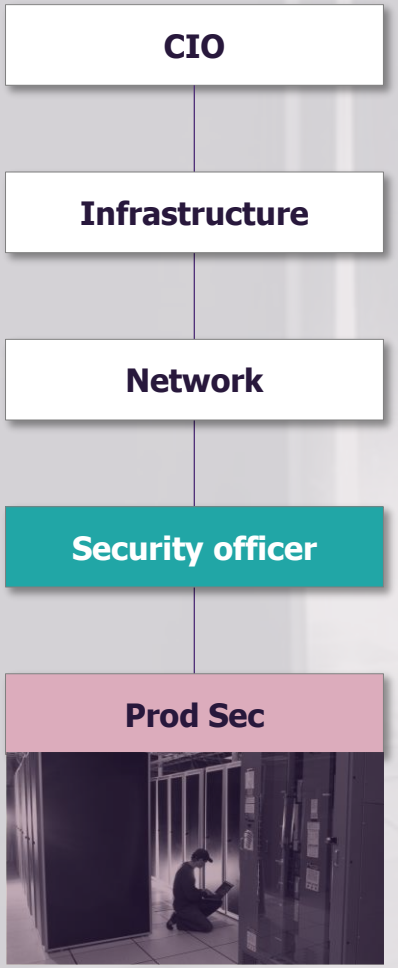
Security Operating Model
Trends & challenges

Gabriel AMIRAULT
Senior Manager

Vincent ROYER
Associated Partner


Once upon a time, long ago, there was… a CISO

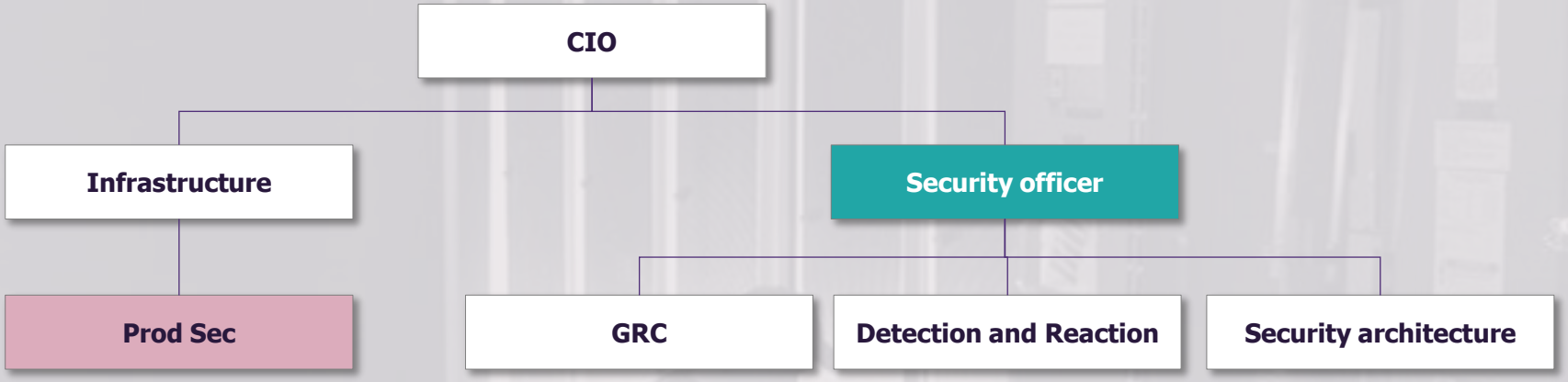
A bit of history…



15/20 years ago…

- **CISO** was not a CISO but more of a security officer
- Usually a tech guy in charge of security operations
- …almost unknown to Top Management

