



SNIA
Seminar Nasional Internal Audit

Diselenggarakan oleh:
YPIA 

Supported by:
 **BPJS**
Ketenagakerjaan
panggil kami **bpjamsostek**


mandiri

E MATERI

SEMINAR NASIONAL INTERNAL AUDIT 2021

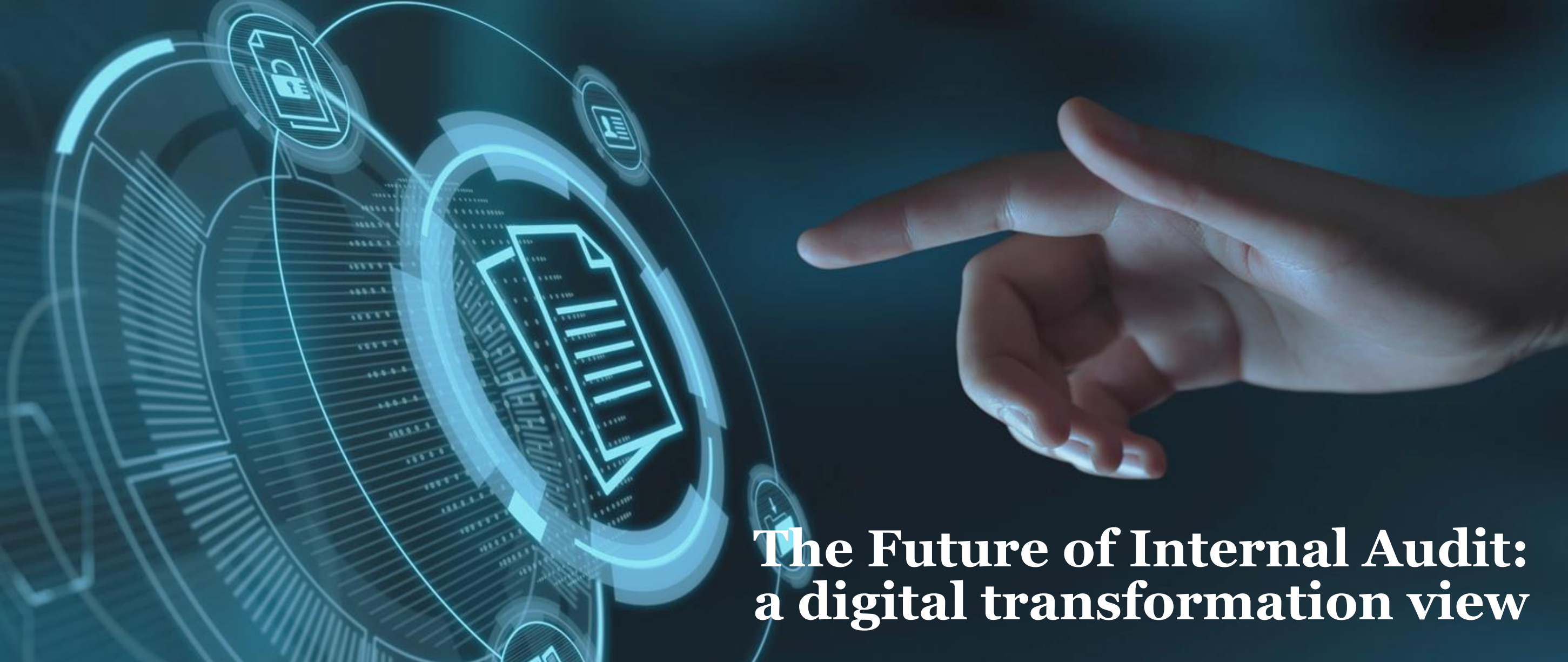
 Wolters Kluwer

 **insight**
CONSULTING

 **IA**
The Institute of
Internal Auditors
Indonesia

 **BANK BPD BALI**

 **SMi**
PT SARANA MULTI INFRASTRUKTUR (PERSERO)



The Future of Internal Audit: a digital transformation view

Presented by: Budi Santoso, SE, Ak, MForAccy, PGCS, CA, CFE, CPA (Aust.)
1 December 2021



