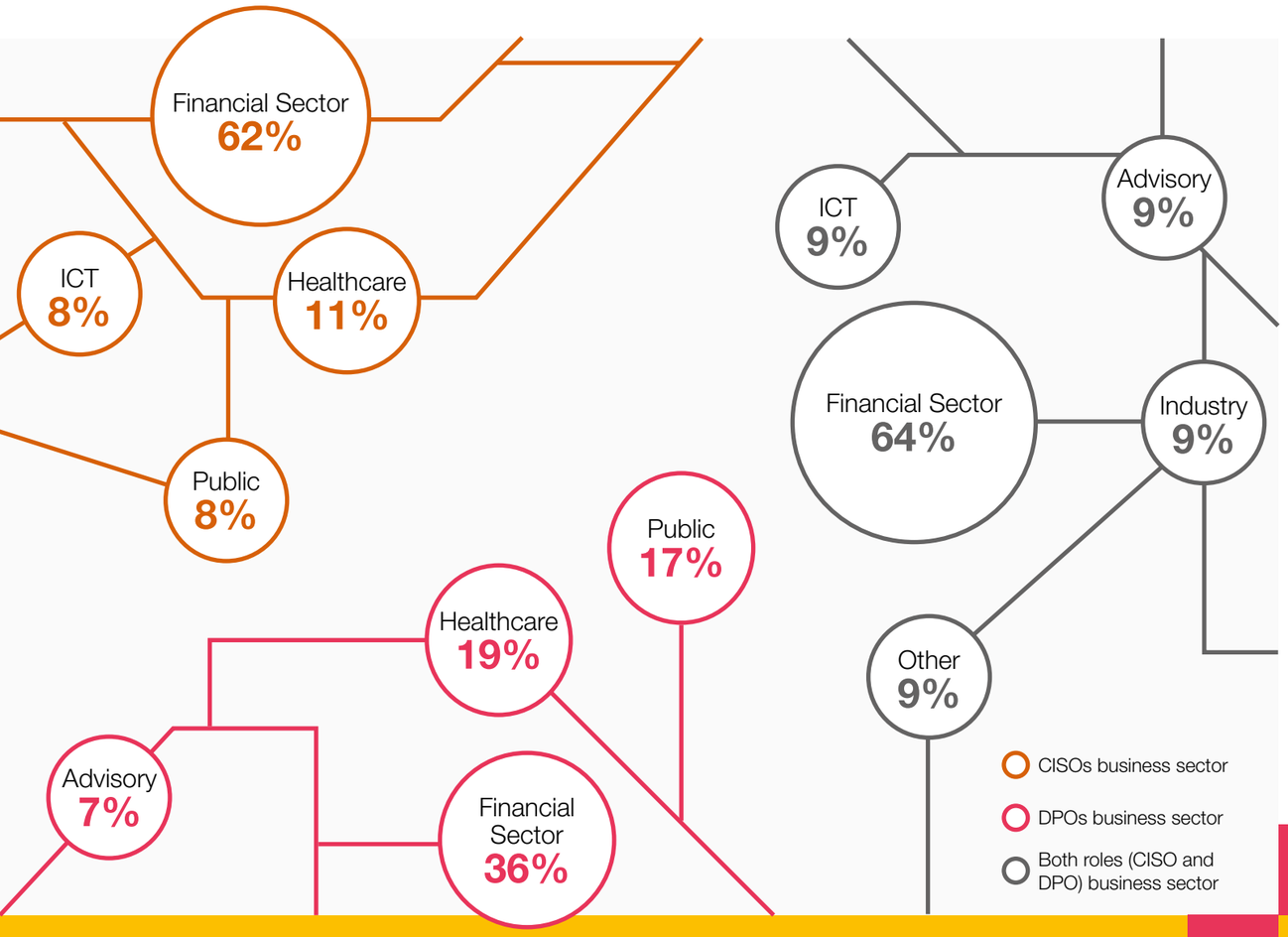
of DPOs' respondents

12%

of both roles' respondents

The companies we surveyed

Over 50% of the respondents to this year's survey are employed by entities with a turnover of more than €100 million, which raises the bar high for a potentially very hefty fine for non-compliance with the General Data Protection Regulation (GDPR - up to 4% of the annual global turnover). Even if the GDPR fines might not be on the minds of CISOs, the potential reputational and financial damage remains a real threat. Additionally, although the majority of the respondents represent the financial sector (62% for CISOs, 36% for DPOs and 64% for respondents holding both roles), healthcare and public sectors (amongst others) have also been covered by those surveyed, allowing us to get a good insight into these sectors as well.