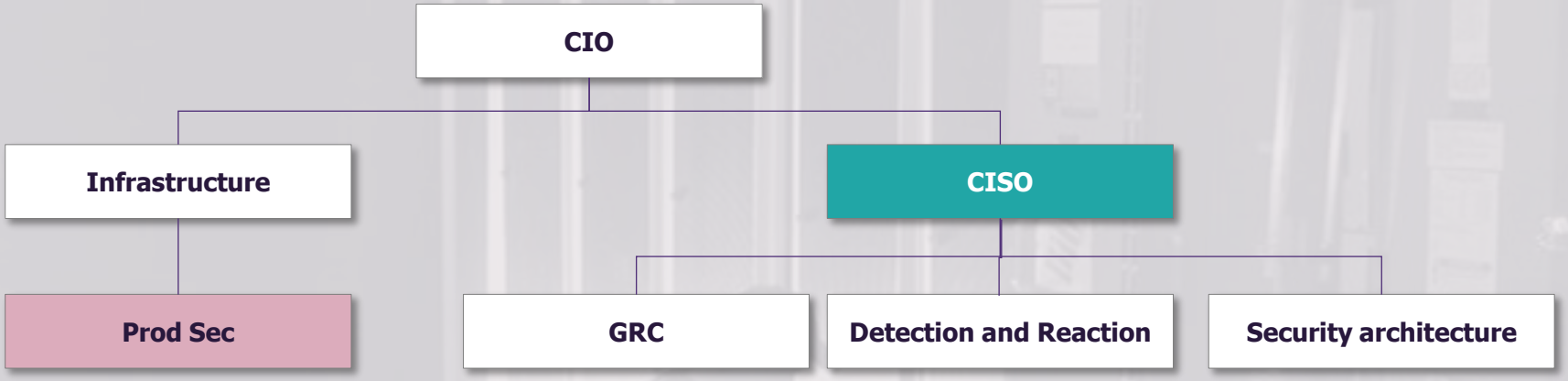
A bit of history…



10 years ago…

- CISO moved up the range
- He structured his team
- Top management is starting to become aware of the cyber challenge

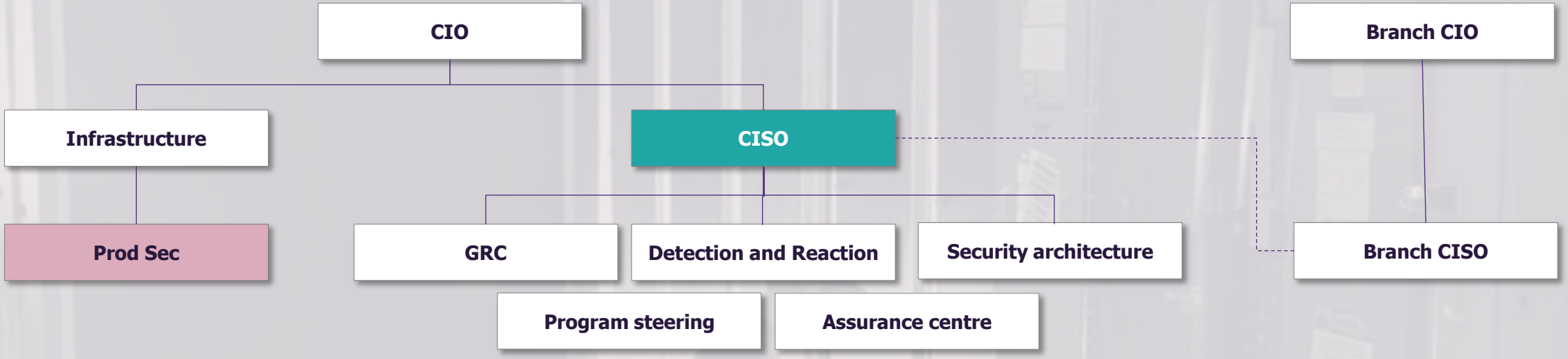
A bit of history…



10 years ago…

- CISO moved up the range
- He structured his team
- Top management is starting to become aware of the cyber challenge