BACKGROUND

Budi Santoso is Director in PWC's Forensic Services and Financial Crime Territory Leader, based in the Jakarta office. Budi has more than 17 years of experience in Indonesia and other countries in South East Asia conducting corruption/fraud and money laundering investigations, asset tracing, litigation support, designing, implementing and evaluating anti-fraud programs (both prevention and detection), fraud risk assessment, internal control assessment and improvement, compliance due diligence, US FCPA & UK ABAC reviews, business process reviews, good corporate governance reviews and business intelligence. An experienced trainer, he is also capable in leading internal audit, compliance, and antifraud and investigation unit transformation.

RELEVANT EXPERIENCE

- 10 years : worked for the elite Indonesian Corruption Eradication Commission (KPK), serving as Head of the Commissioner's Office, Head of the Prevention Secretariat, and also as an investigator/examiner (2005-2015)
- 2 years : Senior Manager in the Fraud Investigation and Disputes team at Ernst & Young (EY) Indonesia (2016-2018)
- 2.5 years : Senior Director for Kroll in the Singapore office (2018-2020)

PROFESSIONAL ASSOCIATION

- 3.5 years : Director of Training for the Association of Certified Fraud Examiner (ACFE) Indonesia Chapter and
- 2 years : Board Member ACFE Singapore Chapter.

EDUCATION AND PROFESSIONAL CERTIFICATION

- Bachelor of Economics in Accounting from Sebelas Maret University (Solo) – 2004
- Official education at Indonesia Police Academy (Akpil-Semarang) - 2006
- Master of Forensic Accounting from University of Wollongong (Australia) - 2009
- Postgraduate Certificate in Corruption Studies, University of Hong Kong (China) – 2012
- Integrity system short course, Malaysia Anti-Corruption Academy (Malaysia) - 2013
- Governance & anticorruption short course from International Law Institute, Georgetown University (USA) - 2015
- Certified Fraud Examiner (CFE)
- Chartered Accountant (CA)
- Certified Practicing Accountant (CPA Aust.)

Agenda

- 1 The Challenges
- 2 GRC Overview
- 3 Roles of Internal Audit
- 4 Digitally fit function; impact of technology innovation
- 5 Why do we need Internal Audit Transformation?
- 6 Transforming the Value Proposition of Internal Audit
- 7 Expected outcome of Internal Audit Transformation
- 8 Anti-fraud Management

[Contents](#)





1 The Challenges

Evolving Priorities

Global Risk Study

Contents

Which IA topic is top of mind for your management team?
Choose one answer.

Which IA topic is top of mind for your audit committee?
Choose one answer.