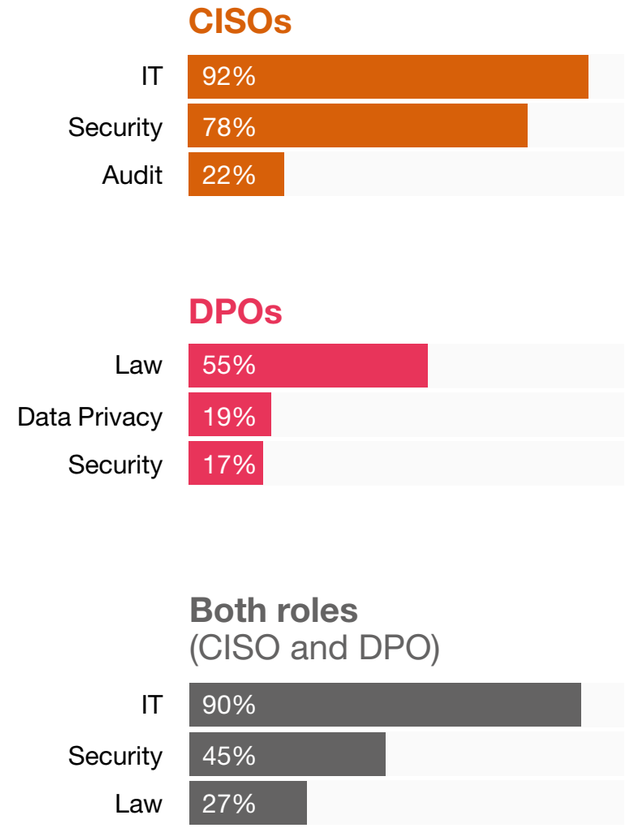


The typical CISO/ISO and DPO/DPP

Education, Skills, Experience, Profiles & Positions

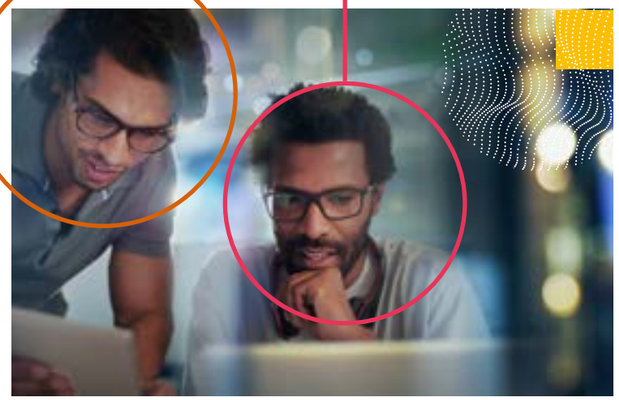
Higher education being quite the standard in today's world, it comes as no surprise that both CISOs and DPOs hold at least a master's degree (89% for CISOs, 95% for DPOs), focusing on IT or security and law respectively. Interestingly enough, in cases where respondents held both roles, only 63% hold a master's degree and the majority have strong IT and security backgrounds, whilst only 27% indicate having a background in law. We assume that these educational background tendencies result from the job evolution of these individuals, who have first pursued a career in the information security domain (i.e. CISO) and data protection (i.e. DPO) was added later on.

It is also quite clear from the survey results that the IT/ security domain remains a field predominantly occupied by men (only 8% women CISO respondents). The data privacy area is also occupied primarily by men, yet women represent a third of the respondents.



CISOs: average seniority of **8.1** years

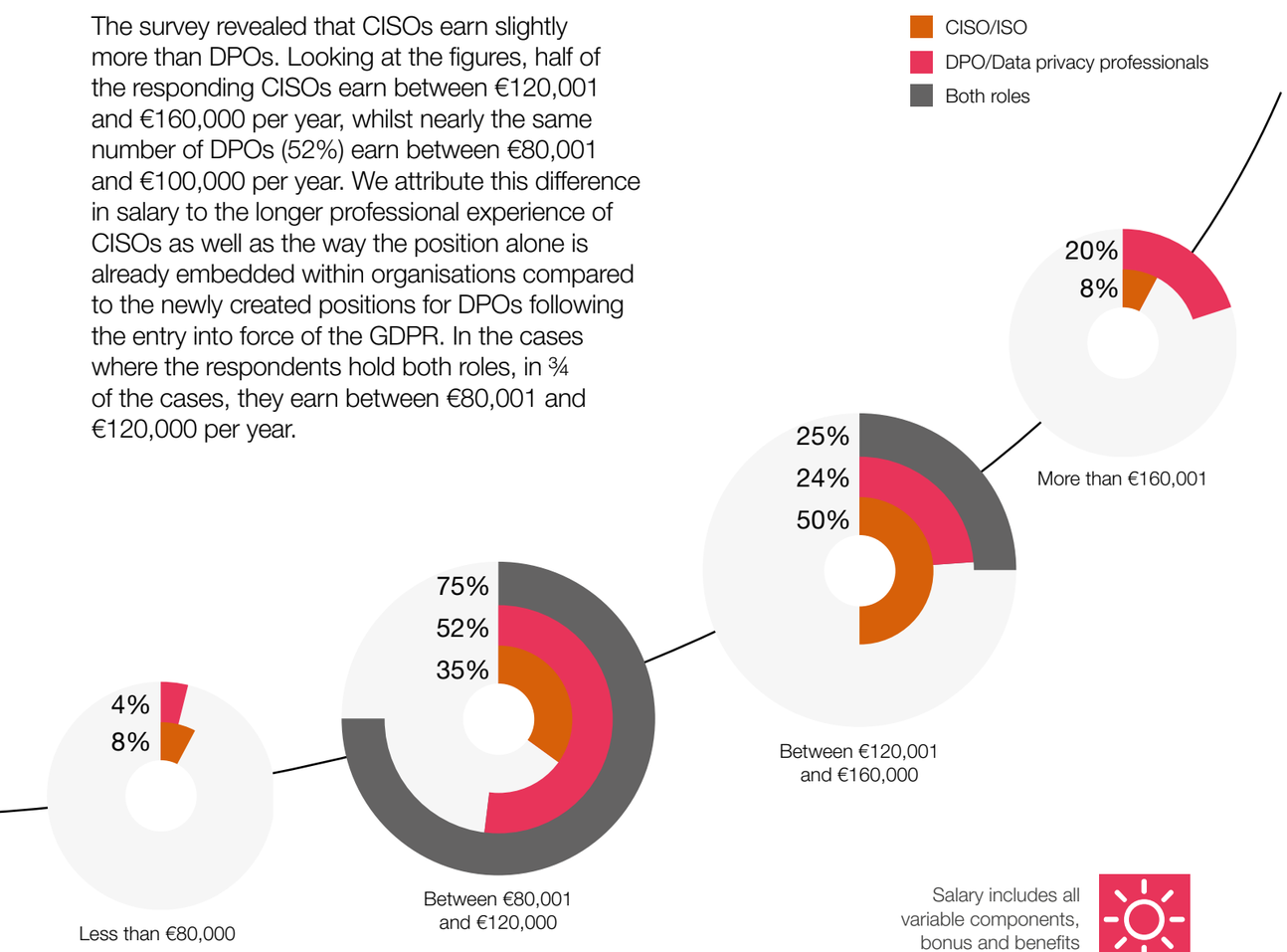
DPOs: average seniority of **5.6** years