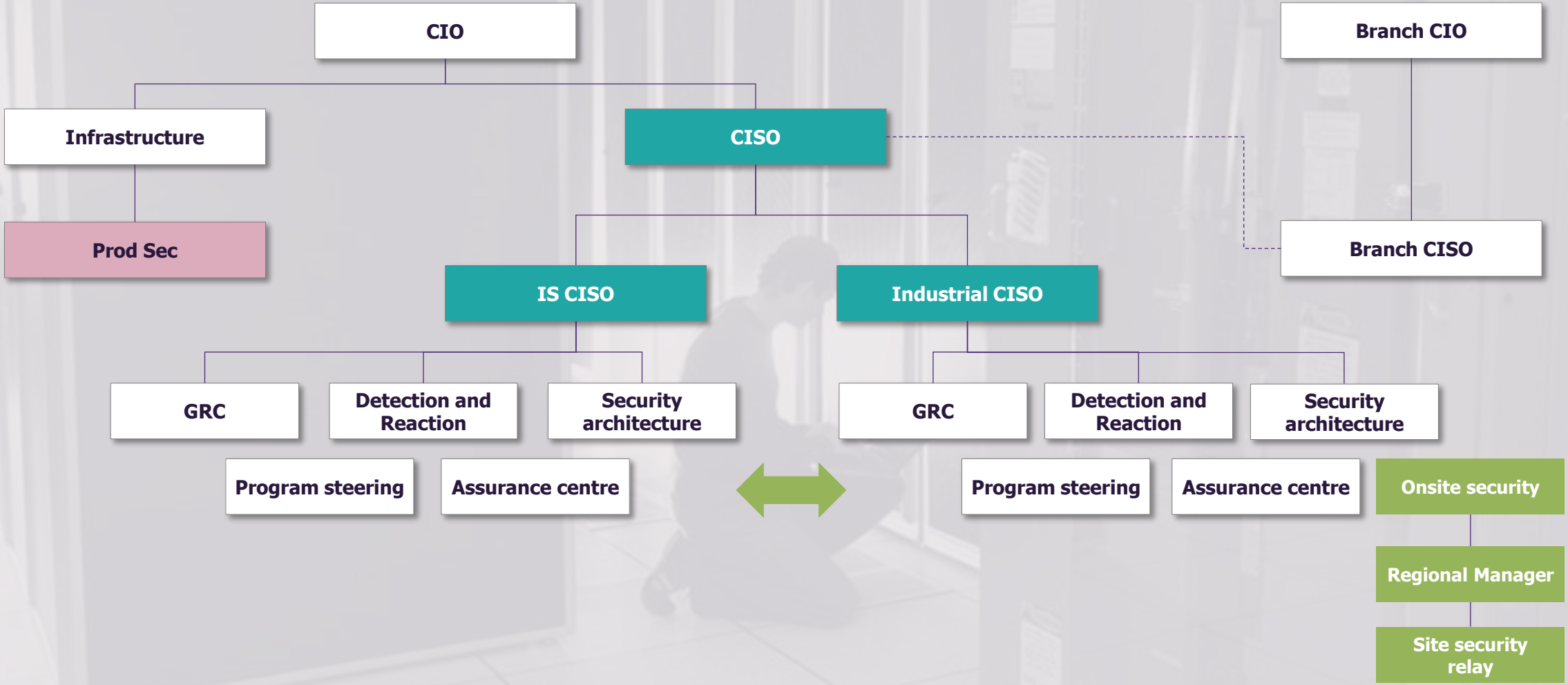
A bit of history…



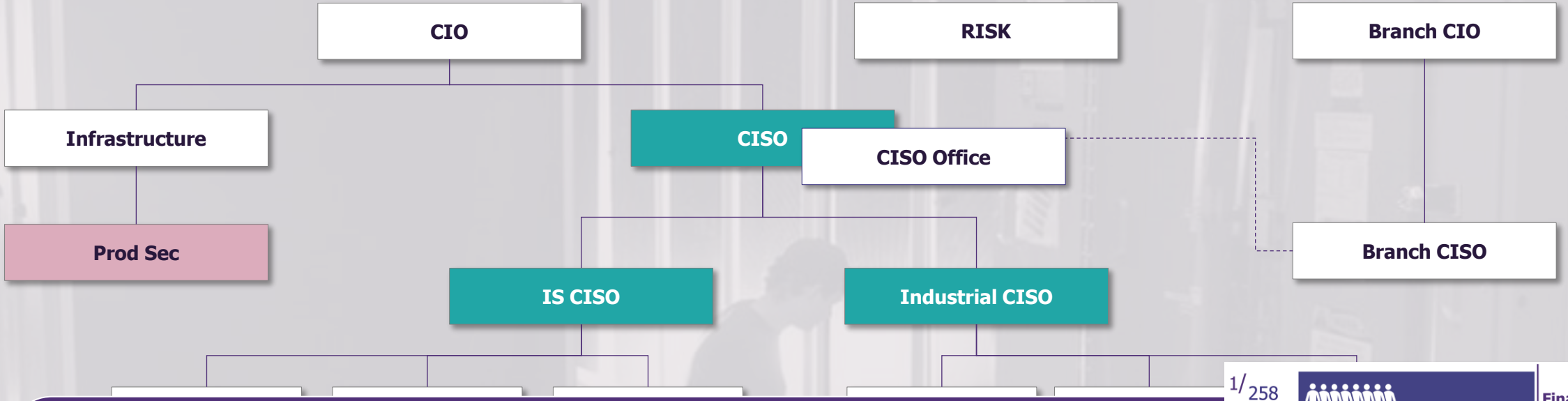
5 years ago…

- Cyber rolls out across business lines
- Cyber activities become industrialised
- Top management requests regular cyber reporting

