

Cyber Security Department

Out of the shadows: CISO in the Spotlight!

Key results of the 2016 survey
conducted by CPSI and PwC
Luxembourg



15 June 2016

pwc

Introduction

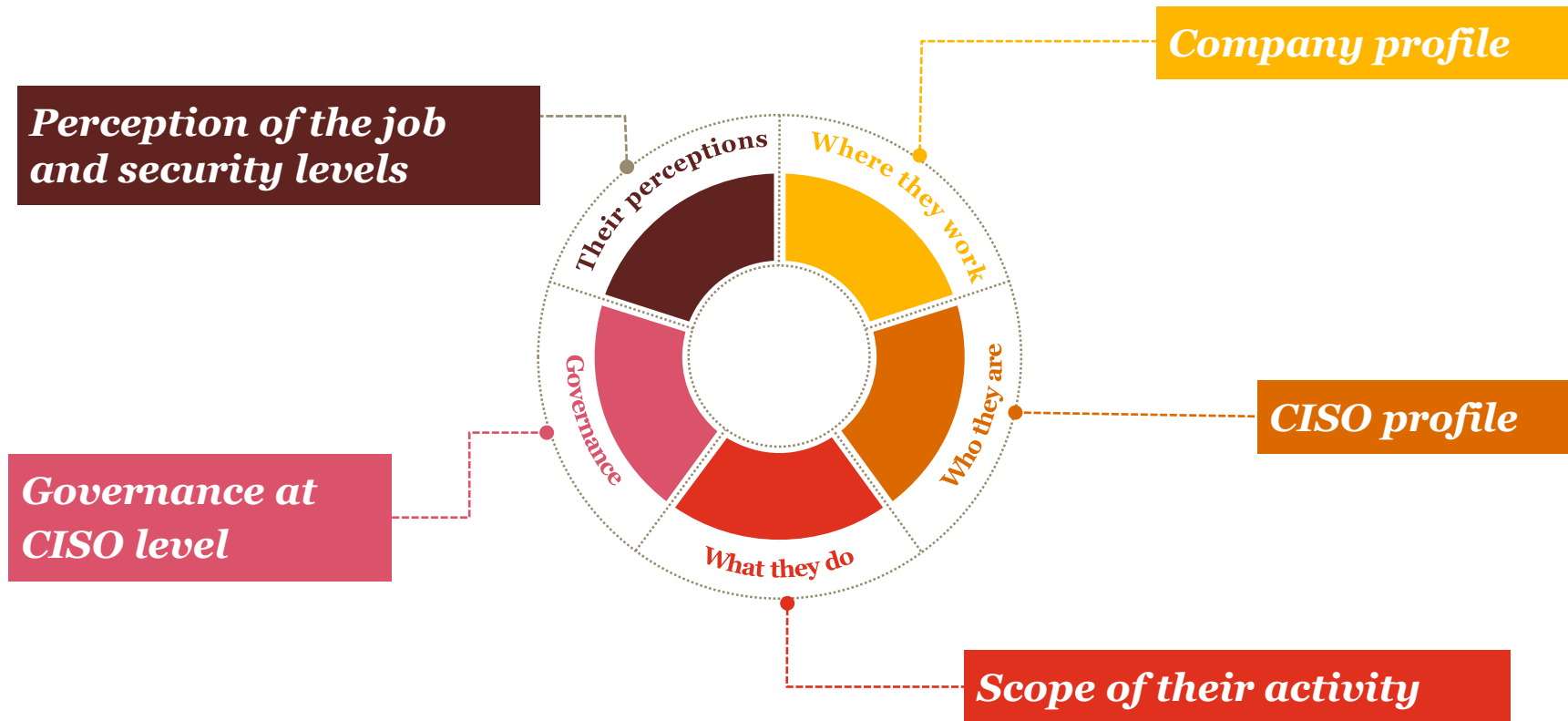
What's the profile of a Chief Information Security Officer (CISO) in Luxembourg? Where does he stand in the organigram? What challenges and opportunities does he have?

The "CISO in the Spotlight" survey, conducted by CPSI and PwC Luxembourg aims at shedding light on the CISO role in Luxembourg by looking at it from several perspectives.

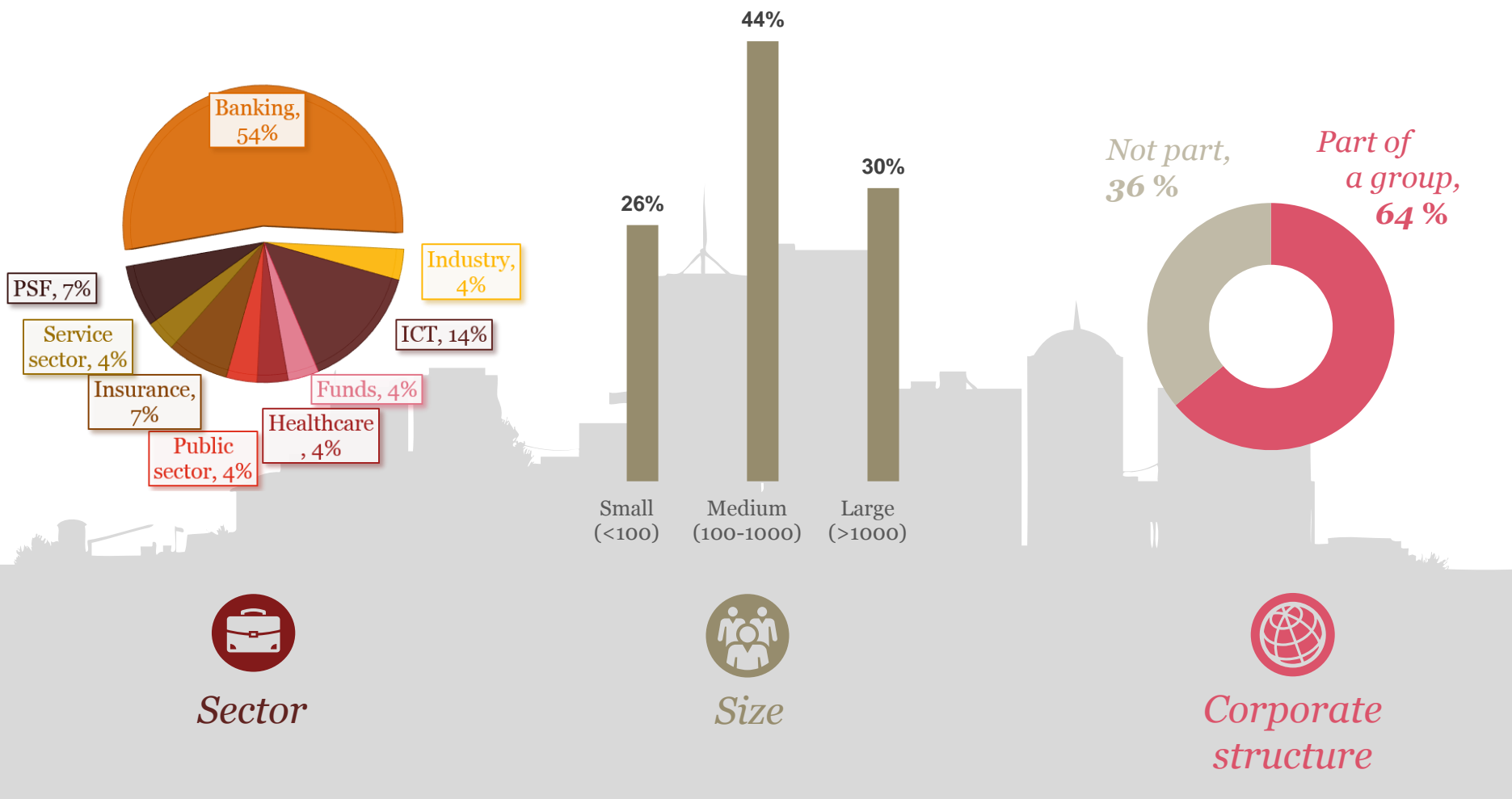
Table of contents

1	Scope of the survey	4
2	Company profile	5
3	Typical profile of a CISO	6
4	CISO's activity	7
5	Governance at CISO level	21
6	Perception of the job	26
7	Your contacts	31