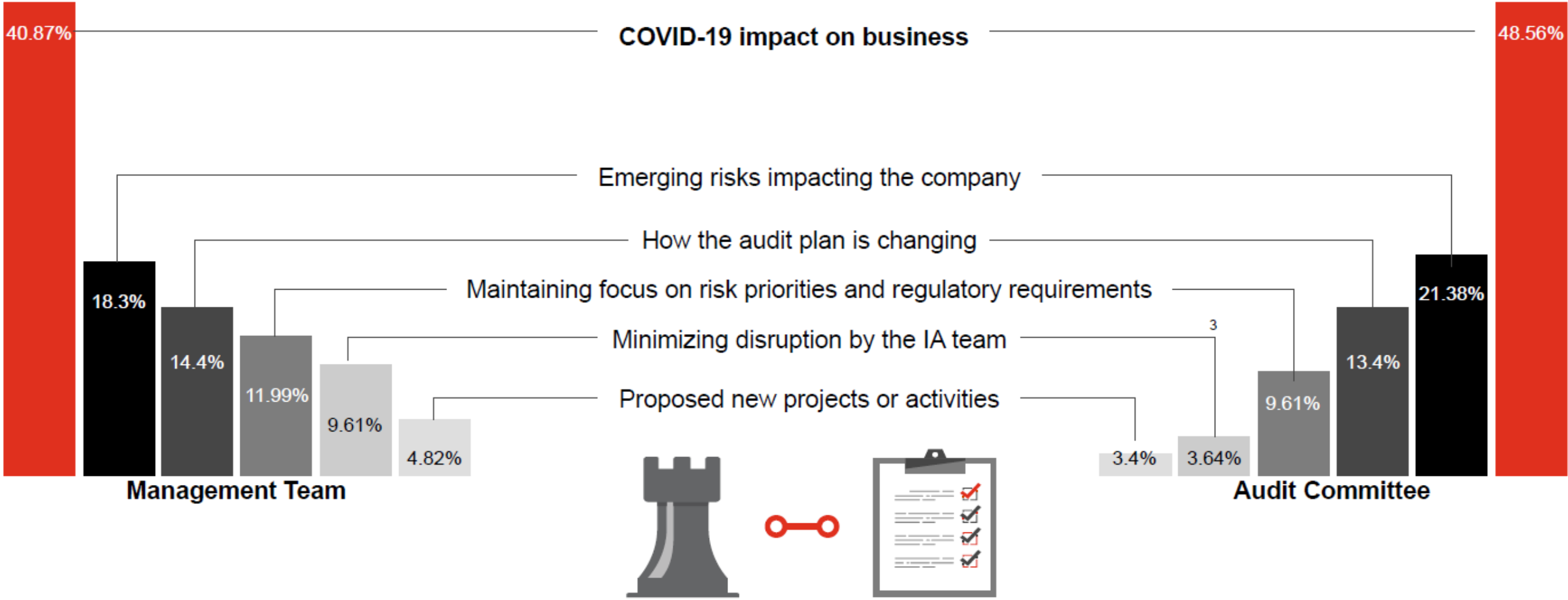














Exhibit 1: COVID-19’s impact on non-financial services industries

Impact	Industry sectors	Comments (exemplary)
Positive	 Digital platforms	Increased consumption due to pandemic (e.g., of masks) and increased use of digital platforms and digitisation efforts across industries
Neutral	 Consumer goods & retail (food)  Telecommunications	Stable B2C consumption as more consumers work from home and travel is limited
Slightly negative	 Agriculture  Healthcare  Utilities  Pharma & life sciences  Technology & software	Overall reduction in economic activity and GDP drives less consumption . Workforce availability and/or productivity are at risk
Negative	 Chemicals  Industrial manufacturing  Freight transportation	Production stopped or output reduced throughout lockdown, uneven recovery
Very negative	 Services  Consumer goods & retail (non-food)  Automotive  Entertainment & media  Passenger transportation, travel, hospitality	Point-of-sale closure and order cancellations through lockdown, time frame and strength of recovery unclear

Source: PwC

Findings at a glance (continued)

Risk function collaboration is increasingly imperative

- As businesses become more connected, risks become more connected and complex.
- Studying business risks only in silos can lead to a singular view of risks and a lack of visibility to risk inter-relationships.
- It is more critical than ever for risk functions across the organization to closely collaborate.
- Failure to do so creates blind spots to risk, while close collaboration produces significant gains.