A bit of history…

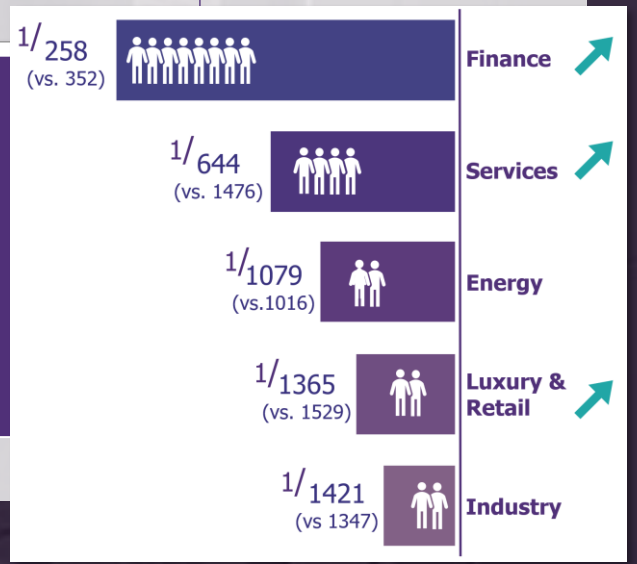


A bit of history…

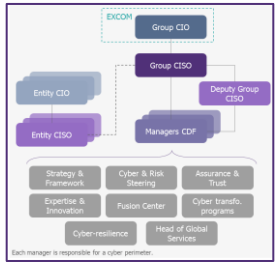


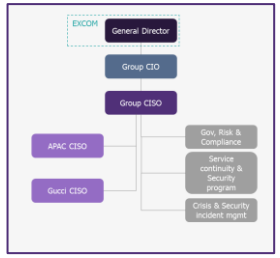
Today, models are relatively stable and mature, but CISOs are facing new challenges:

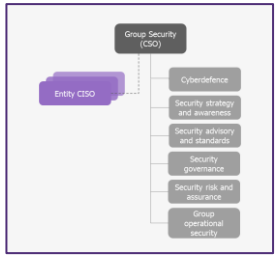
- / Cyber teams are still growing and becoming more difficult to manage
- / There are more are more interfaces with the rest of the structure
- / Regulators require an increasingly consolidated view of risks

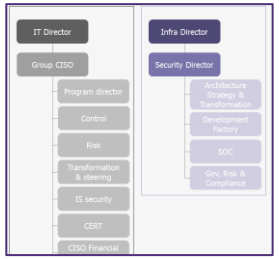


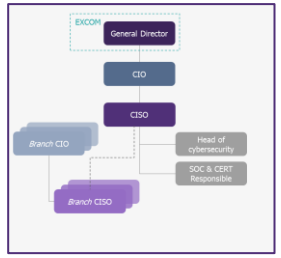
Numerous models on the market... with new common drivers

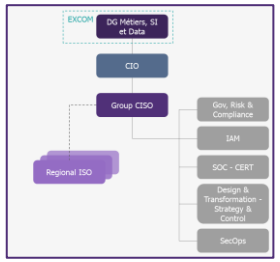


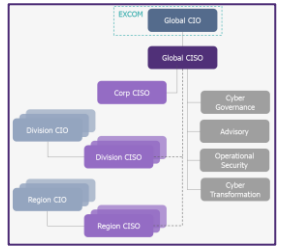


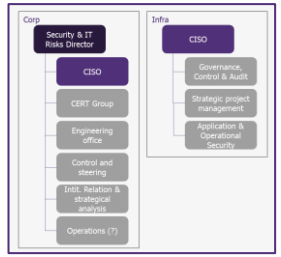










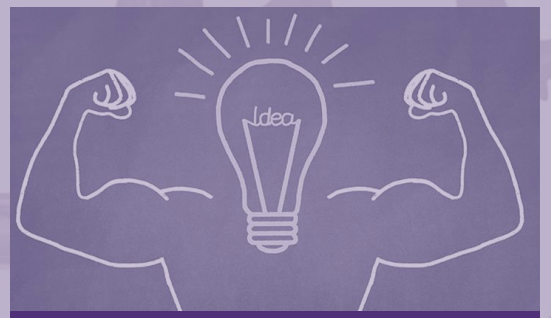


"Clarify roles and responsibilities among the lines of defense / business / IT."