When it comes to years of experience, DPOs also have on average less years of seniority as DPO/privacy professionals (5.6 years) compared to CISOs/ISOs (8.1 years), which seems to correlate to the entering-into- application of the GDPR four years ago in 2018, yet certain respondents have held data privacy jobs for more than two decades, which shows that privacy and data protection have been a topic of concern long before the GDPR.

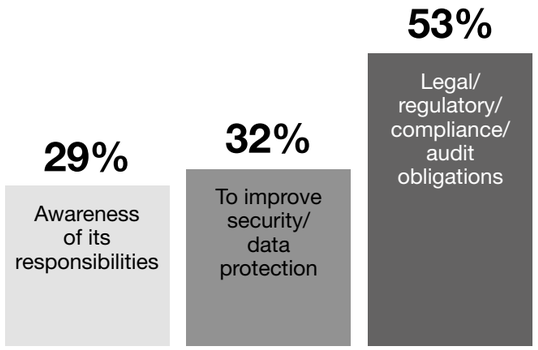
On average, more than 65% of CISOs and 63% of DPOs are aged between 35-54 years old.

The survey revealed that CISOs earn slightly more than DPOs. Looking at the figures, half of the responding CISOs earn between €120,001 and €160,000 per year, whilst nearly the same number of DPOs (52%) earn between €80,001 and €100,000 per year. We attribute this difference in salary to the longer professional experience of CISOs as well as the way the position alone is already embedded within organisations compared to the newly created positions for DPOs following the entry into force of the GDPR. In the cases where the respondents hold both roles, in ¾ of the cases, they earn between €80,001 and €120,000 per year.



Salary includes all variable components, bonus and benefits

Not surprisingly, most of the respondents (regardless of their role) have indicated that they have been nominated into their role because of legal or regulatory requirements (over 53%). Nearly a third of the respondents indicated that they have been nominated into their role to improve security and/or data protection within their organisations and nearly 29% have been nominated as their organisation was aware of its responsibilities when it comes to information security and personal data protection matters.



These roles should empower the organisation to further build their brand and create value, rather than simply have roles imposed by (forced on organisations due to) laws and regulatory obligations.

89% of CISOs have a master's degree and above compared to **95%** of DPOs.

The majority of CISOs (94%) and DPOs (89%) have internal roles within the organisations. We hope that over time, organisations will continue recognising the roles of CISOs and DPOs as an opportunity to improve the quality of their products, the robustness of their processes, the clarity of their governance, the security of their infrastructure and as a way to build trust and transparency towards customers, employees and other stakeholders.

94%
of respondents have an **internal CISO/ISO** function.

89%
of respondents have an **internal DPO/DPP** function.

Only about **8%** of CISOs are of the female gender.

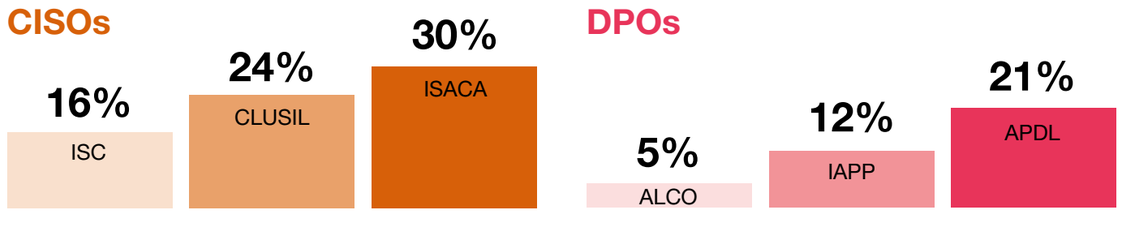
VS

33% of DPOs.