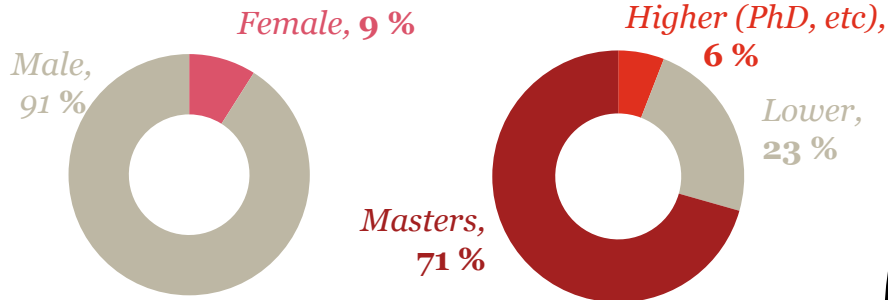
Scope of the survey



Company profile

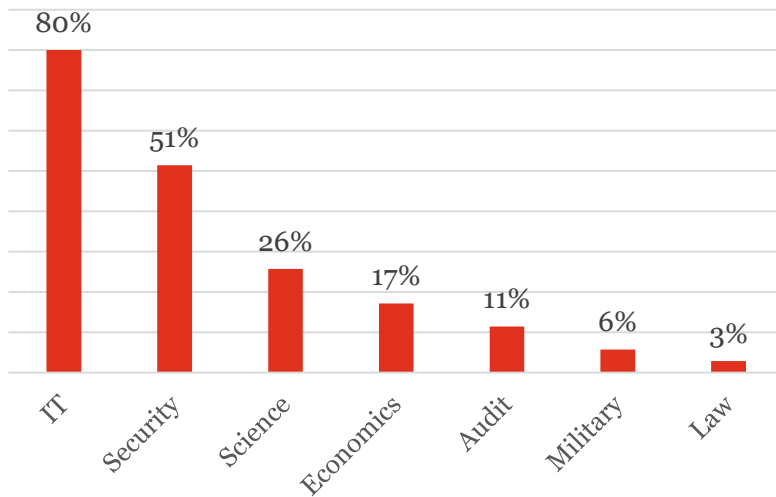


Typical profile of a CISO



▶ Gender

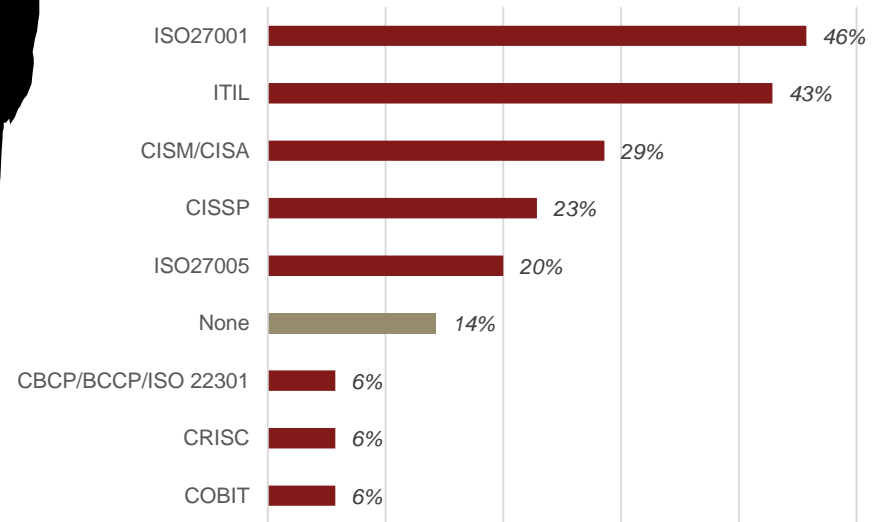
▶ Qualification



▶ Backgrounds



▶ Experience



Others (<5%): ICT, Nates, HP AIS, ...

▶ Certifications

CISO's activity

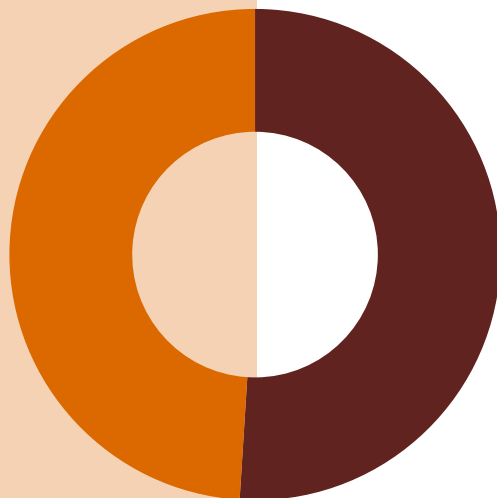
▶ *CISO : a full-time role?*

No, 49 %

Other roles:

- *Chief Risk Officer*
- *Chief Information Officer*
- *Chief Operating Officer*
- *Data Privacy Officer*
- *Compliance Officer*
- *Organisation*
- ...

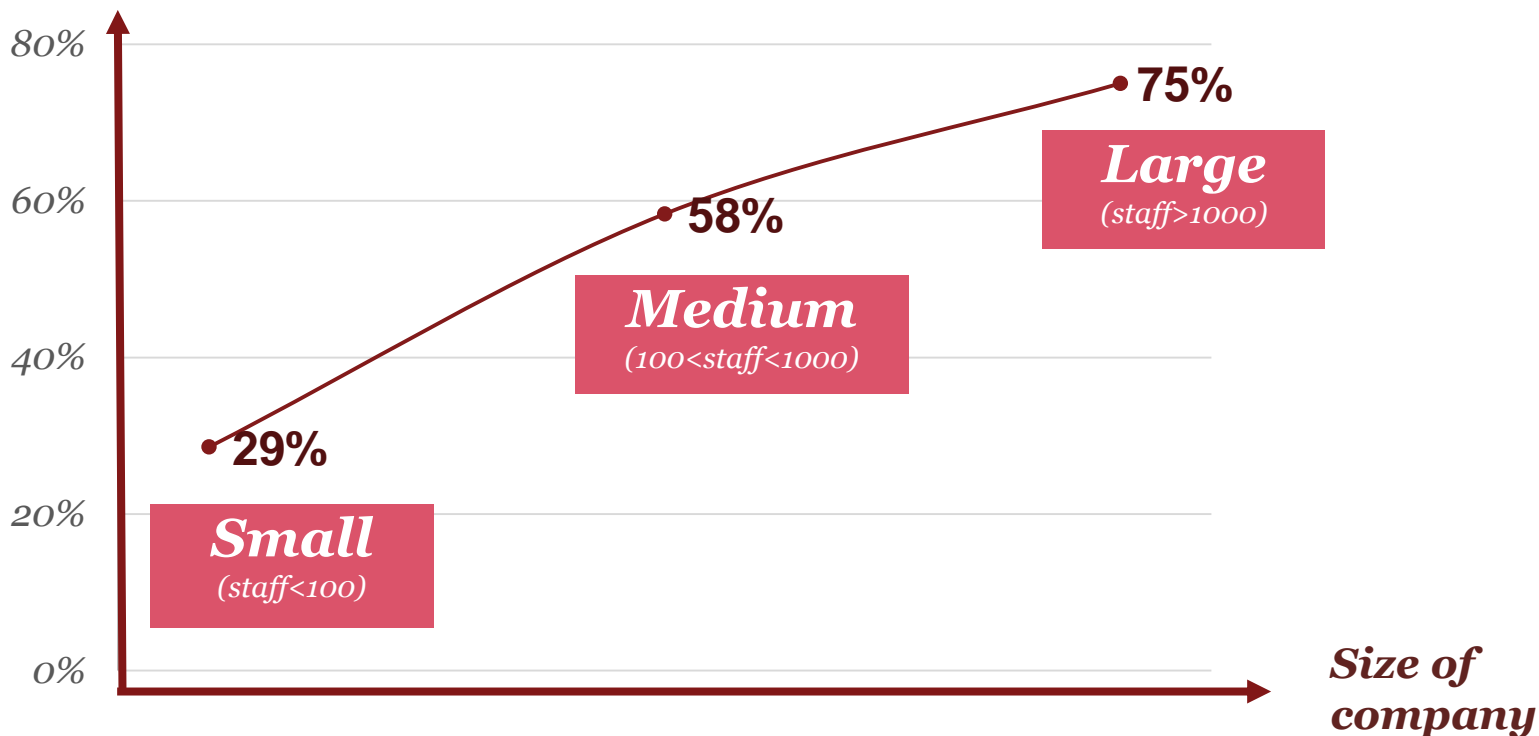
Yes, 51 %



CISO's activity

▶ Full-time CISO roles

Full-time CISO roles (%)