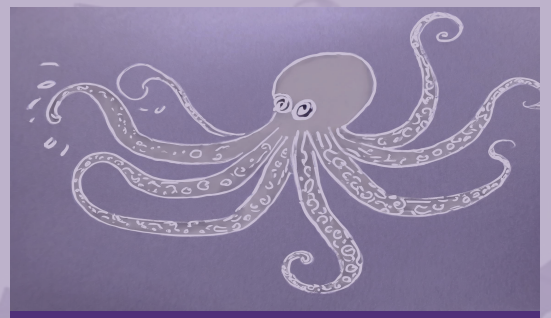
"Strengthen the group's authority, on a global scale."

"Search for efficiency levers among entities (redundancy, pooling)"

3 major trends for Groups' CISOs



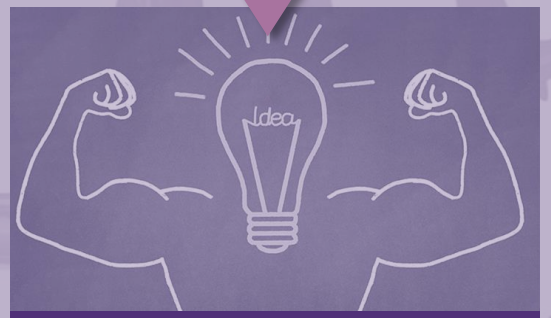
Strengthen his authority



Extend his field of action

Security is not just the CISO's business

3 major trends for Groups' CISOs



Strengthen his authority

Extend his field of action

Security is not just the CISO's business

Groups' CISOs are strengthening their accountability with a more compelling governance

Reinforce the relationship with BU CISOs

- Strong functional reporting line
- Possibly direct reporting line
- Granular model to be planned for sub-entities

Define and enforce a common Group strategy

- Group Framework with a compliance target to reach
- Group level control and reporting
- Cyber budget consolidation and monitoring at group level

Create Cybersecurity service lines

- Provide services and expertise for all entities
- Centralization of specific teams
- Coordination of Cyber expertise communities

➔ Implement a Lines of Defense (LoD) model

Under the impulse of FS regulators, organizations have implemented Cyber functions organized into different Lines of Defense (LoD)

Separation of Duty

Group CISO (LoD1.5, sometimes LoD2)

- Strategy and Policies definition
- Control deployment , follow-up & C-Level Reporting
- Shared Cyber Security services (SOC/CSIRT, VOC, IAM…)
- Advanced expertise (incl. OT), Security support on critical projects

Operational/BU CISOs (LoD1.1)

- Follow the deployment of policies & security rules
- Manage Security BAU (vuln. remediation, local incident/exception management, operational reporting…)
- Project Security support

Financial Institutions

Industry / Retail / Energy

	Financial Institutions		Industry / Retail / Energy
LoD3	Internal Audit / General Inspection		Safety / Risk and Internal Audit
LoD2	Operational Risk / Compliance	Transposed	**Group CISO**
LoD1	**Group CISO** Operational / BU CISOs		Operational / BU CISOs

To enforce a common strategy, the Group's CISO is positioned as a provider of cybersecurity services and support to the entities

Group-wide tools and services

Provide and impose standardized security solutions to all entities

DLP
SOC / CERT
PKI/KMS
VOC
IAM
…

Shared services and activities delegated to the Group

Avoid redundancy & consolidate costs, harmonize practices and centralize cutting-edge expertise

Awareness
Assurance / Red Teaming
Homologation
Security into project
Cloud Security
…

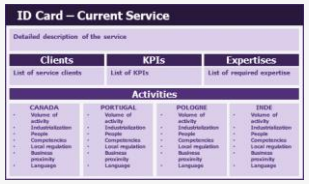
How to encourage Group services adoption?

- Product mode (QoS, client-oriented, scalability…)
- Industrialisation and promotion
- Incentiveness (ROI & cost-effectiveness, framework compliance…)

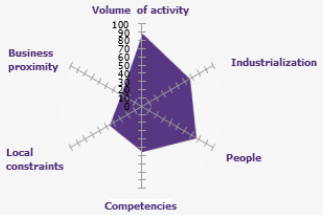
Cyber Smart Sourcing: how to scale up cyber services and boost efficiency?

How?

AS IS Services ID Card formalization



Activities scoring & eligibility matrix



Definition of smart sourcing scenarios

In the financial sector, the trend is towards 30% of budget activities being offshored

What & Where?