Almost a quarter **(24%)** of CISOs were 55 years old and over, while only **15%** of DPOs were in the same age category.

Active association memberships help CISOs and DPOs stay in touch with recent events and developments as well as share/exchange with their peers. Associations such as ISACA (30%), CLUSIL (24%) or ISC2 (16%) are the three most popular amongst CISOs. The APDL (21%), IAPP (12%) and ALCO (5%) are the preferred choice of DPOs. It is quite clear from the survey results that CISOs are more active in association memberships than DPOs. We could argue that this is due to the GDPR being in force only since 2018 and associations focusing on privacy are yet to gain the necessary traction and attention. We would nevertheless recommend to all those active in the privacy field to get together with their peers, share experiences, discuss challenges and pitfalls and explore what the future holds for privacy.

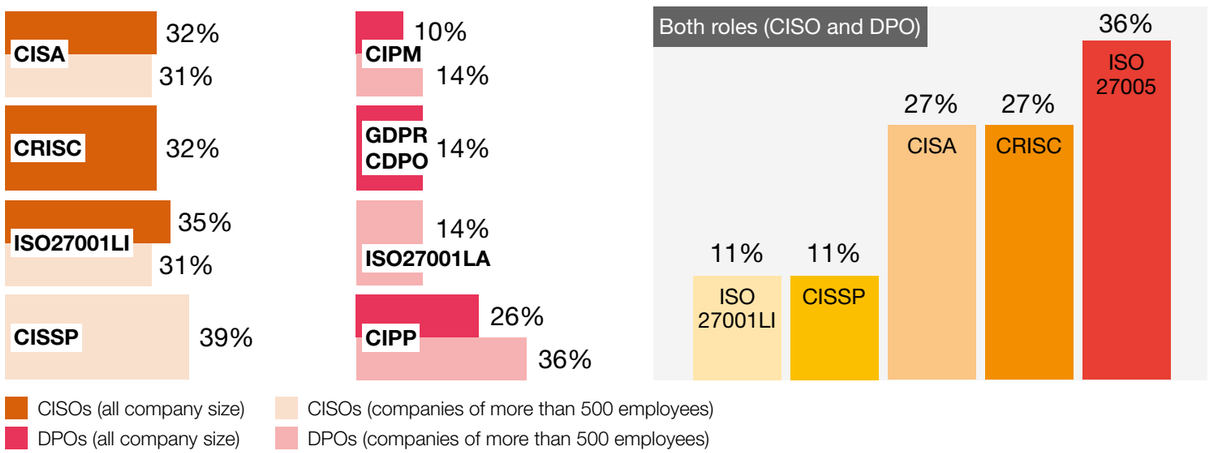
Top 3 associations



As per the industry certifications the top three for CISOs are ISO 27001 Lead Implementer (35%), CRISC and CISA (both at 32%). For entities with more than 500 employees, CISSP has an edge over other certifications, covering over 39% of CISO respondents. In the data privacy world, CIPP remains the top choice for DPOs, representing over 26% overall and nearly 36% for entities with more than 500 employees.

GDPR-CDPO and CIPM come second and third, representing 14% and 10% of the certifications respectively. When respondents hold both roles, the certifications linked to information security dominate over those linked to data protection, where ISO 27005, CRISC and CISA are the top 3 certifications indicated by the respondents.

Top 3 industry certifications



In certain cases, often depending on the size of the company, CISOs (15%) and DPOs (32%) hold more than one role (66% of respondents occupying both roles work in less than 500 employees companies). In the case multiple roles are held, DPOs tend to allocate only around 25% of their time to data protection/ privacy topics.

If DPOs hold multiple positions it is likely to be Chief Compliance position, or also Chief Risk Officer positions whilst CISOs are often within the risk area, be it the Chief Risk Officer or Operational Risk Officer.

The CISO/ISO's and DPO's role (additional functions they occupy)

85% of **CISOs' respondents** are full-time in the **CISO** role.

68% of **DPOs' respondents** are full-time in the **DPO** role.

Among "part-time DPOs",

87.5% respondents allocate in most cases **25%** of their time to their DPO role.

The remaining **75%** of the time is allocated to their other roles.

What DPOs must pay attention to when holding numerous positions is ensuring that the potential conflict of interest is managed and that the two positions do not interfere with one another.

The fact that DPOs are more likely to have another role within an organisation suggests that companies might not be paying sufficient attention to data privacy, do not allocate sufficient resources to this field or do not assess the necessary workload to perform the work.

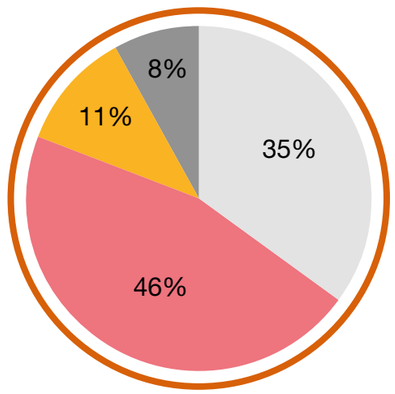
Information security does not seem to have such drawbacks, as 85% of CISO respondents hold the CISO position as their full-time job. It will be interesting to see if DPOs will see their workload increase, as data privacy slowly builds its way into the culture of organisations, as information security has done over the last years.