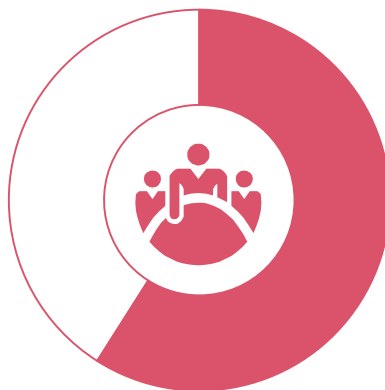
CISO's activity

▶ Information security strategy



56%

*are aligned with
business strategy*



59%

*are approved by
senior management*

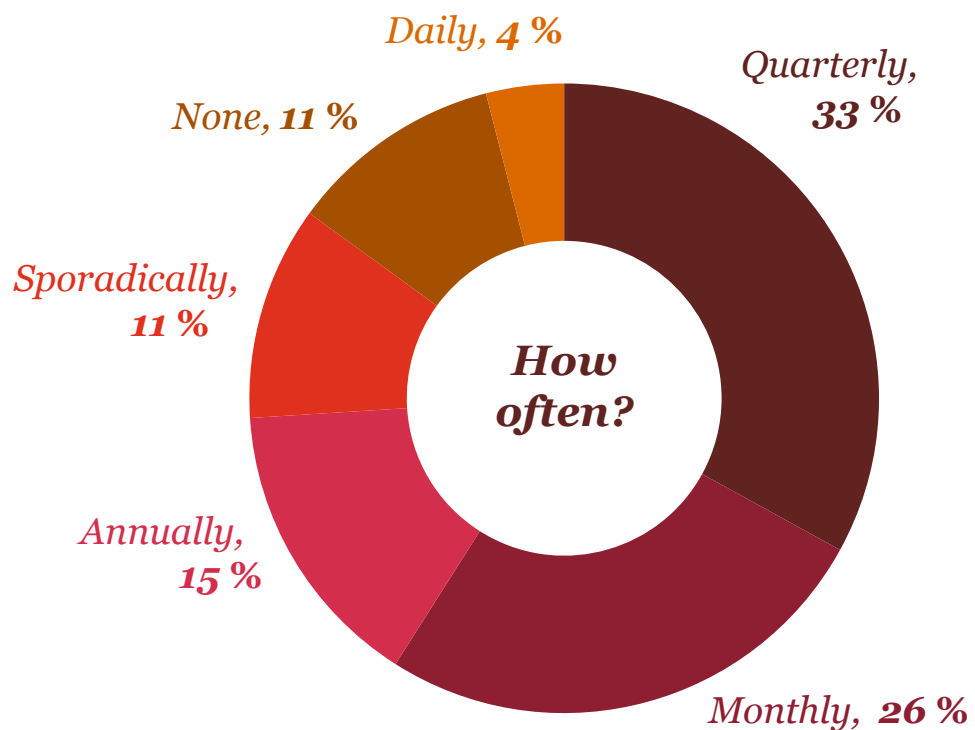


30%

*outline future state
of information security*

CISO's activity

▶ Use of metrics



50%

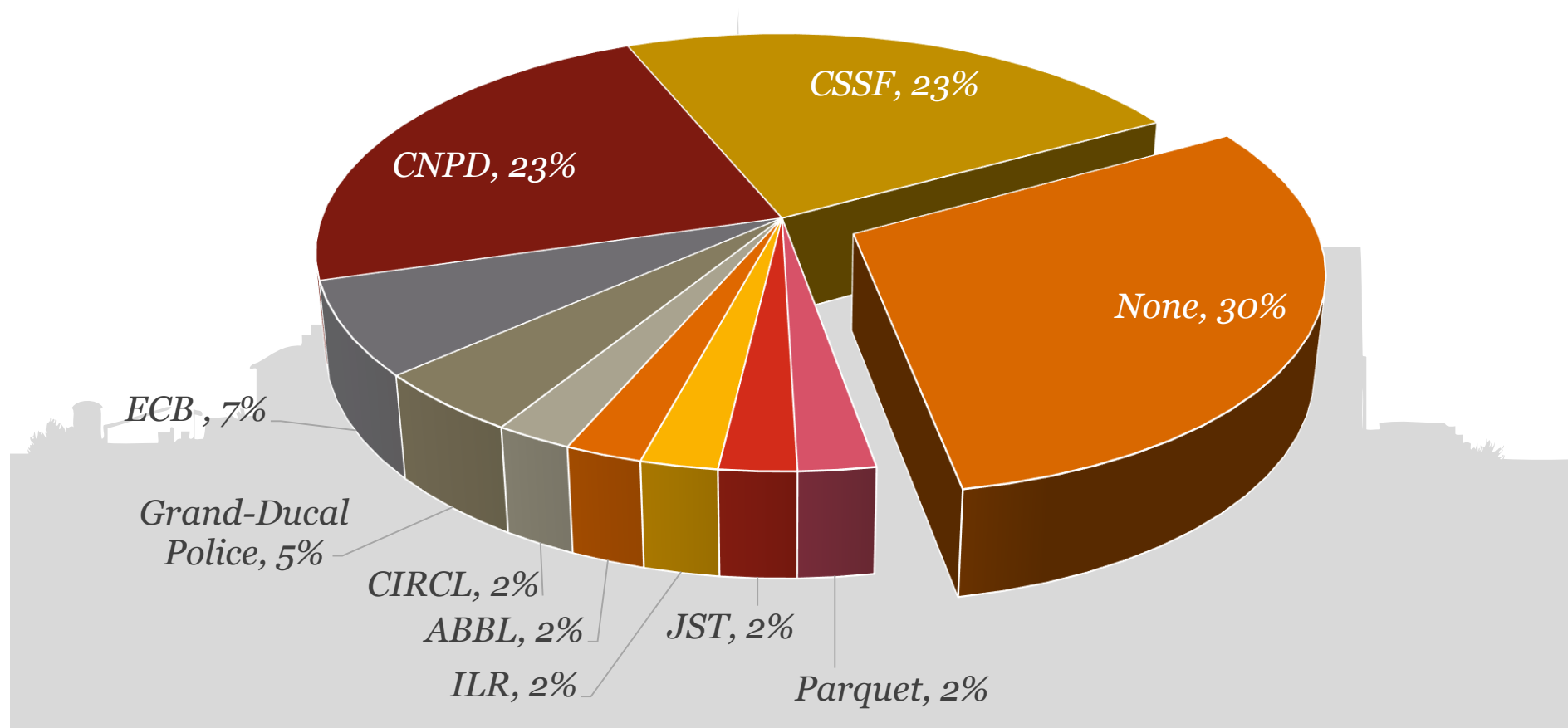
are reported to risk management

29%

are reported to CEO

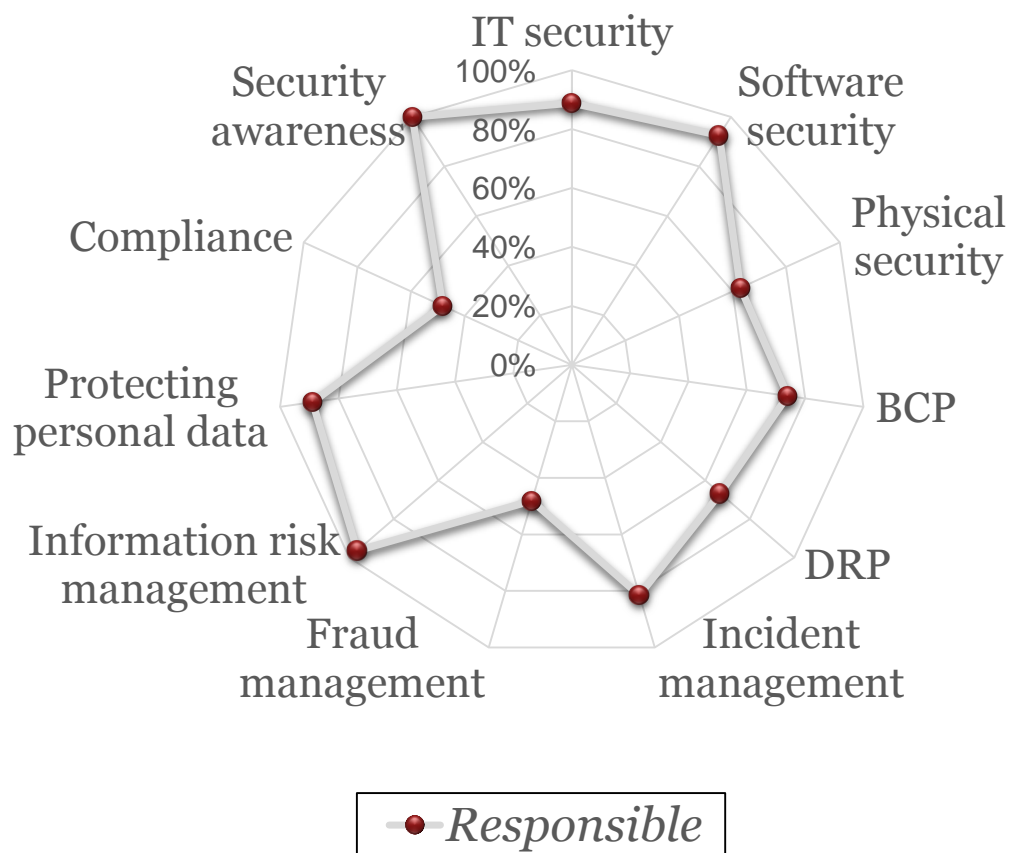
CISO's activity

► Communication with authorities



CISO's activity

► Responsibilities



