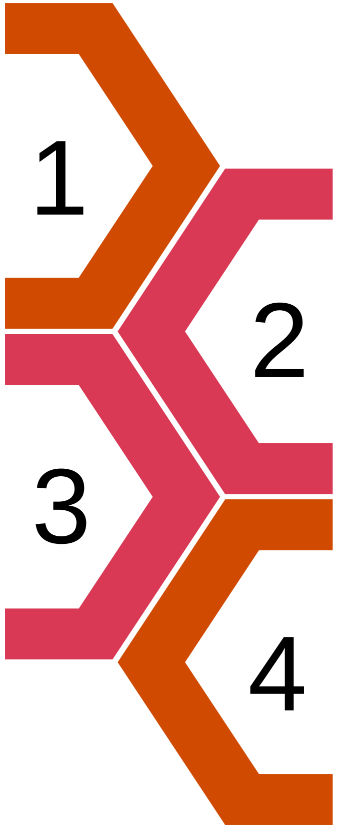
The future of cyber risk management

July 2019

Pain points in effectively managing and overseeing cyber risk

It is challenging to achieve **a common understanding** of **cyber risk management** efforts that spans the **3 lines of defense**



Cyber risk tolerance and **risk appetite** is not established or understood.

Security strategy does not **align with business objectives** or risk appetite.

Enterprise risk parlance is not used to articulate cyber risks.

The Board and **Executive** Leadership has **limited visibility** into impact of cyber risks.

Risk management ‘**ownership**’ is not established.

Roles and responsibilities across the **three lines** are often ambiguous.

Controls are **not designed to address risk** but to manage compliance.

Audit fatigue due to proliferation of compliance requirements.

PwC Survey – Technology risk management

Results from PwC's 2019 Survey into leading practices

https://www.pwc.com/ca/en/risk-opportunity/publications/568032-global-technology-risk-management-study-v2.pdf