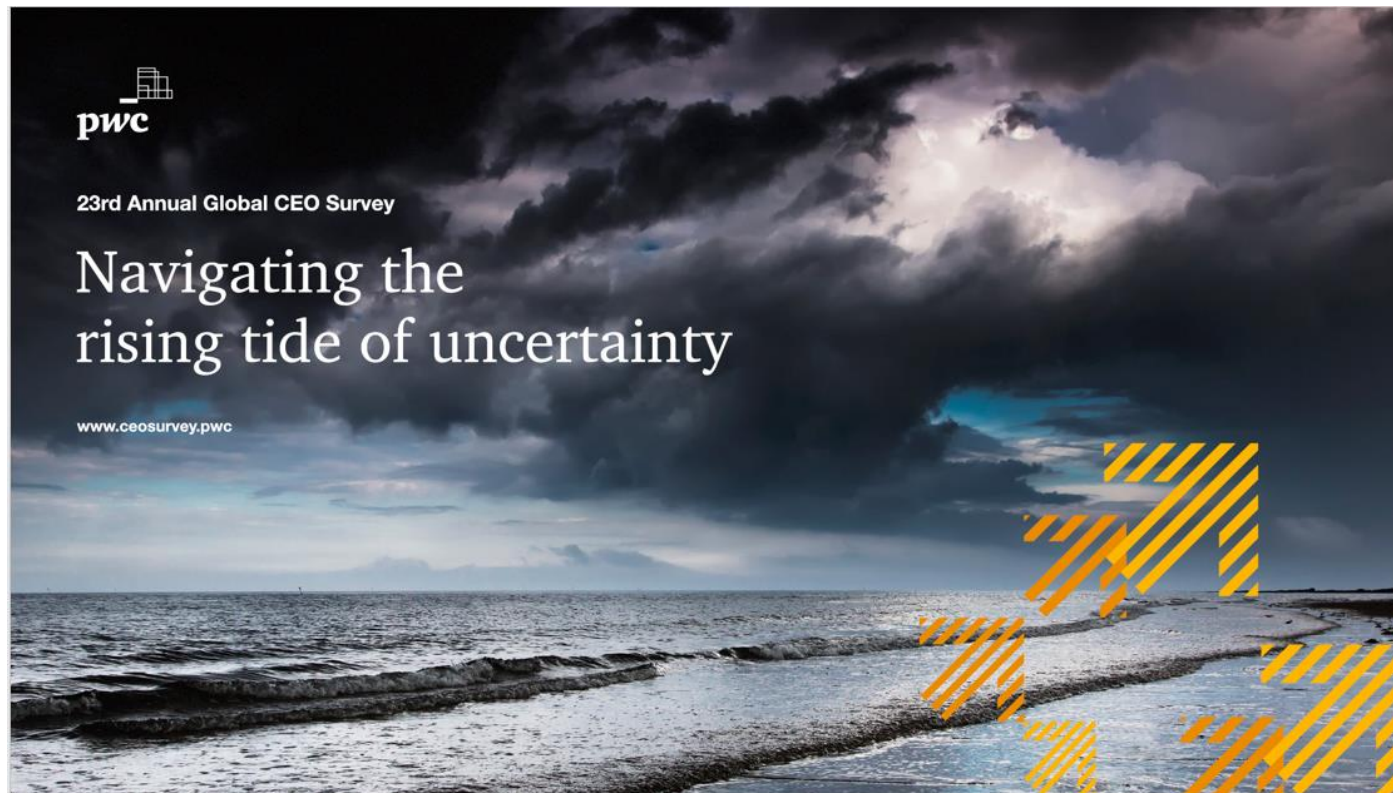
Where are your risk functions on their collaboration journey?



Our 2020 PwC Global CEO Survey revealed a record level of pessimism

[Contents](#)

More than half of the CEOs we surveyed believe the rate of global GDP growth will decline. This caution has translated into CEOs' low confidence in their own organisation's outlook.