52% are not responsible for **compliance**

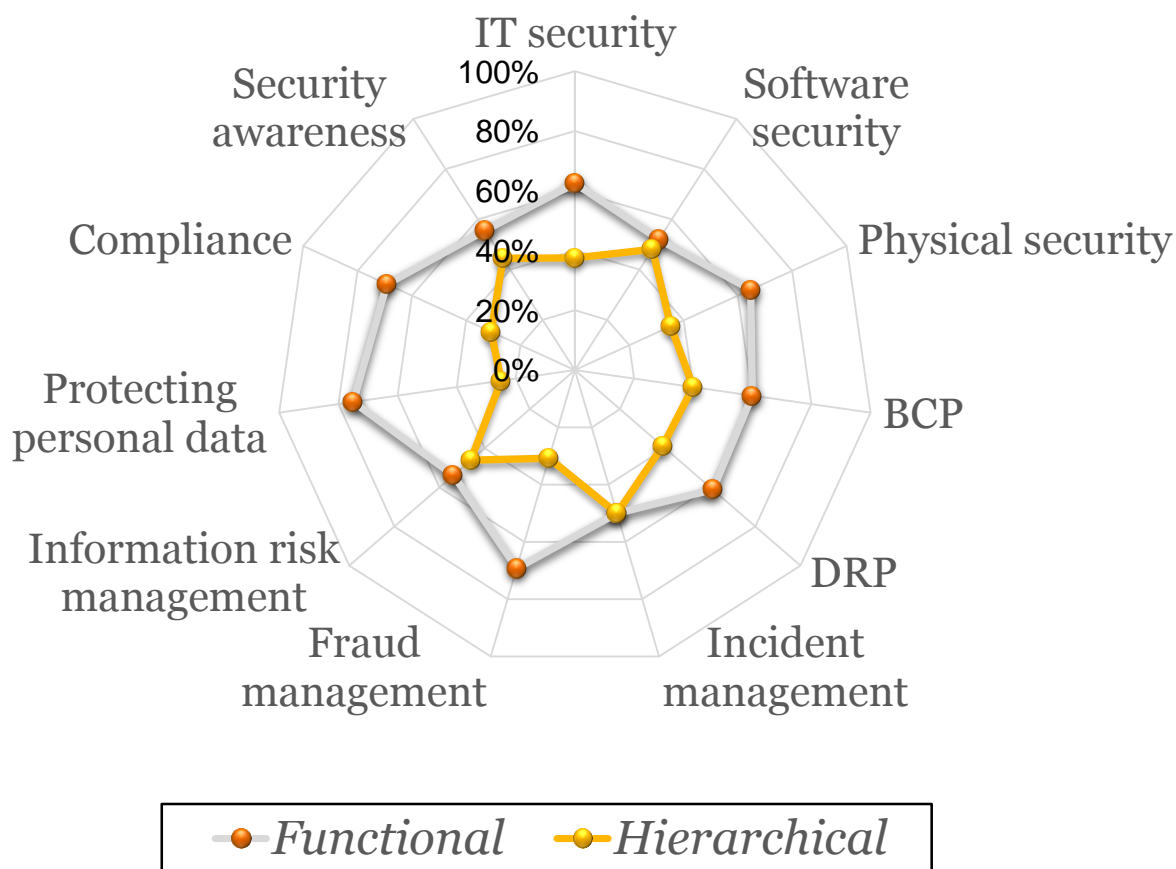
52% are not responsible for **fraud management**

37% are not responsible for **physical security**

26% are not responsible for **BCP**

CISO's activity

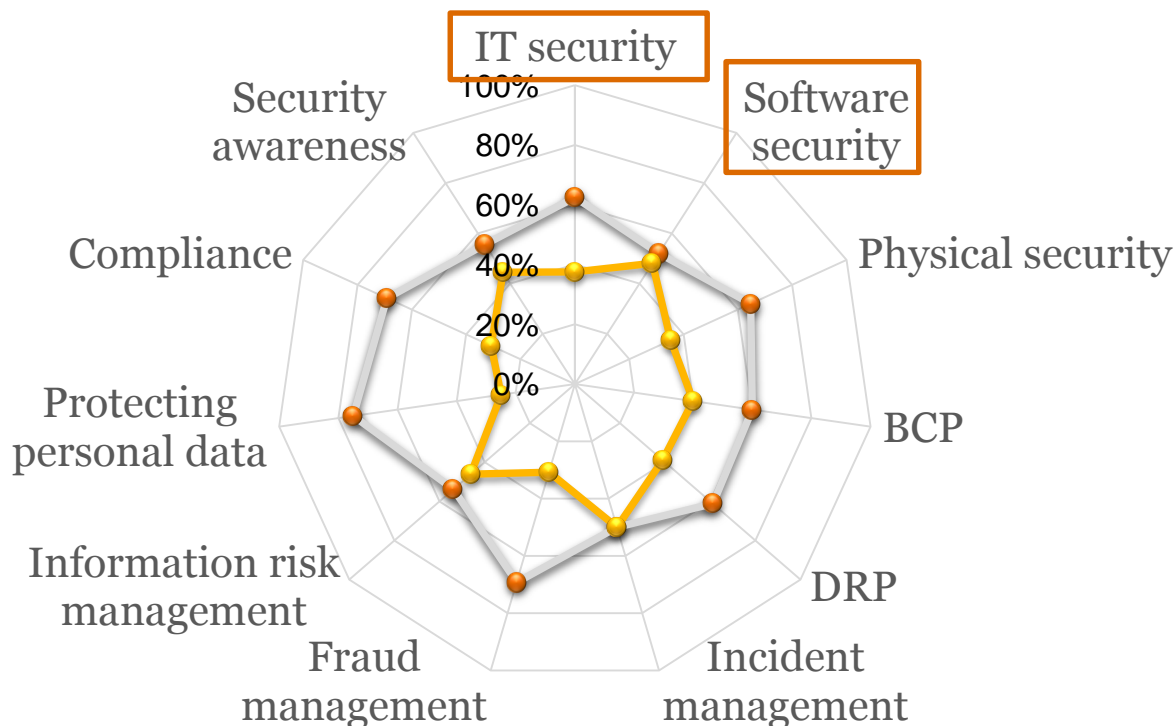
► Responsibility type



Most CISO's have functional responsibilities regarding security capabilities

CISO's activity

► Responsibility type



● Functional ● Hierarchical

IT Security

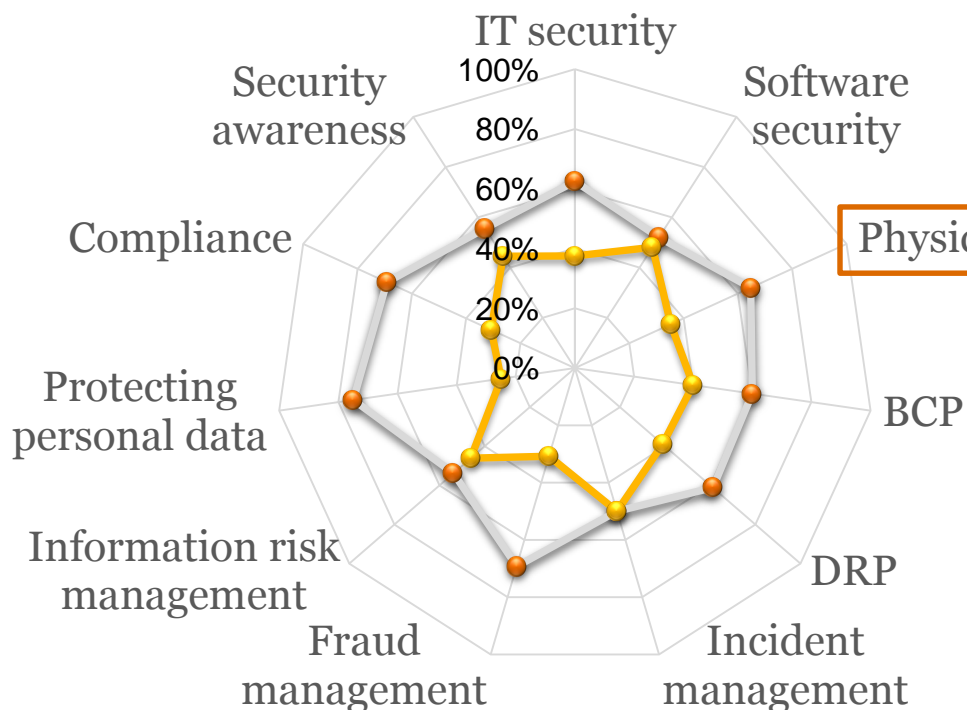
38% *have a hierarchical responsibility*