On-shore

Services with very sensitive activities (inc. data management): **Red Teaming**, **Crisis Management**…

Local constraints requiring on-site activity

Service with strong need of proximity with clients of the service

Near-shore

Services requiring qualified profiles at a lower cost: **Security into project**, **TPRM**, **Cloud Security**…

The proximity of the location allows better exchanges and management, and local regulation compliance

Off-shore

Services with low added value, trivialized and on order with standardized processes: **VOC**, **Controls**, **L1 SOC**, **standard pentesting**…

The cost of the activity is very low and with few management

For now essentially internal x-shoring but starting to appear in outsourced services

Change

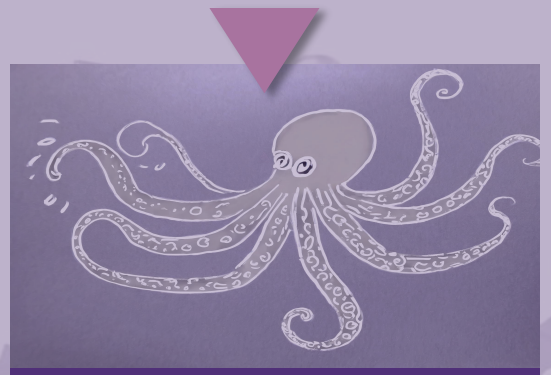
Framing of the Transition Program

- Transition Governance *(prioritization, KPI & dashboard…)*
- Activity transfer methodology *(KT, shadowing, handover…)*
- Change management & Comm'
- Upskilling & Training
- Recruitment plan
- Tooling & Access