Four key themes emerged from our survey

1. Growth

Uncertainty undermines outlook

2. Technology regulation

Setting up guard rails in cyberspace

3. Upskilling

To upskill or not to upskill is no longer the question

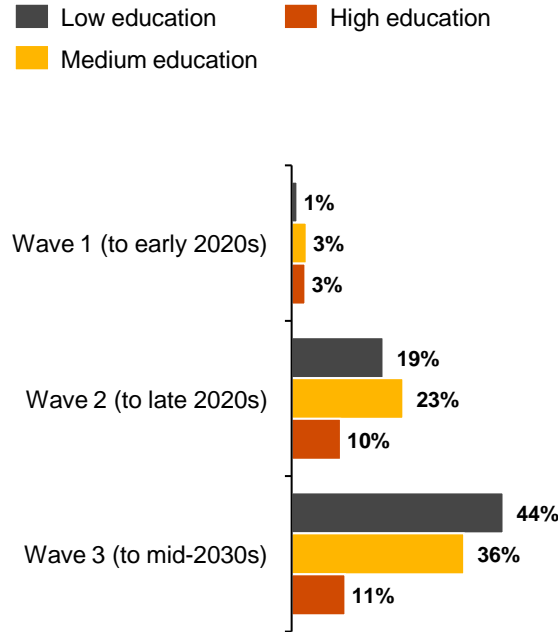
4. Climate change

An opportunity cloaked in crisis

Four key forces are driving the upskilling imperative

1. Increasing job automation

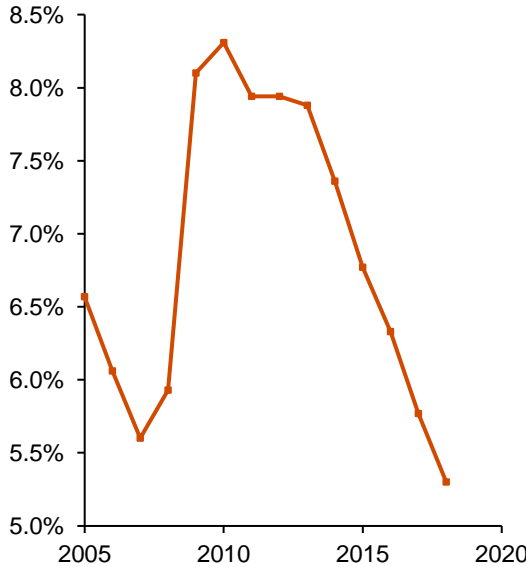
1. Percentage of existing jobs at potential risk of automation by education level across waves



Source: PwC, *Will robots really steal our jobs? An international analysis of the potential long term-impact of automation*

2. Decreasing talent availability

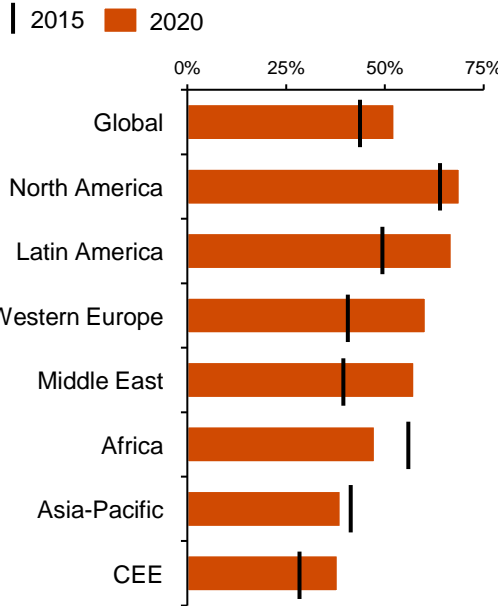
OECD unemployment rate (% of total labour force)



Source: OECD

3. Decreasing mobility of skilled labour

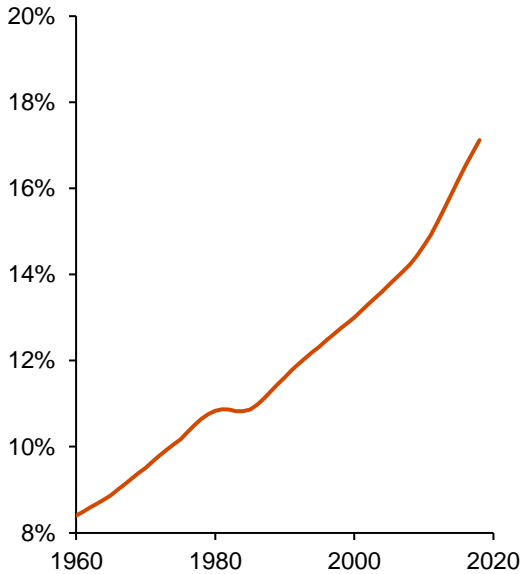
Is cooperation among gov'ts and businesses leading to greater movement of skilled labour between markets? (showing only 'no')