Organisations should make sure that any potential conflicts of interests are assessed and evaluated, as only 50% of the respondents indicate such an evaluation has not been officially documented (this mainly impacts companies with fewer than 500 staff). As per the GDPR, a DPO should not determine the means and purposes of a processing activity, thus avoiding conflicts of interests and maintaining a pure advisory role[1].

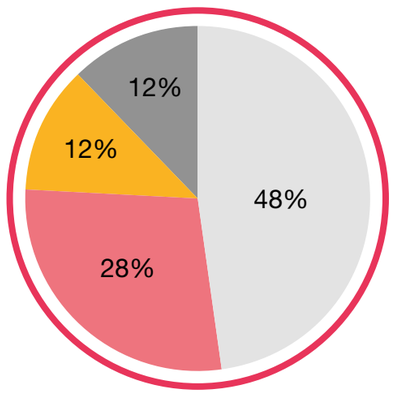
Nearly 50% of the DPO respondents have indicated they report directly to the CEO (or members of the executive management), which is in accordance with the GDPR the correct reporting line. Yet nearly a third of the respondents have indicated they report to N-2 or even N-3 within the company hierarchy, which could be considered in breach of the Regulation, but also can create an unnecessary filter between the CISOs/ DPOs and the top management[2].

The CISO/ISO's and DPO's position within the company

CISO/ISO's position



DPO/DPP's position



*members of the executive management / acting as advisor to the CEO

Such a filter may significantly influence the messages being passed on to decision makers (the controllers) and put at risk not only the organisations, but mainly data subjects as inadequate data protection measures might be in place. On the CISO front, over 81% report directly to the CEO or N-2 within their organisations.

From a reporting line perspective, CISOs are most likely to sit within the IT department (38%) or Risk (27%) whilst DPOs are sitting within Compliance (36%) or are directly reporting to Management (27%). Especially for the CISOs, sitting within the IT department may raise issues in terms of its role, which should be a second line of defence role, whilst the IT department generally has more operational functions, being part of the first line of defence.

The survey has revealed another interesting fact, that neither all CISOs (38%) nor all DPOs (56%) are involved in new projects from the start. If this becomes a standard habit for organisations to only include CISOs or DPOs at later stages of projects, information security and data privacy might not be taken sufficiently into consideration and might be difficult to implement once the projects are ongoing[3]. In addition to the difficulty of implementing sufficient security measures and ensuring that data protection principles are applied, the cost of late implementation within the project timeline tends to increase significantly. In addition to increasing implementation difficulties and costs, this can be seen as non-compliance with the privacy by design and by default principle of the GDPR.

Surprising results were observed on the company committee memberships, where nearly 20% of CISOs and over 30% of DPOs do not sit on any committees. An even bigger number arises when looking at committee memberships for holders of both roles, where the percentage increases to 44% not being members of any committee. This might be explained by the fact that employees often hold multiple positions in smaller entities, where incidents are tackled on an ad hoc basis, rather than setting up official and dedicated committees.

62% of **CISOs and** **44%** of **DPOs** are involved in new projects from start.

19% of CISO/ISO respondents do not belong to any committees in the organisation.

32% of DPO/DPP respondents do not belong to any committees in the organisation.

44% of respondents with both roles do not belong in any committees.

1 GDPR Art 38(6): The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

2 GDPR Art 38(3): The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. […]. The data protection officer shall directly report to the highest management level of the controller or the processor.

3 GDPR Art 25(1) & (2):

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

With both information security and privacy areas being heavily involved in the assessment of risks and the determination of the right courses of action, we wonder whether these results suggest overlapping roles and responsibilities within organisations or whether they indicate that organisations slightly overlook/underestimate these two topics. In certain cases, especially for smaller organisations, the absence of committees and non-official roles is easily explained by the size of the structure and the "simplicity" of day-to-day operations, where employees tend to have multiple roles and are in frequent contact, meaning, therefore, they can tackle any potential issues in an ad-hoc manner. We would nevertheless expect these roles to be clearly documented in order to avoid any room for doubt as well as organisations being able to deliver on the accountability principle of the GDPR.

The preferred choice to monitor service providers remains the completion of questionnaires, forms or interviews with the counterparts (CISOs - 59%, DPOs - 40%), closely followed by internal risk assessments (CISOs 43%, DPOs 33%) or audit assignments (CISOs - 38%, DPOs - 24%). A relatively high percentage of organisations rely on a best effort basis (CISOs - 24%, DPOs - 29%), which could prove costly if not done correctly and non-reliable service providers are selected.

CISOs' and DPOs' main challenges

The challenges CISOs and DPOs face revolve around raising sufficient awareness, dealing with sufficient involvement and budget allocation (a full 57% of CISOs and nearly 90% DPOs indicate they have no budget whatsoever allocated to the execution of their tasks) as well as collaborating with IT and implementing GDPR within the organisation in general.

