Guardians of trust

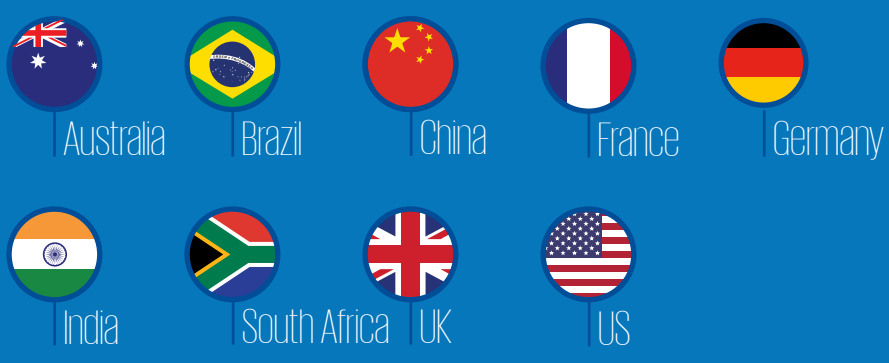
Who is responsible for trusted analytics in the digital age?

A trusted organisation has traditionally been anchored by the behaviours and decisions of trusted people. As people give way to machines, a trusted organisation (and a trusted platform) also requires trusted data and analytics.

KPMG International's *Guardians of trust* report looks closely at the intimate relationship between trust and digital transformation within an organisation — who is responsible for ensuring trusted analytics and what good governance can look like in a digital world.

The Study

Over 2,190 executives were surveyed across 9 countries representing 6 industries



Industries:

- **Banking/Financial Services**
- **Insurance**
- **Telecom**
- **Retail**
- **HC/LS**
- **Govt.**

Trust in analytics is lacking*

Only 35% of respondents say they have a high level of trust in their own organisation's use of different types of analytics

and 25% admit that they either have limited trust or active distrust.

Trust in an age of digital transformation*

Trust is becoming a defining factor of an organisation's success or failure. Underpinning a company's license to operate effectively, trust reduces uncertainty and builds resilience as well as:

influences reputation

drives customer satisfaction and loyalty

inspires employees

enables global markets to function

Executives and customers are wary of technology

Rapid, uncertain tech disruption can lead to unstable levels of internal and public confidence.

Trust in a digital world

The need for trust is expanding from trust in brands, organisations and their employees to also include trust in machines, algorithms and analytics.

The trust gap grows: C-suite executives question the trustworthiness of data, analytics and intelligent automation*

Few decision-makers trust the way their organisation uses different types of analytics. But the trust gap is not reducing with experience or time.

92% are worried about the impact on reputation

Understanding that trust in analytics is founded on four key anchors

Trusted analytics is not a vague concept or theory. At its core are rigorous strategies and processes that aim to maximise trust.

Levels of trust vary by geography*

The trust gap is not the same in every country and decision-makers may need to adjust their approach depending on the market they are in.

high levels of trust in India vs Australia

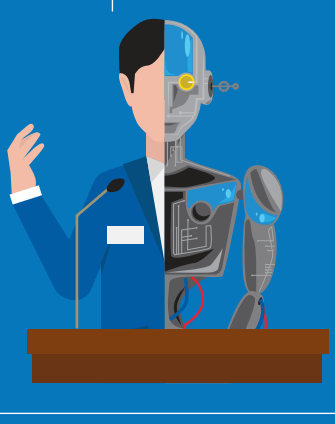
Spreading the blame*

Everyone should share some level of responsibility and accountability for faulty or untrustworthy analytics.

62% say that the blame for an autonomous vehicle accident lies with the organisation that developed the software.

Like human, like machine

The governance of machines should not be fundamentally different from the governance of humans.



Creating the foundation

There are eight areas that form the basis for emerging standards, enablers and controls for trusted analytics.

- **Governance**
- **Processes**
- **Regulation**
- **Data**
- **People & culture**
- **Technology**
- **Strategic alignment**
- **Alliances and supplier networks**

Who holds organisational responsibility?*

It is not clear who **within** the organisation has primary responsibility for ensuring the trustworthiness and accuracy of advanced analytics and models. A larger percentage says it rests with the technology function.

Key takeaways

If you can't measure it, you can't manage it	Prioritise risks	Create trust-impact personas
Create a buddy system	Stay legal	Checklist manifesto for data and analytics
Don't let the board off the hook	Be flexible with horses for courses	Create a mesh governance framework

* Source: A commissioned study conducted by Forrester Consulting on behalf of KPMG International, July 2017