Source: PwC, 23rd Annual Global CEO Survey
Base: Global respondents (2020=1,581; 2015=1,322)

4. Ageing talent

OECD population ages 65 and above (% of total population)



Source: World Bank Group

Financial Crime Convergence

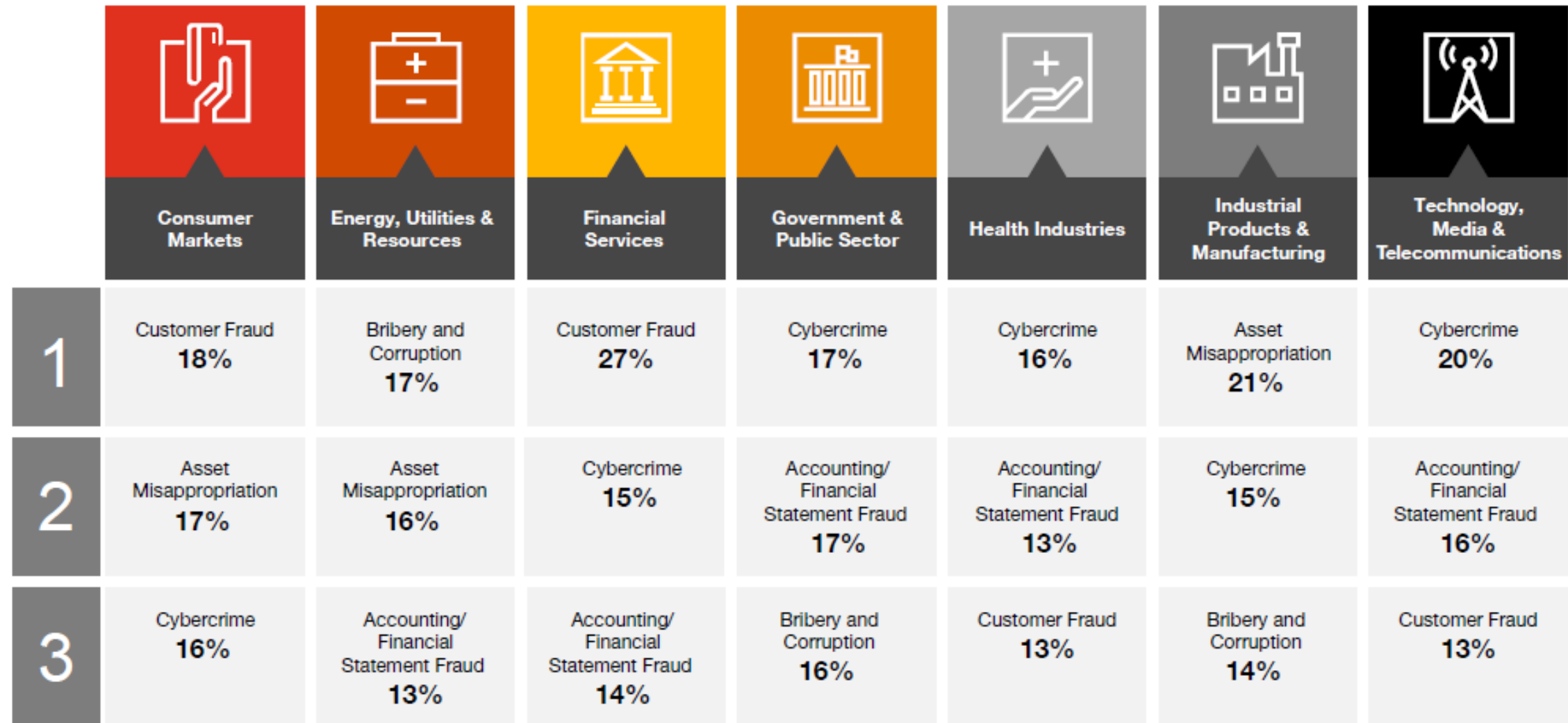
Fraud, cyber, Anti- Money Laundering, and Anti-Bribery & Corruption are the major components of financial crimes, and present organizations with a number of intersecting and overlapping risks that must be mitigated.