Software security

48% *have a hierarchical responsibility*

CISO's activity

► Responsibility type

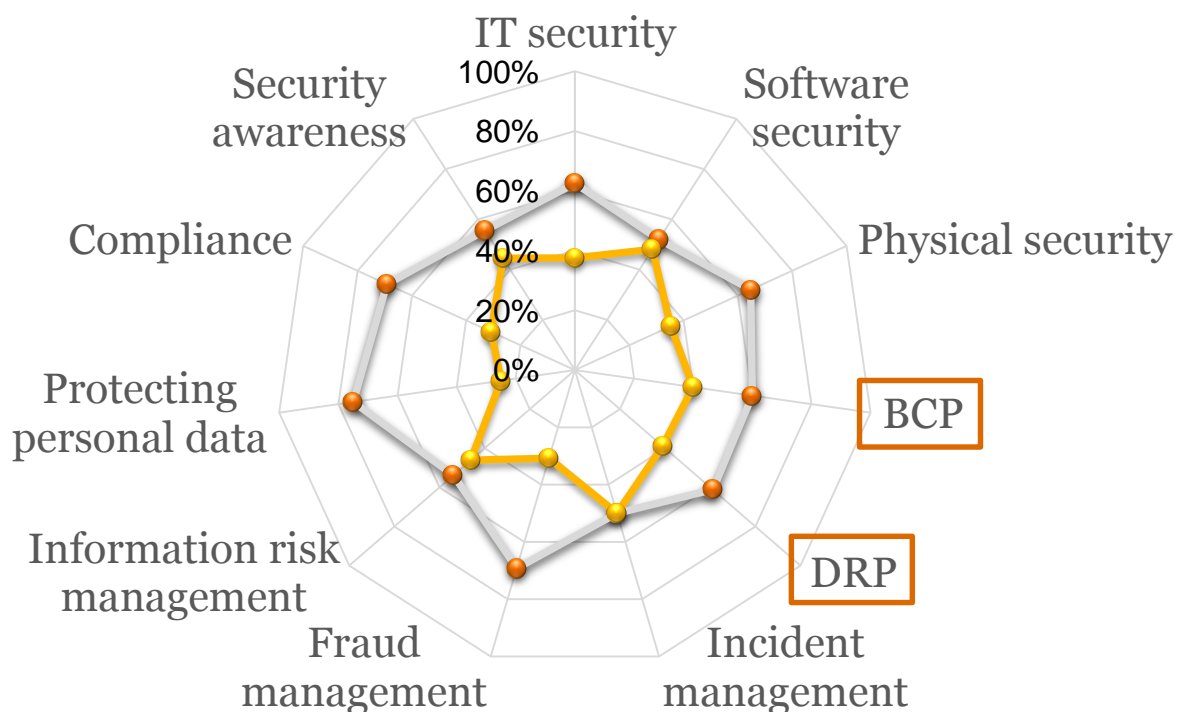


Physical security
35% *have a hierarchical responsibility*

● Functional ● Hierarchical

CISO's activity

► Responsibility type



● Functional ● Hierarchical

BCP

40%

have a hierarchical responsibility

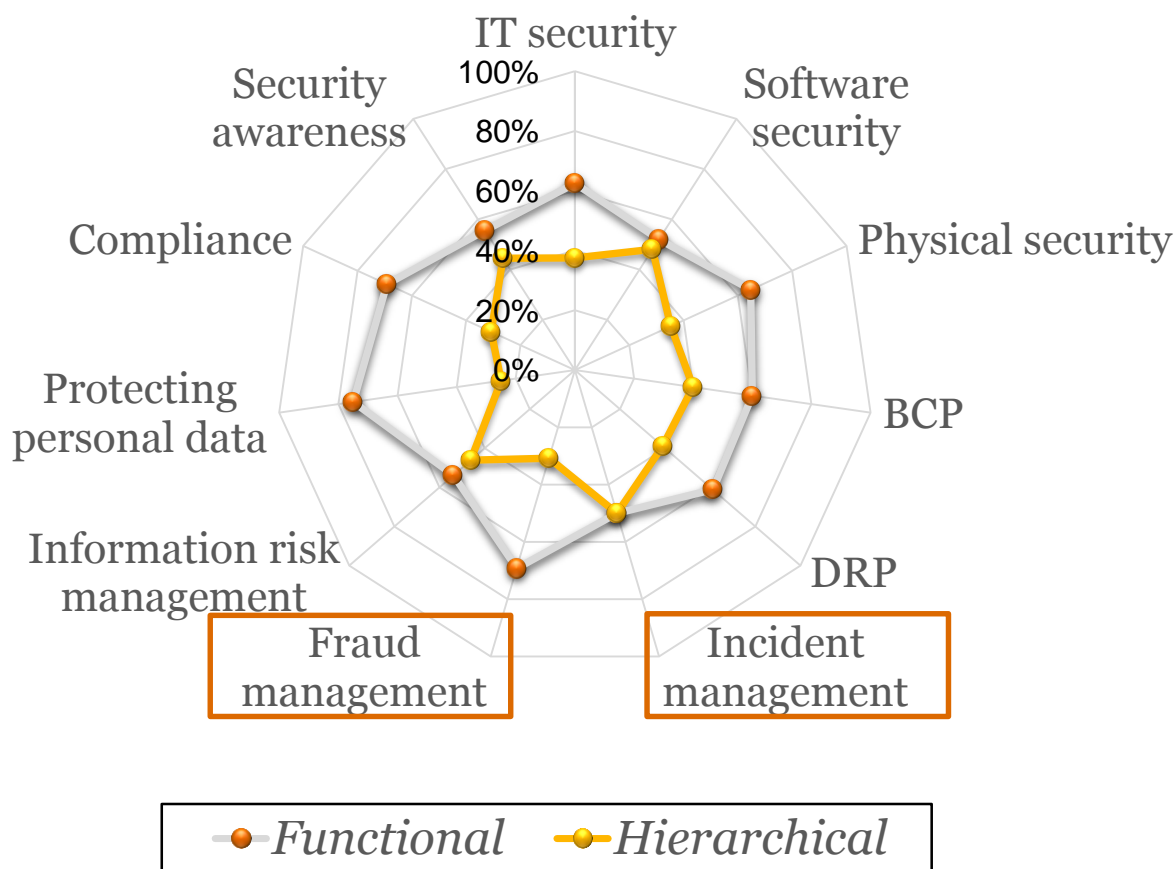
DRP

39%

have a hierarchical responsibility

CISO's activity

► Responsibility type



Incident management

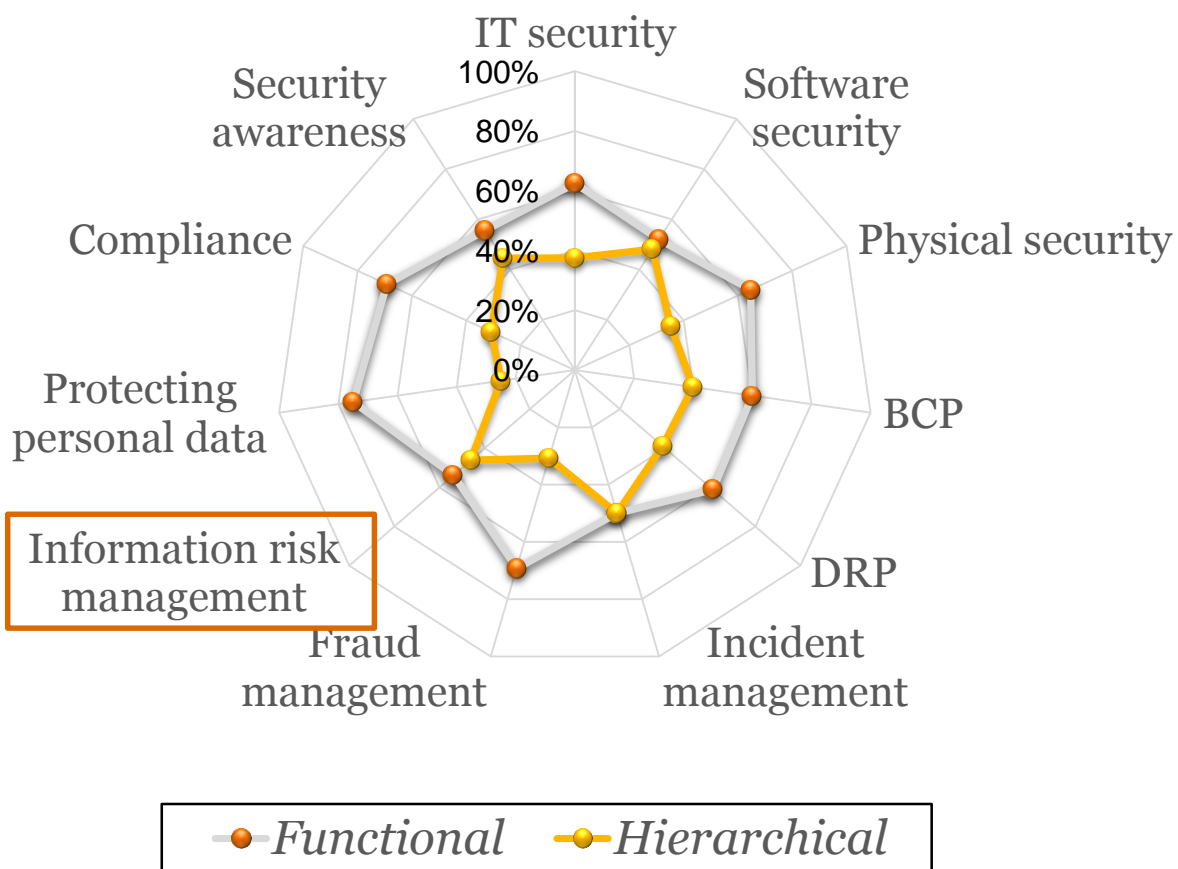
50% *have a hierarchical responsibility*