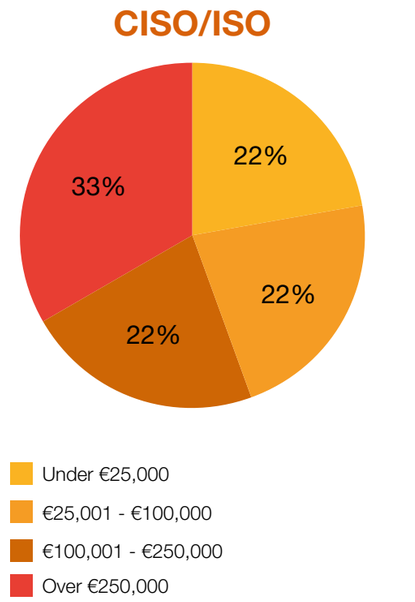
CISO/ISO

- Effectively dealing with threats and budget.
- Improving the awareness of risks and the awareness of CISO role.
- Effectively working with IT.

DPO/Data privacy professionals

- Increasing the awareness on GDPR.
- The application and enforcement of GDPR.
- The involvement of the DPOs.

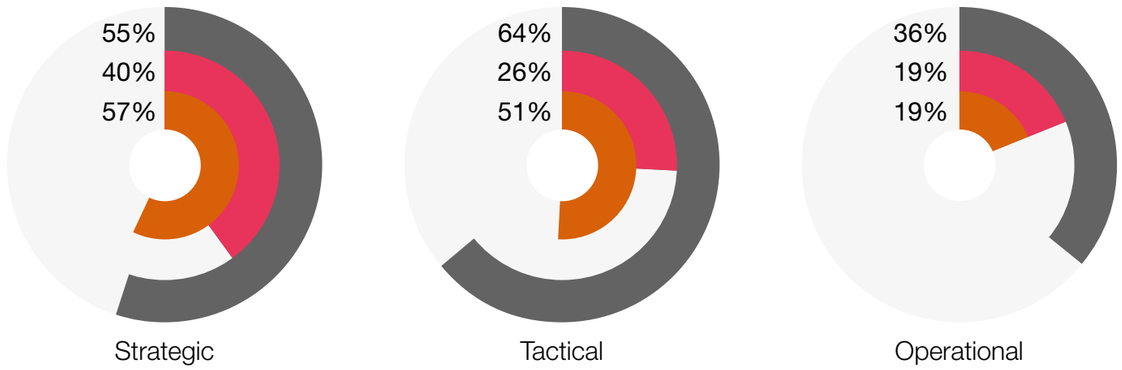
The CISO/ISO's and DPO's budget within the company



- **88%** of **DPOs** declare having **no budget.**
- **57%** of **CISOs** declare having **no budget.**
- **55%** of **CISO** respondents declaring having a budget have a **minimum budget of 100k€**.
- **45%** of the **CISOs** are **unsatisfied** with their budget which they judge insufficient,
- For the respondents who undertake **both roles**, **50%** of them declare having a budget vs **50%** having no budget.

Another challenge both CISOs and DPOs are probably facing is that they (around 20% in both fields) see their roles as operational—which especially in the case of DPOs—is something to avoid, as the GDPR clearly indicates that DPOs should hold an advisory role and should avoid being too "hands on" when assisting their colleagues with applying the data protection principles[4]. Regardless of these challenges, over 90% of CISOs and DPOs are pleased with their position and role within their organisation. Yet a relatively significant 15% of CISOs and 5% of DPOs (and 12% holding both roles) feel sanctioned since accepting their role.

CISO and DPO role perception



The survey also shows that data privacy and information security has improved over the years and both roles see further improvement in the future. Slightly over a half of our respondents (63%) believe that the cyber resilience maturity level within their organisation is 'defined' (as per the CMMI scale). When it comes to compliance with data protection regulations, more respondents (71%) see the maturity level as 'defined'. As already mentioned, the collaboration between CISOs and DPOs seems essential, but we must not forget that the sufficient involvement and implication of other departments is crucial. CISOs and DPOs may put certain wheels in motion, but it is up to the whole organisation to abide by the defined information security and data protection rules and ensure they become an integral part of the organisation's DNA. This is the only way organisations will be able to further develop transparency and trust and improve the relationship with their clients and employees.

4 See GDPR Article 39: Tasks of the data protection officer

Companies should re-orient their focus from purely tackling business-related risks to including in their considerations the risks that their business could impose on data subjects. By doing so, they would build a road to more trusted relationships with clients, staff and other stakeholders. In addition, this approach will inherently reduce security risks and non-compliance risks.

According to the CISOs and DPOs, many barriers to success lie within the organisation. Be it the negligence of certain employees, complexity of IT systems or lack of management support, CISOs and DPOs have quite a number of challenges that lay ahead in order to overcome these. Human error has always been, and probably will remain, one of the key causes of data breaches[5]. It is therefore essential to put in place adequate technical and organisational security mechanisms to ensure data is being well protected and human error can be avoided as much as possible. In attempting to avoid human error, we see organisations implementing intelligent software, but also, and perhaps most importantly raising awareness on a regular basis.

The collaboration between CISOs and DPOs seems to be a very positive one, as over 90% have declared to have a good, or even very good, collaboration with each other.