Once transited to RUN, remember to "cut the cord" to empower X-shore teams

3 major trends for Groups' CISOs

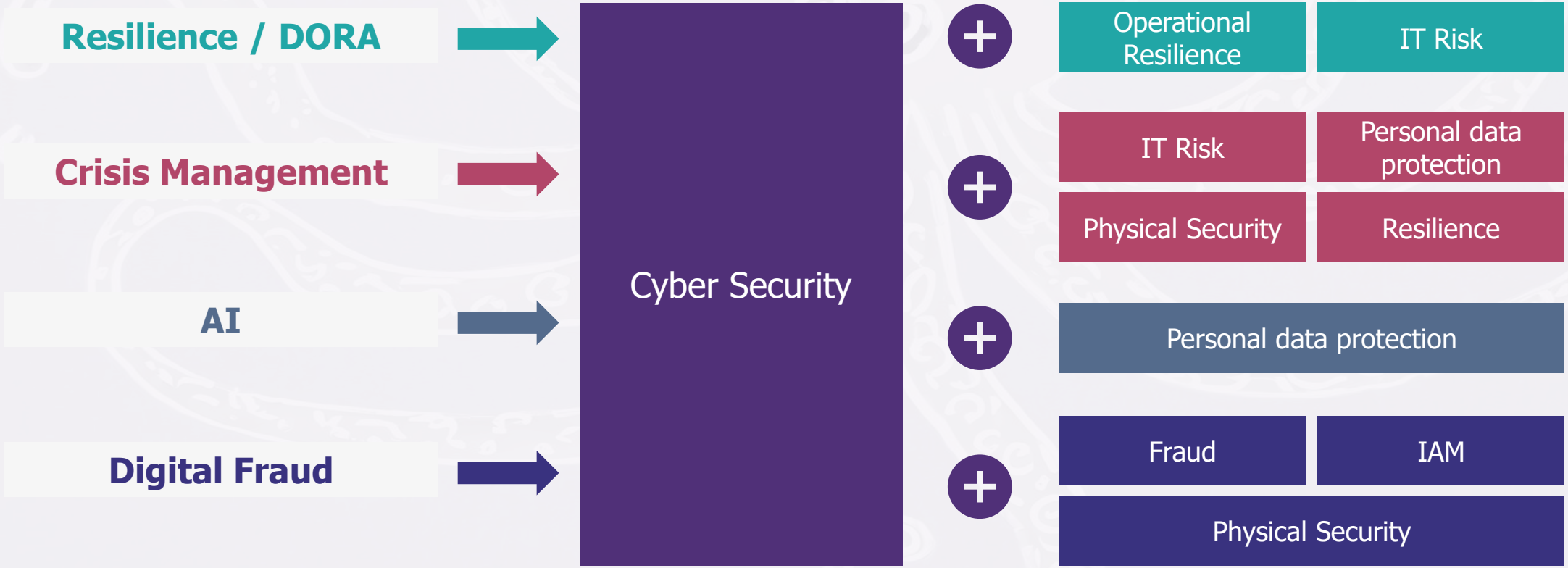
Strengthen his authority



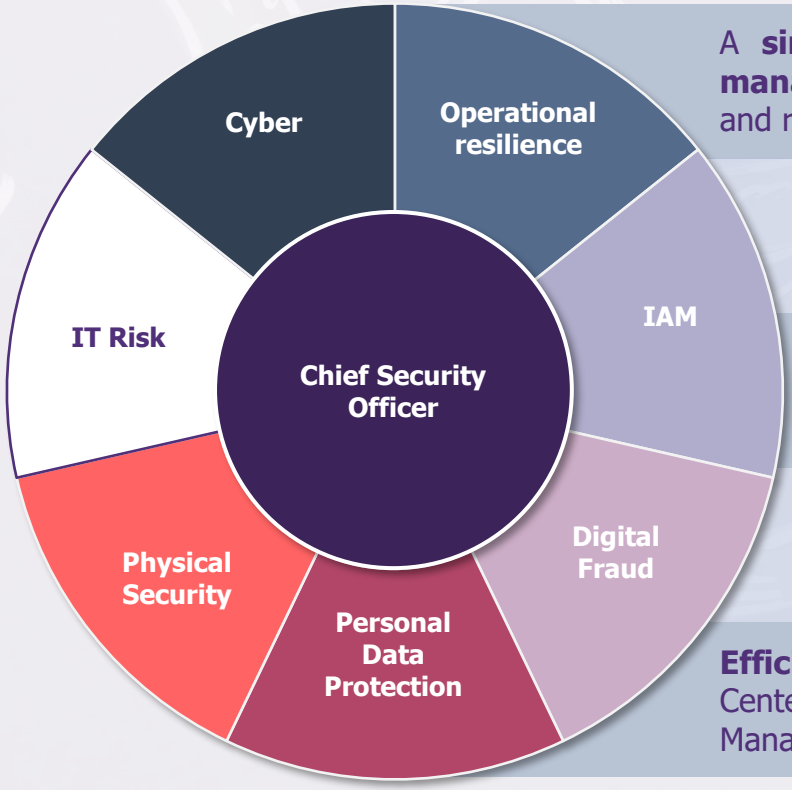
Extend his field of action

Security is not just the CISO's business

CISO has to work more and more closely with other risk teams…



...leading to the convergence of different risk functions under the responsibility of a Chief Security Officer (CSO)



Benefits of the convergence

A **single** point of contact **reporting** to **top management** with a holistic view of security and risks

A **unified** and **coordinated approach** towards **business** functions: same vocabulary, methods, tools…

Convergence of critical perimeters through the common definition of **IBS** *(Important Business Services)* and **risk tolerance**

The ability to provide dynamic **career paths** and **attract talents**

Efficiency gains in key activities (Fusion Center, Threat Intelligence, Third-Party Risk Management)

In major European Banks:

40% have appointed a CSO - at least 3 functions converged

35% are in the process of appointing a CSO

No common mandate of the scope of the CSO

Key points to start the convergence journey

0 Pooling responsibilities and adjusting the reporting level of the CSO

- **Group converged functions** under the direct responsibility of the CSO
- …with the potential impact of the CSO's reporting line, and therefore the CISO's

1 Build stronger synergies between converged functions processes

- **Global** policies/**framework**
- **Consolidated risk vision** (taxonomy, risk mapping, alignment with business processes…)
- Shared identification of the **Important Business Services** (IBS)
- Single control **framework** (permanent controls, NIST assessments…)
- **Regulatory watch** (Cyber, Resilience, Privacy…)

2 Start bringing cross-functional teams together

- **Convergence the steering functions**
  - **CSO Office** to steer the entire scope: budgets, skills and Talent Management, awareness-raising, coordination…
  - **Control Tower**: control engineering for the Group/testing campaigns, consolidation of risk indicators and dashboards…
  - **Program** management
- **Upskill the teams on different areas of expertise** ➔ Coordination of **expert communities**
- **Provide common services**
  - **Unified threat** monitoring: Fusion Center (Fraud & Cyber & Physical Security) and Threat Intelligence
  - **Unified service offers** to the business