Fraud management

31% *have a hierarchical responsibility*

CISO's activity

► Responsibility type

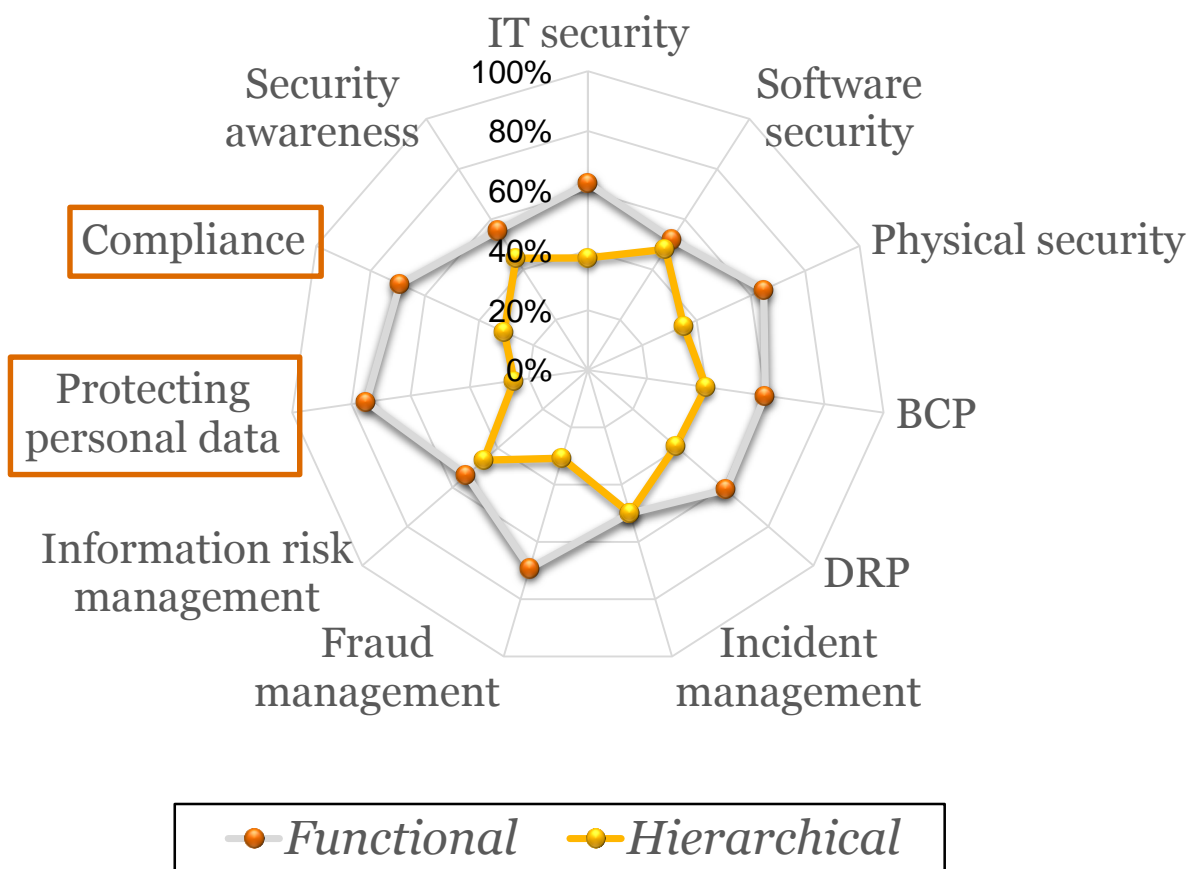


Information risk management

46% *have a hierarchical responsibility*

CISO's activity

► Responsibility type



Protecting personal data

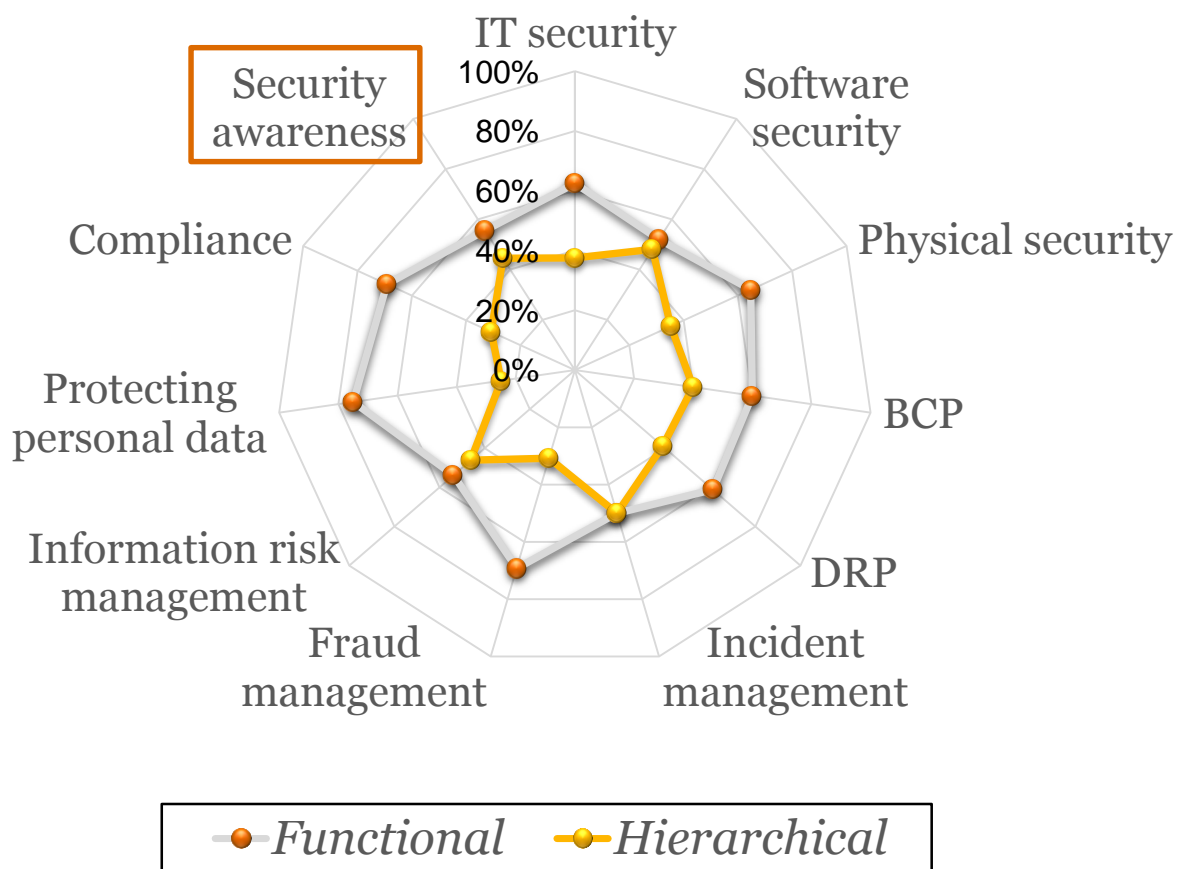
25% *have a hierarchical responsibility*

Compliance

31% *have a hierarchical responsibility*

CISO's activity

► Responsibility type



Security awareness
44% *have a hierarchical responsibility*

Governance at CISO level

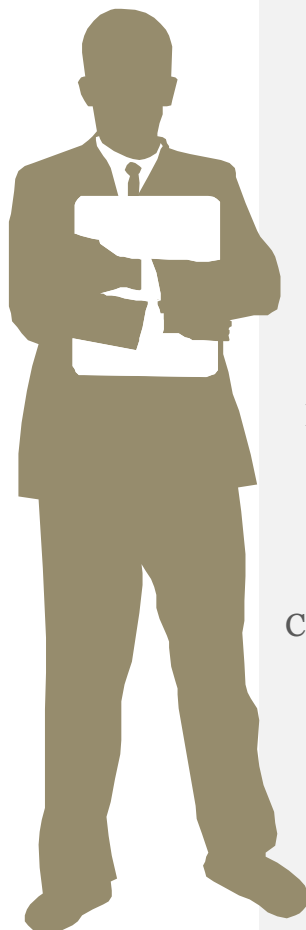
▶ Do you report directly to a member of the Board?

74%

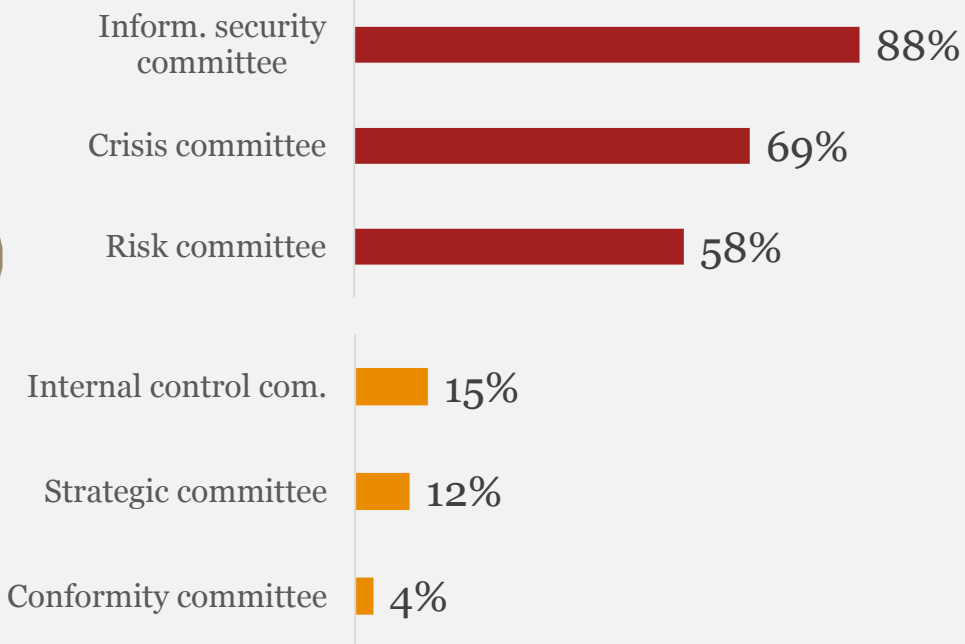
do in small to medium companies (staff < 1000)