Survey participants

Over 100 participant firms globally

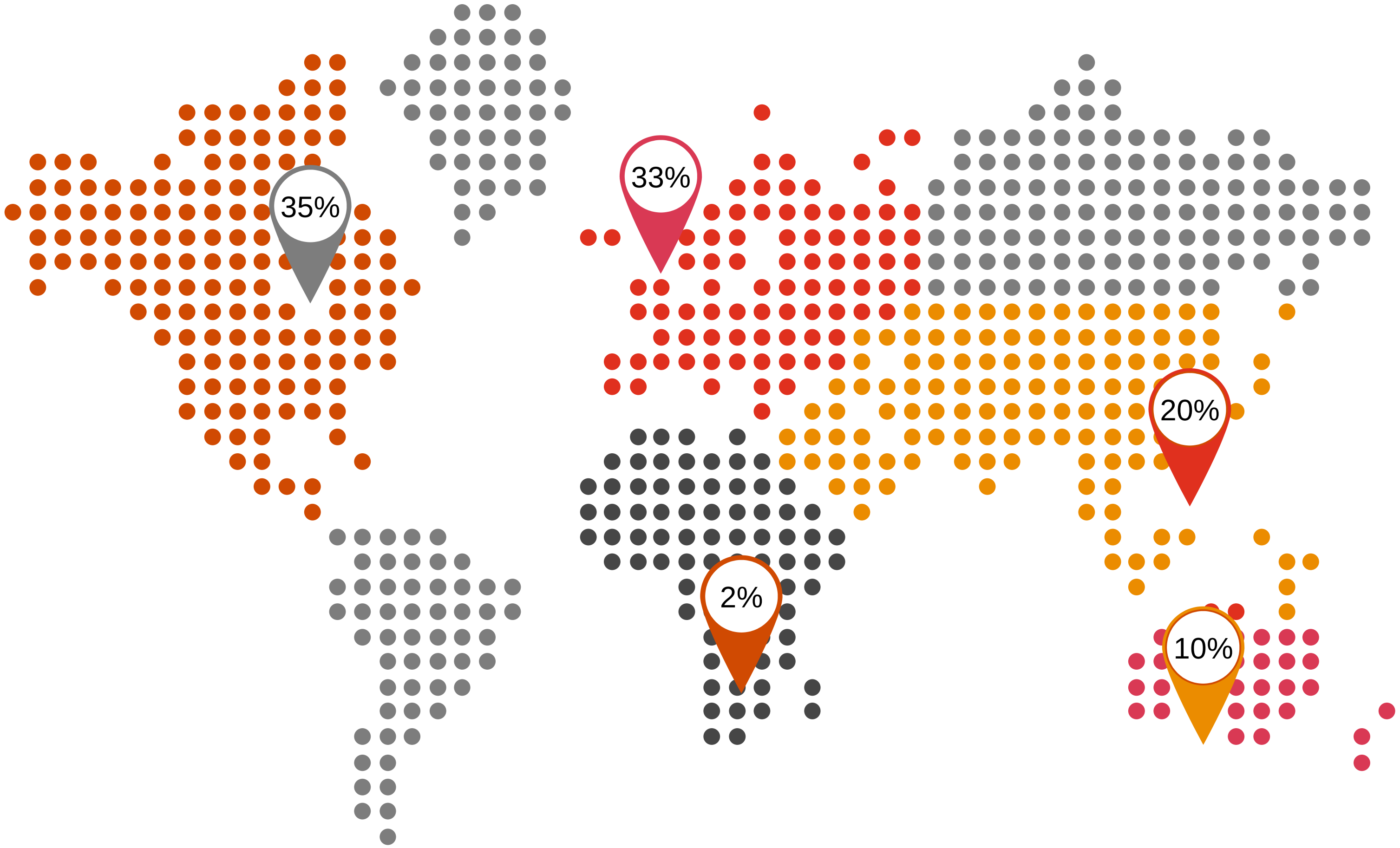
84% Financial services

Across all Lines of Defence:

52% 1st LOB

38% 2nd LOB

10% 3rd LOB



Difficulty aligning activities and defining roles and responsibilities across the 3LOD have given rise to challenges

Our respondents also indicated differing perspectives exist among 1st and 2nd line functions:

61%

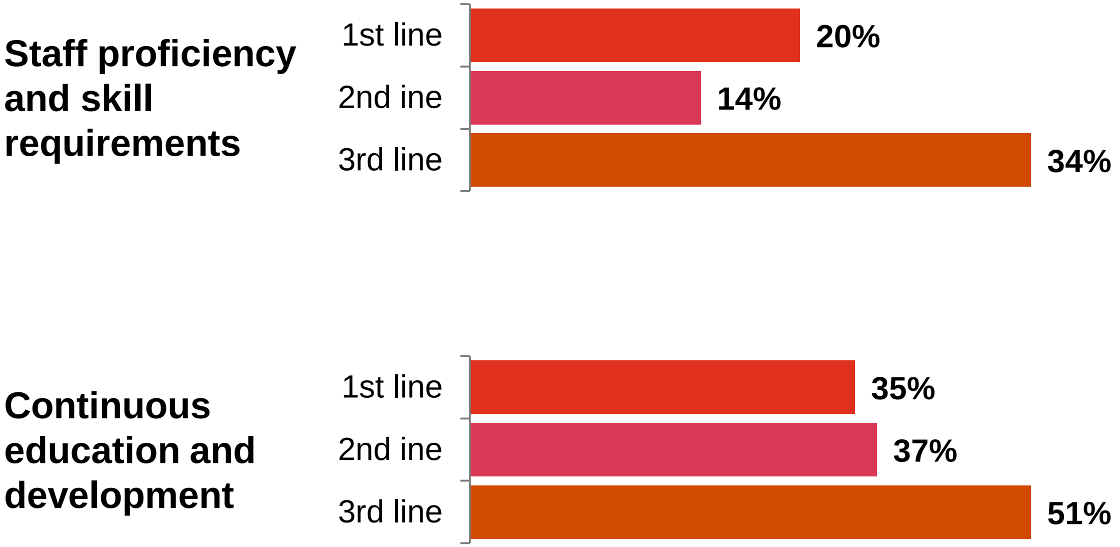
of 1st line TRM functions believe that Technology is very well aligned to the business strategy and objectives