As the information security and privacy topics go hand in hand in our opinion, we hope to see CISOs and DPOs further engage together by holding regular meetings (at the moment, only 49% collaborate at least once a week) and working alongside each other to align their objectives and interests when it comes to information security and data privacy.

We see an overall increasing understanding of the importance of information security and data privacy within the market. The two roles facing the challenges these two domains bring must further strengthen their positions in their organisations and must ensure they have sufficient support from top management. CISOs and DPOs should continue working closely together, ensuring that their colleagues are well aware when to contact them and involve them as early as possible in projects.

15% of CISOs, 8% of DPOs, and 12% of respondents with both roles feel sanctioned since being in this position (freeze in salary, decrease in responsibility…).

93% of CISOs and DPOs declare having good or very good collaboration with each other.

49% of CISOs and DPOs declare collaborating with each other at least once a week.

5 CNPD Rapport d'activités 2020: 64% of the cause of data breaches are linked to non-malicious internal acts (human errors) (https://cnpd.public.lu/content/dam/cnpd/fr/publications/rapports/cnpd/rapport-annuel-+-annexes-2020-CNPD-BD.pdf)

Key takeaways

01 Ensure that any potential conflicts of interests in your role(s) have been assessed, evaluated and documented;

02 Involve CISOs & DPOs at the earliest stages of any project, it can save you precious time and money if you do this to improve the security and privacy level of the processed data;

03 Use information security and data protection to empower and facilitate your business-as-usual operations. By defining information security and data protection guidelines, you remove the internal struggles of unclarity in the course of action, whilst also protecting your organisation and data subjects alike;

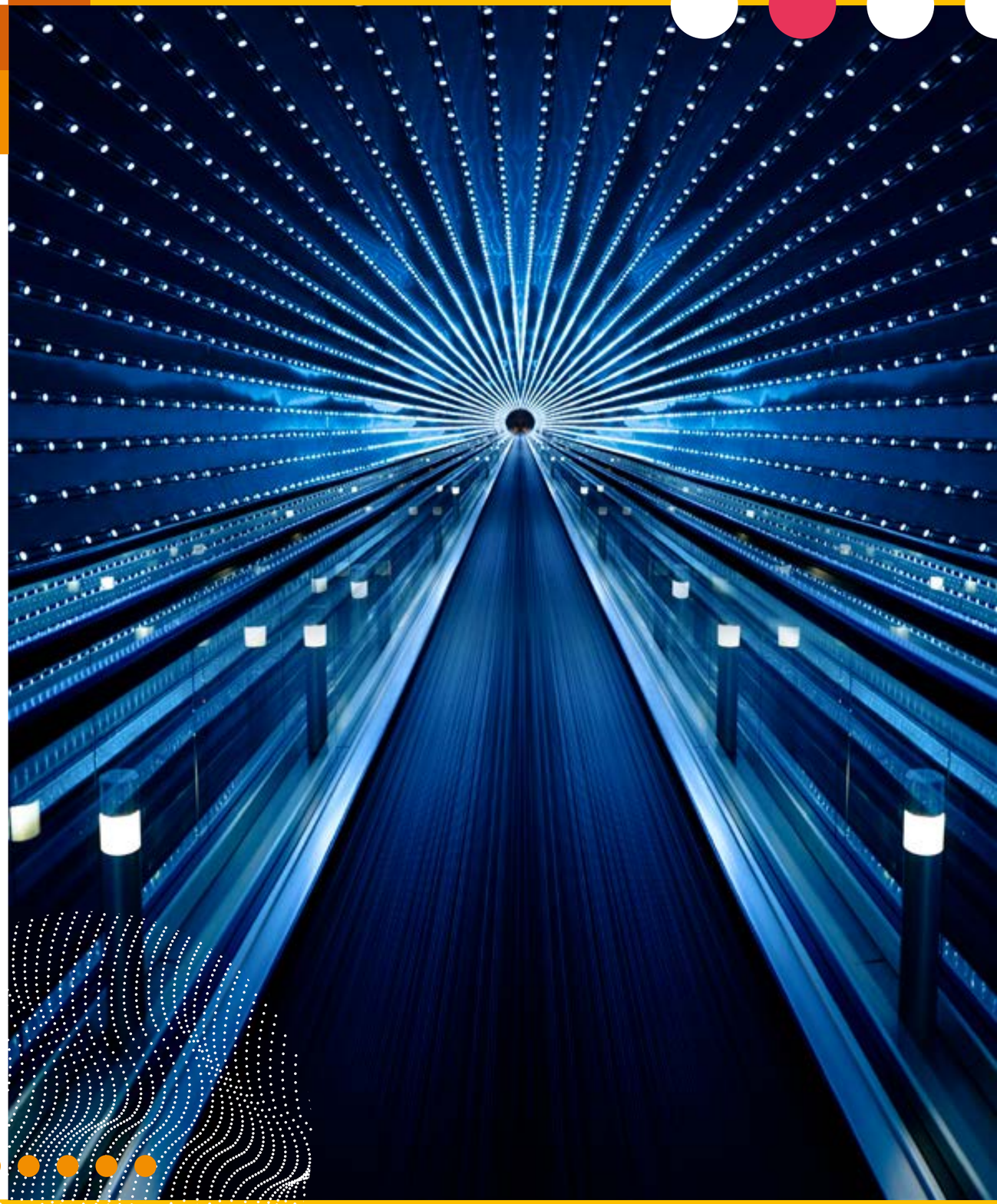
04 Take necessary measures to provide sufficient budget and training to CISOs and DPOs: if you do not enable them to be at the top of their game, your organisation could struggle to successfully tackle the information security and data protection challenges and would not be able to forecast the necessary developments and improvements to maintain the trust of your stakeholders and keep up to date with recent developments in information security and data protection;