50%

do in large companies (staff > 1000)



▶ Involvement in committees

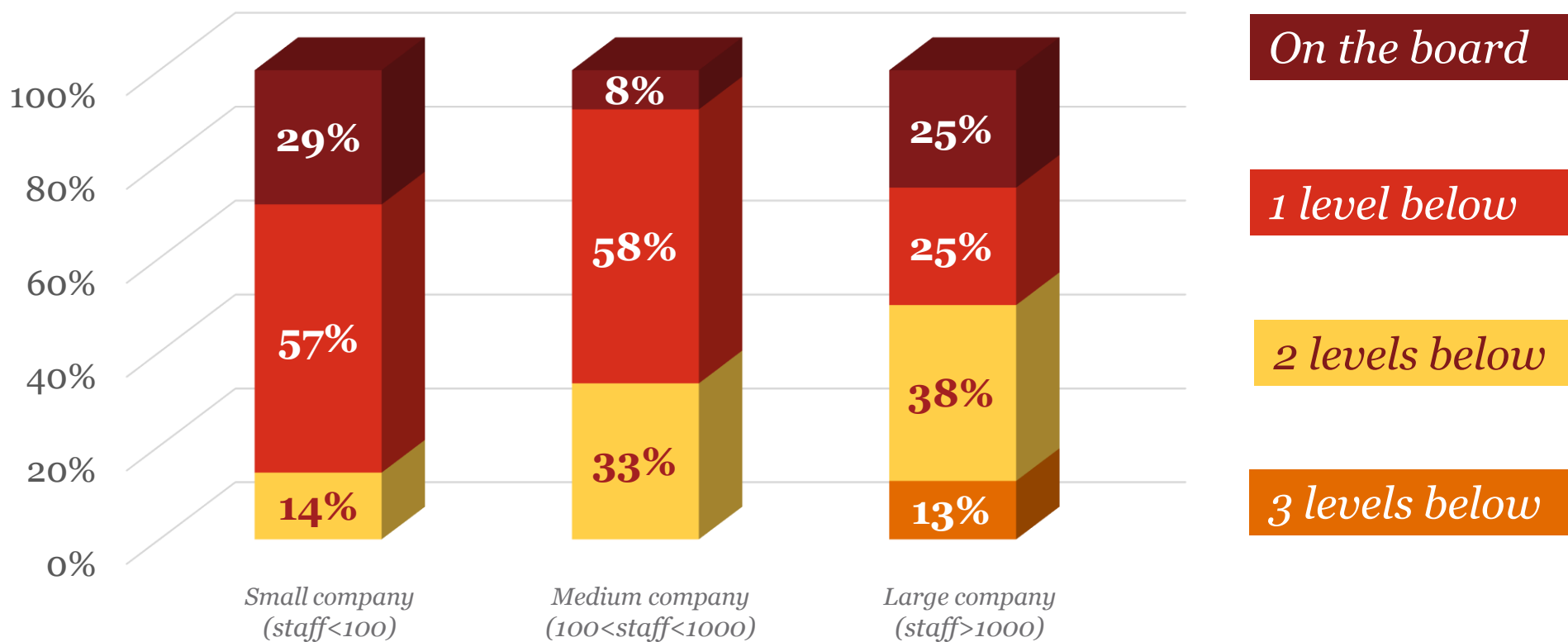


93% are part of some committee

0% are part of an executive committee

Governance at CISO level

▶ Level in relation to the Board



Governance at CISO level

▶ Most frequently outsourced

Security monitoring, **52 %**



Threat and vulnerability management, **52 %**



Network security, **48 %**



▶ Least frequently outsourced

Privacy, **7 %**



Third party management, **11 %**



Governance and organisation, **11 %**



Governance at CISO level

▶ Most frequently outsourced

Security monitoring, **52 %**

Threat and vulnerability management, **52 %**

Network security, **48 %**

▶ Least frequently outsourced

Privacy, **7 %**

Third party management, **11 %**

Governance and organisation, **11 %**



Governance at CISO level

▶ Most frequently outsourced

Security monitoring, **52 %**



Threat and vulnerability management, **52 %**



Network security, **48 %**

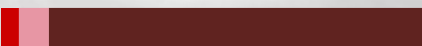


▶ Least frequently outsourced

Privacy, **7 %**



Third party management, **11 %**

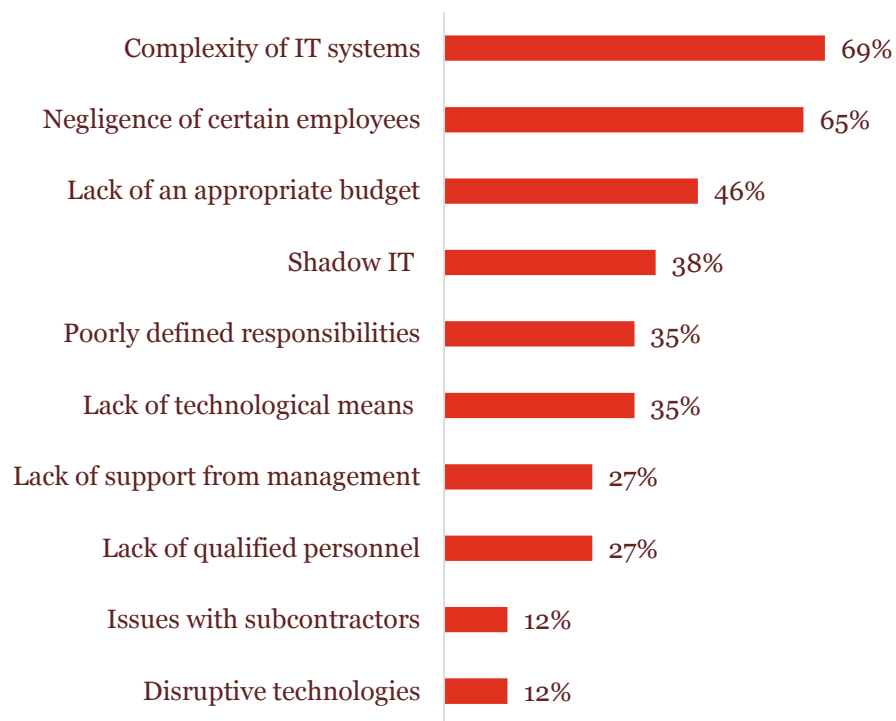


Governance and organisation, **11 %**

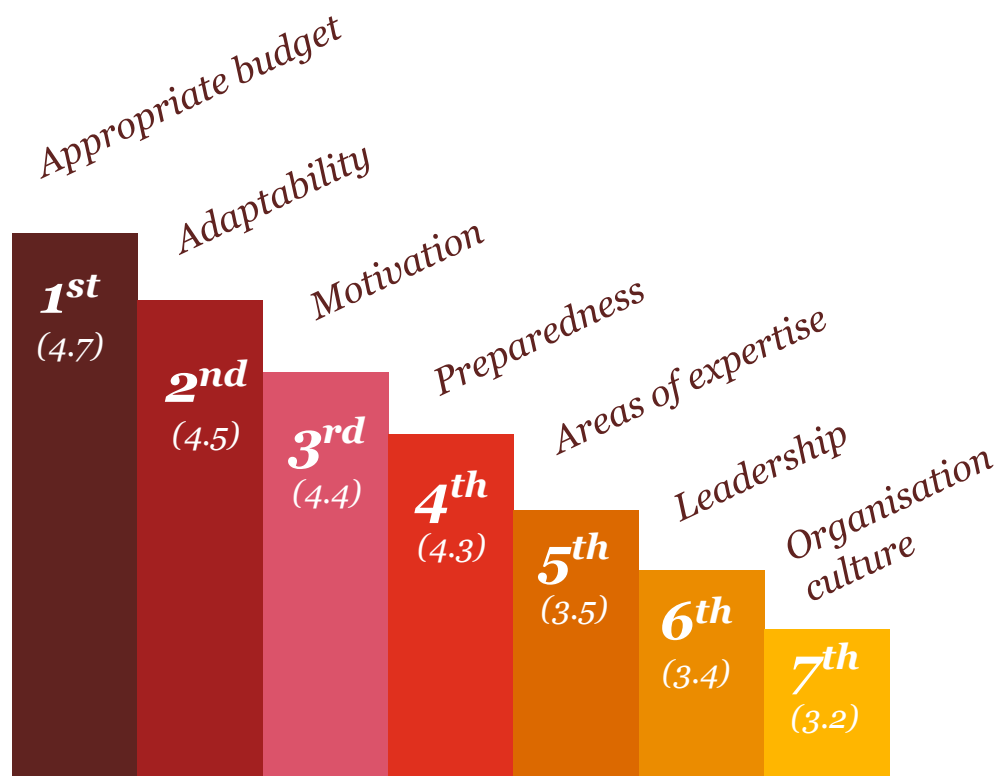


Perception of the job

▶ Main barriers to success



▶ Top 7 success factors



Average rank (1-7)