yet

83%

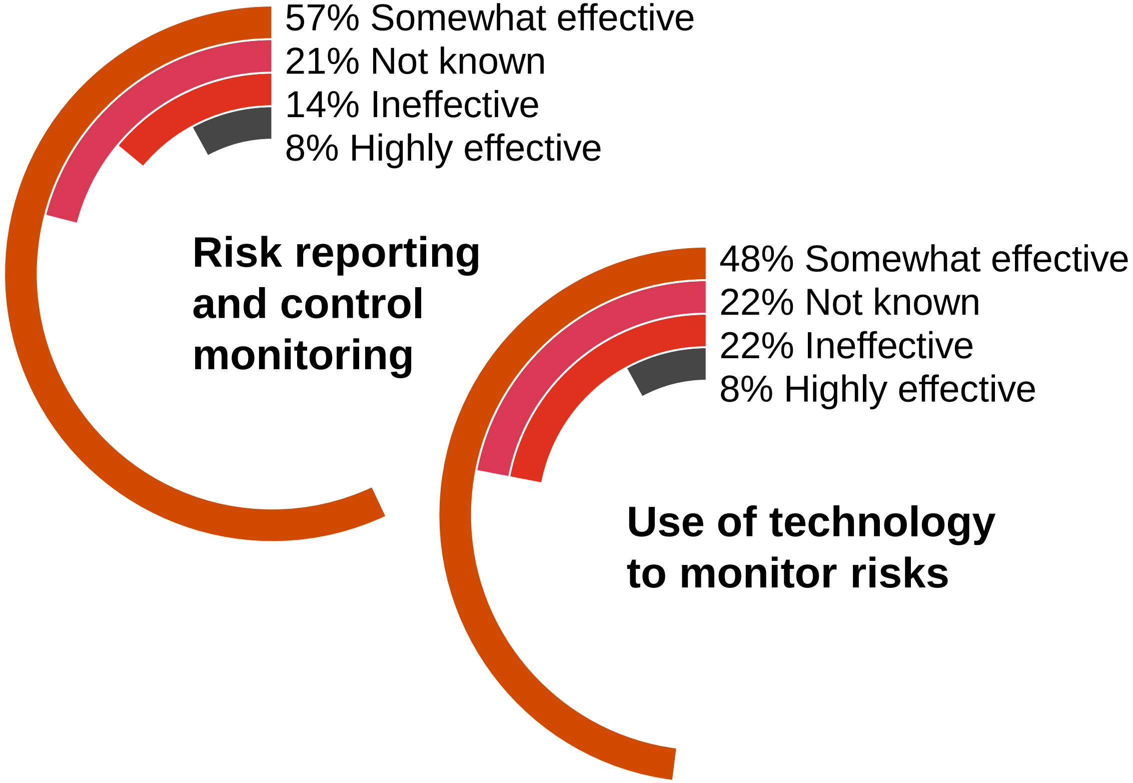
of 2nd line TRM functions believe that Technology is only slightly aligned to the business strategy and objectives

% of respondents across 3LOD who considered the following tasks were adequately covered in their function's framework:



Technology risk management functions are struggling to provide timely information to interested parties

We asked respondents how effective their organisation was at delivering the following activities:



74%

of Technology Risk functions believe that a ‘Live’ risk dashboard and plan, driven by organisational data would help them add value and focus on what matters most

but

13%

Have funding and plans in place to be able to build this capability

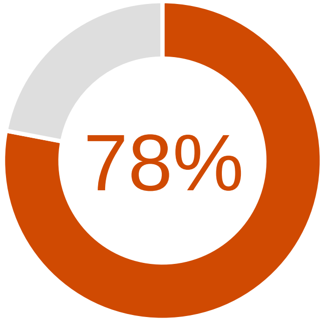
and

8%

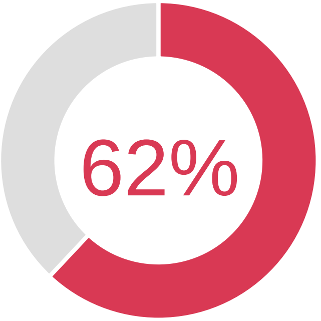
Feel that they have the data (availability and quality) to trust it

Functions should look to leverage automation and standardisation to improve timeliness and quality of information

Embracing data and using automation to standardise and streamline critical activities will be integral to the TRM function of the future's ability to proactively generate and action upon insights.



of Technology Risk functions are seeking ways to automate **risk management activities**



of Technology Risk functions say that technology teams are exploring ways to automate **processes and controls**

Top risks to successful automation

1	**Data quality** – The quality and integrity of data needed in automation is low or not as previously understood resulting in ineffective processes	78%
2	**Complexity** – The organisations technology, process and regulatory ecosystem is too complex and transformation is proving difficult to implement	67%
3	**Funding** – Unable to release funding to invest in automation and process improvement as competing priorities are emerging.	65%
4	**Culture** – The organisation has difficulty in implementing its decisions quickly and these projects may not be completed.	55%
5	**Skills and resources** – Skills are limited and in high demand across the organisation.	48%

Tech and cyber risk management function of the future

The function of the future

Case for Change

Build the business case to drive change

1

Vision

Establish a vision and value-add purpose

2

Data driven

Pragmatic measurement methodologies on a maturity journey to automation

3

Reporting

Enhanced reporting to focus on top and emerging risks

4

Alignment

Clear ownership across the three lines of defence

5

Capabilities

Develop the function around a professional framework

6

Companies are being driven to change the way they manage risk

Case for Change

Build the business case to drive change

1

How do I measure and **demonstrate the effectiveness** of our **cyber security investments** in relation to our key cyber risks?

How are our **cyber risks aligned** to our **strategic priorities** and enterprise risk appetite?