05 Encourage the sharing of information and practices between DPOs and CISOs through formal and informal sessions;

06 Assess thoroughly the CISO's position within the company. CISOs are still closely linked to the IT department. Sitting in IT may not be appropriate for a control function that should be managing information security risks;

07 Use information security and data protection to further increase the trust and confidence of your staff, customers and other stakeholders by focussing not only on protecting your business, but also the data subjects (the latter may also be your customers);

08 Ensure that CISOs' and DPOs' advice on the information security and data protection path is enforced by top management, and that the rest of the organisation carries it through consistently and makes it work.



Comparison with the 2020 edition of the “Out of the shadows: CISOs in the spotlight!” survey

This year’s survey edition focused both on the role of the CISO and the DPO. We indeed believe that these two roles are intricately intertwined and aim at the same final goal: the protection of the company’s information.

While we wanted to have a fresh start for the survey, we also wanted to highlight the key elements and evolution of the CISO results compared to the previous edition of 2020.

This year top certifications for the CISO have been shuffled: while ISO27001 Lead Implementer remains on the podium, the CISSP and the ITIL certifications have been replaced by the CISA and CRISC, which might be explained by a shift of the CISO role to a more control and risk oriented-function that is aligned with the expected position of the CISO as 2nd line of defence. The CISSP remains the top certification in the 2022 edition for companies of more than 500 employees, as it was in the previous edition.

85%
of the CISO respondents this year are in a full-time position compared to
64%
in the previous edition. When they are not, their additional roles remain the same, being in particular the Chief Risk Officer, still in the 2nd line of defence.

Going against market best practices, which aim at eliminating any conflicts of interests, the survey results show an ever-increasing tendency of CISOs to be positioned within the IT department (from 22% in 2018, 33% in 2020 to 38% in 2022). This may reflect the attempts by the organisations to enhance the communications between the Information Security and IT security teams and increase efficiency while risking that the operational issues and production requirements outweigh the security expectations. It could also very well be that this is the last resort within organisations where security is understood.

We see an increase in CISO reporting to top management within the organisation:
+30%
compared to the previous edition of the CISOs are reporting to the CEO / n-1 or n-2 position representing 81% of respondents, hopefully demonstrating the understanding of the organisation that the CISO’s voice must be heard at the highest level.

When looking at the challenges our CISOs have faced over the last two years the responses we got in the previous edition were perfectly on the spot: new threats and budget, awareness and collaboration within the organisation are definitively on the agenda and should remain on the top for the next edition…

Contacts

About PwC

PwC Luxembourg (www.pwc.lu) is the largest professional services firm in Luxembourg with over 3,000 people employed from 75 different countries. PwC Luxembourg provides audit, tax, and advisory services including management consulting, transaction, financing and regulatory advice. The firm provides advice to a wide variety of clients from local and middle market entrepreneurs to large multinational companies operating from Luxembourg and the Greater Region. The firm helps its clients create the value they are looking for contributing to the smooth operation of the capital markets and providing advice through an industry-focused approach.

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms of 158 countries and 250,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com and www.pwc.lu.

About clusil

CLUSIL a.s.b.l. develops cooperative actions with public authorities, semipublic authorities for the security of information. With about 200 members from all economic sectors, it is a wellestablished and independent actor among the Information Security Landscape of Luxembourg and the "Greater Region". In more than 25 years we have come a very long way and are very proud of the many achievements.

About CNPD

The National Data Protection Commission (Commission Nationale pour la Protection des Données – CNPD) is an independent public institution with legal personality. It is financially and administratively autonomous.

It verifies the legality of the processing of personal data and ensures the respect of personal freedoms and fundamental rights with regard to data protection and privacy.

The CNPD verifies if personal data is processed in accordance with the following provisions:

- the General Data Protection Regulation (GDPR);
- the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the general data protection framework;
- the Act of 1 August 2018 on the protection of individuals with regard to the processing of personal data in criminal and national security matters;
- the Act of 30 May 2005 regarding the specific rules for the protection of privacy in the sector of electronic communications;
- other legal texts containing specific provisions on the protection of personal data.

Marc Lemmer
Data Protection Commissioner, CNPD
marc.lemmer@cnpd.lu

Alain Herrmann
Data Protection Commissioner, CNPD
alain.herrmann@cnpd.lu

Cédric Mauny
President, CLUSIL
cedric.mauny@clusil.lu

Koen Maris
Cybersecurity Leader, PwC Luxembourg
koen.maris@pwc.com

Antonin Jakubse
Senior Manager, Privacy, PwC Luxembourg
antonin.jakubse@pwc.com

Maxime Pallez
Senior Manager, Cybersecurity, PwC Luxembourg
maxime.pallez@pwc.com