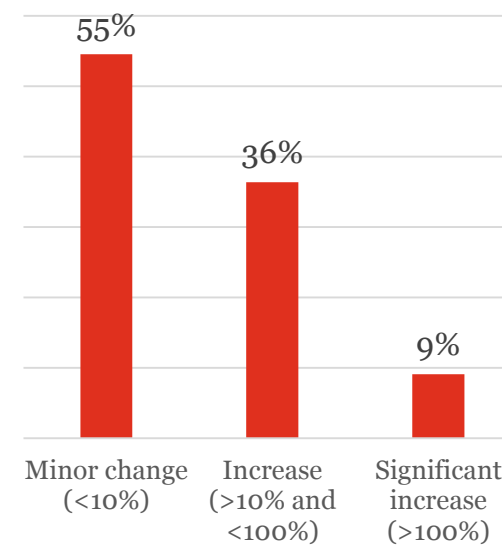
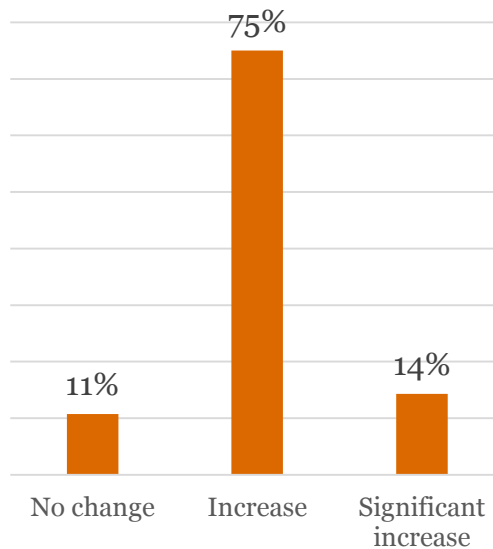
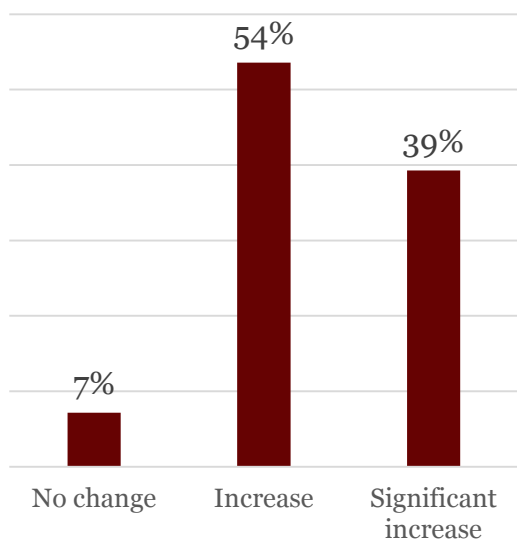
Perception of budget

| **73%** *think the budget they manage is sufficient*



Perception of security

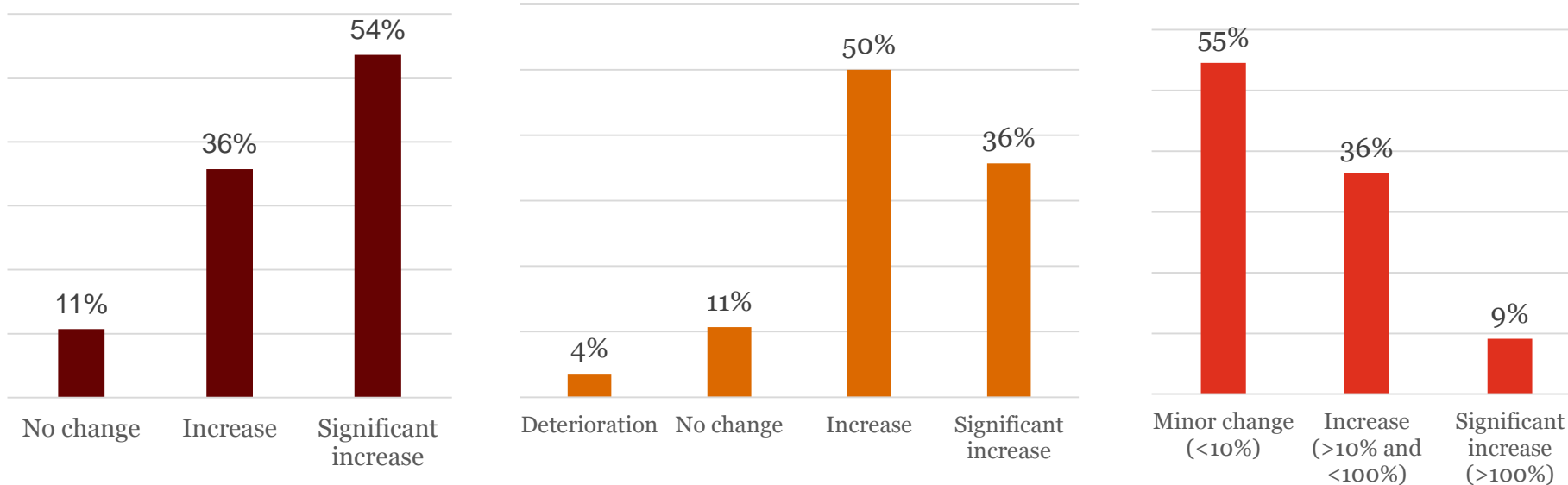
► Over the last three years



 **Level of threat**
 **Security level of the company**
 **Budget evolution**

Perception of security

► In the years to come



Level of threat

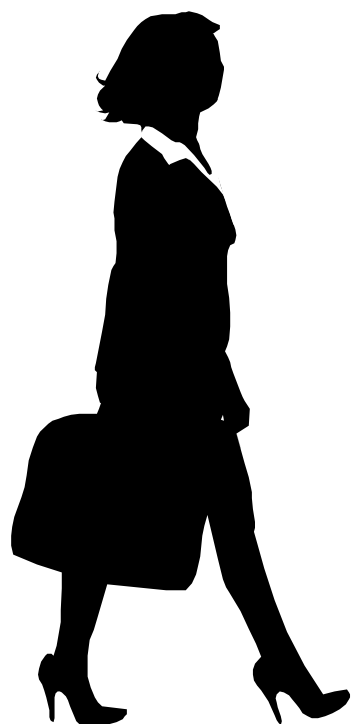


Security level of the company



Budget evolution

Perception of the job



▶ How complex is your job in the current context?

Easy

0 %

Reasonable

8 %

Acceptable

31 %

Complex

62 %

▶ How would you qualify your job in the current context?

*Worst job
I've ever
had*

0 %

*Not good
but not the
worst job*

0 %

*Good job,
but not the
best*

50 %

*Best job
I've ever
had*

50 %

Your contacts

Rodolphe Mans

President, CPSI

rodolphe.mans@bil.com

Vincent Villers

Cybersecurity Leader, PwC Luxembourg

vincent.villers@lu.pwc.com

Ludovic Raymond

Cybersecurity Director, PwC Luxembourg

ludovic.raymond@lu.pwc.com

Marie Bianchini

Marketing, PwC Luxembourg

marie.bianchini@lu.pwc.com

This publication is exclusively designed for the general information of readers and is (i) not intended to address the specific circumstances of any particular individual or entity and (ii) not necessarily comprehensive, complete, accurate or up to date and hence cannot be relied upon to take business decisions. Consequently, PricewaterhouseCoopers, Société coopérative (“PwC Luxembourg”) does not guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. The reader must be aware that the information to which he/she has access is provided “as is” without any express or implied guarantee by PwC Luxembourg.

PwC Luxembourg cannot be held liable for mistakes, omissions, or for the possible effects, results or outcome obtained further to the use of this publication or for any loss which may arise from reliance on materials contained in it, which is issued for informative purposes only. No reader should act on or refrain from acting on the basis of any matter contained in this publication without considering and, if necessary, taking appropriate advice in respect of his/her own particular circumstances.

PwC Luxembourg (www.pwc.lu) is the largest professional services firm in Luxembourg with 2,600 people employed from 58 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 by contributing to the smooth operation of the capital markets and providing advice through an industry-focused approach.

The PwC global network is the largest provider of professional services in the audit, tax and management consultancy sectors. We are a network of independent firms based in 157 countries and employing over 208,000 people. Talk to us about your concerns and find out more by visiting us at www.pwc.com and www.pwc.lu.

© 2016 PricewaterhouseCoopers, Société coopérative. All rights reserved.

In this document, “PwC” or “PwC Luxembourg” refers to PricewaterhouseCoopers, Société coopérative which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity. PwC IL cannot be held liable in any way for the acts or omissions of its member firms.