Am I able to respond to **regulatory** and other external stakeholder requirements?

How do I **communicate cyber risk to the Board** in a language they can understand?

Do I need **insurance**?

CISO

CRO / Compliance

CIO / COO

Data driven cyber risk management will increase efficiencies and better decisions

Data driven

Pragmatic measurement methodologies on a maturity journey to automation

3

Foundational

Data Driven

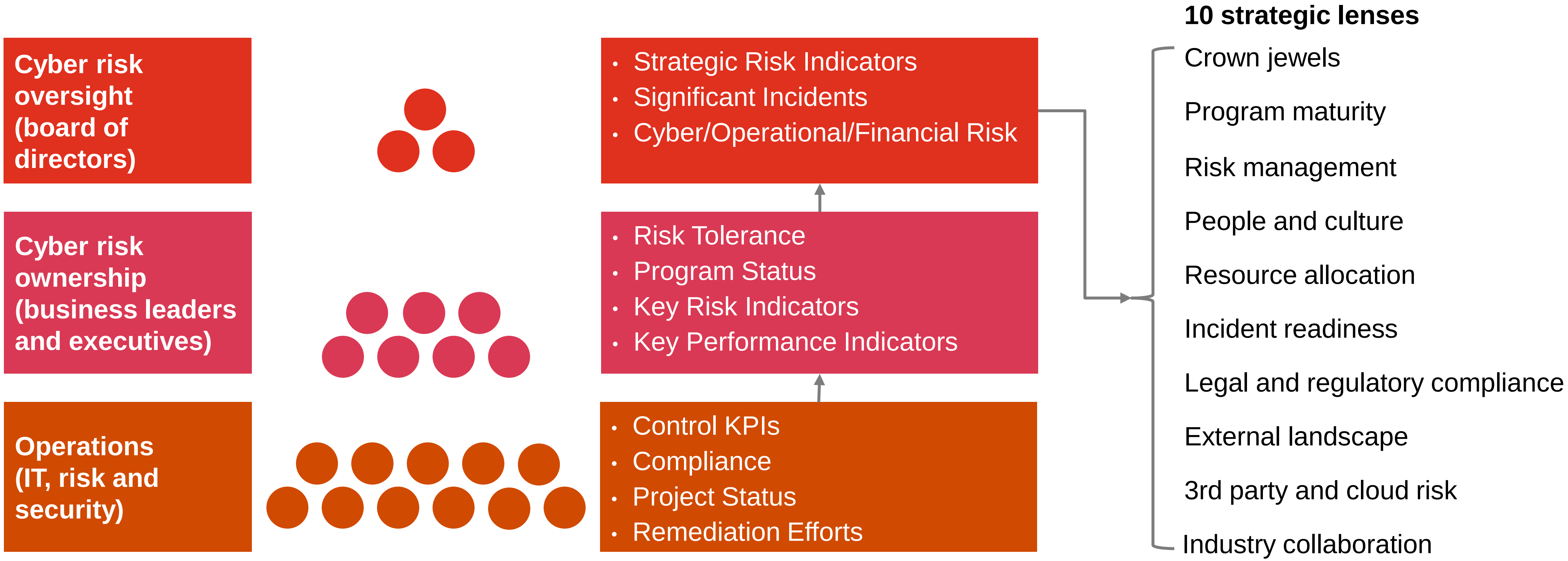
Strategy & Governance	- Security Focussed	- Drives business value through risk insights
People	- “Assessors” - predominantly compliance and assurance skill-set	- “Engineers” - People calibrated or re-tooled to risk reduction
Data & Reporting	- Inconsistent reliance on “expert” judgment - Reporting of operational metrics only	- Consistent, relevant and near real-time data - Audience specific reporting from Board to 1st line
Tools & Technology	- High use of spreadsheets and powerpoint - Limited use of visualization technologies	- Scalable automation to improve data quality - Dynamic and decision oriented risk dashboards

Three tiered strategic reporting

Reporting

Enhanced reporting to focus on top and emerging risks

4



Cyber risk oversight (board of directors)

- Strategic Risk Indicators
- Significant Incidents
- Cyber/Operational/Financial Risk

Cyber risk ownership (business leaders and executives)

- Risk Tolerance
- Program Status
- Key Risk Indicators
- Key Performance Indicators

Operations (IT, risk and security)

- Control KPIs
- Compliance
- Project Status
- Remediation Efforts

10 strategic lenses

Crown jewels

Program maturity

Risk management

People and culture

Resource allocation

Incident readiness

Legal and regulatory compliance

External landscape

3rd party and cloud risk

Industry collaboration

Thank you

pwc.com

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.