3 majors trends for Group's CISO

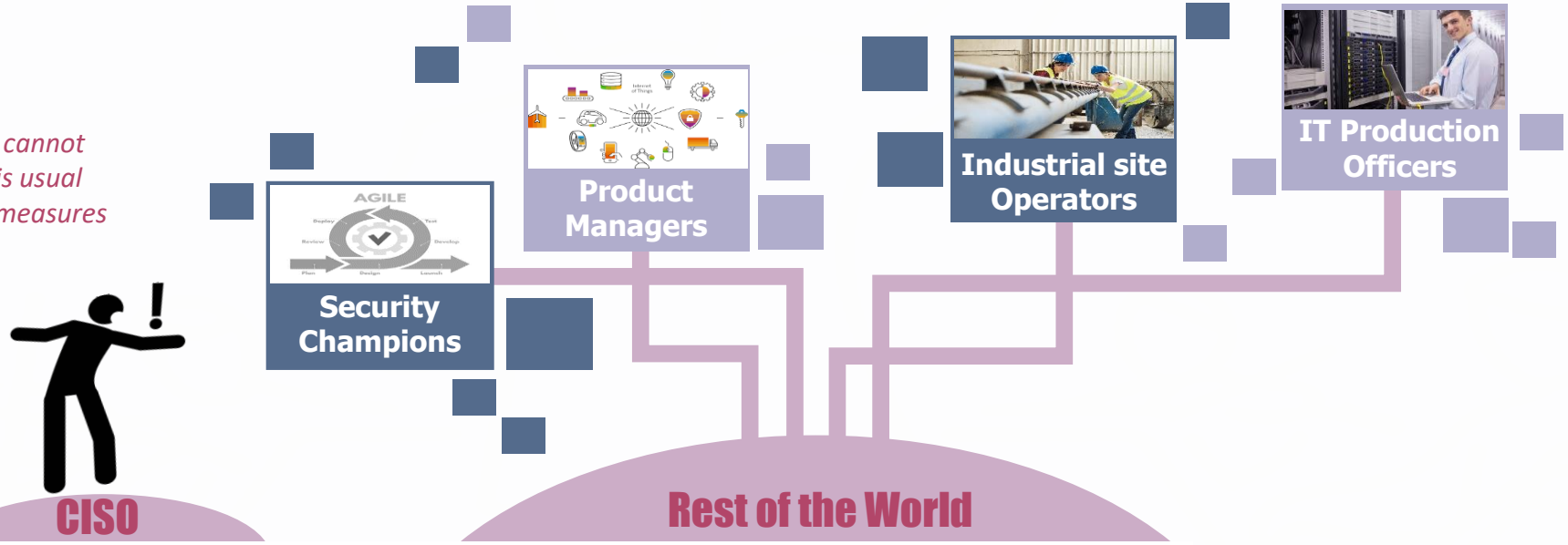
Strengthen his authority

Extend his field of action

Security is not just the CISO's business

Some subjects remain beyond the direct reach of the CISO

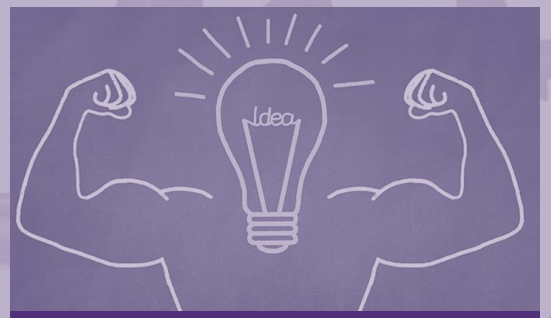
The CISO cannot deploy his usual arsenal of measures



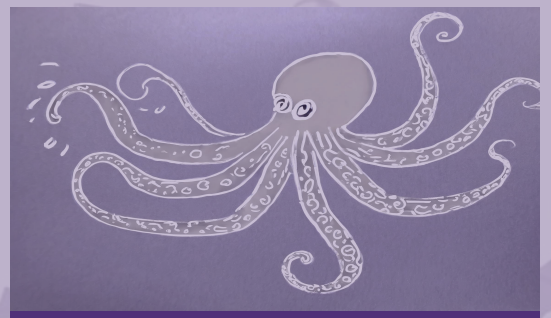
The operating model is less the solution than in-depth work with those others teams

- Guidelines & Standards
- Tooling & Industrialization
- Awareness & Cyber Security culture
- Controls & Compliance Checks
- Sponsoring & Incentives : Cyber skills & Career prospects

3 majors trends for Group's CISO



Strengthen his authority



Extend his field of action

Security is not just the CISO's business

And now how do we go about it?

It's always interesting to challenge whether one's organization **is still suitable**

Clarify your interfaces
(OT/Product stakeholders, DevOps Features Teams, Op. Risk, IT Ops,, Business…)

Identify efficiency levers
(governance, mandate, sponsoring, means, pooling, smartsourcing…)

Specify your needs
(efficiency, regulation, transformation…)

Our Boosters


Wavestone organization benchmark

TOM diagnosis and definition



Cyber roadmap examples

Budget and TOM benchmark



Templates and dashboards to monitor deployment

Wavestone CISO Radar on CISO priorities for 2024



Indicators to assess TOM model effectiveness