- Fraud, Money Laundering, Cybercrime, and Bribery & Corruption exist on **a single continuum of Financial Crime** – one leads to the other; further, criminals are increasingly exploiting opportunities across these pillars
- Accordingly, regulators are increasingly focused on looking at the continuum of financial crimes and **regulatory expectation** is that institutions to **connect the dots among these areas**
- In many cases, fraud, cyber, AML and ABAC programs have **common elements and controls**, such as risk assessment, threat intelligence, due diligence, prevention, detection, and response.
- As a result, there are opportunities to **reduce risk, improve compliance** and **reduce cost** by **converging** these programs.
- Institutions approach to **financial crimes convergence** may vary based on culture, risk appetite and current maturity of existing programs. Although challenging, legacy barriers to convergence can be overcome.



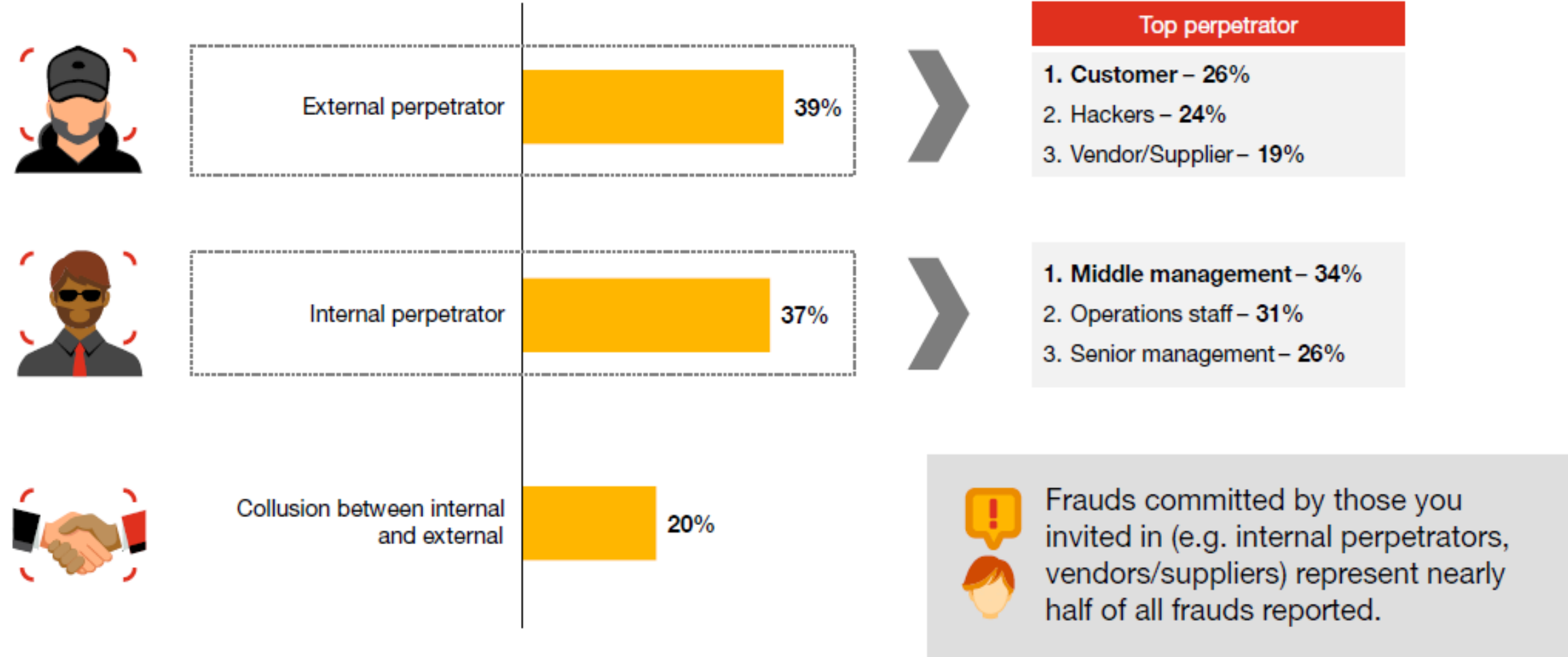
Top 3 frauds in Various Industries

PwC 2020 Global Economic Crime and Fraud Survey



Fraud hits companies from all angles – the perpetrator could be internal, external, or in many instances there will have been collusion

PwC 2020 Global Economic Crime and Fraud Survey



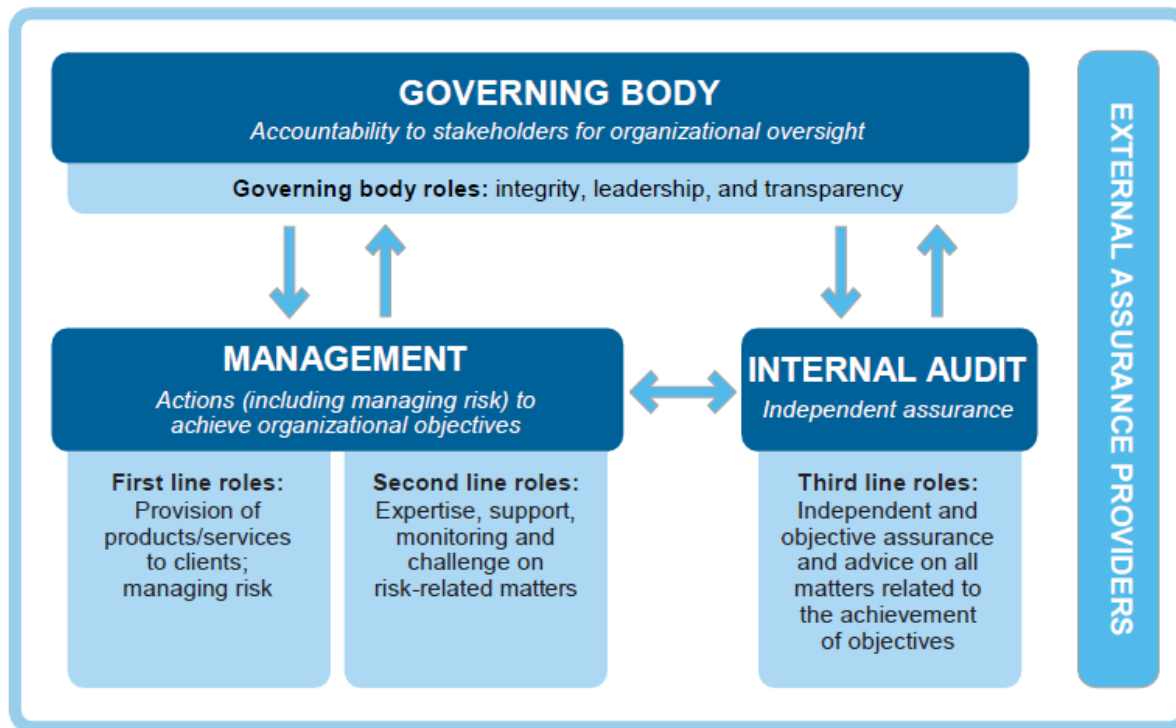


2

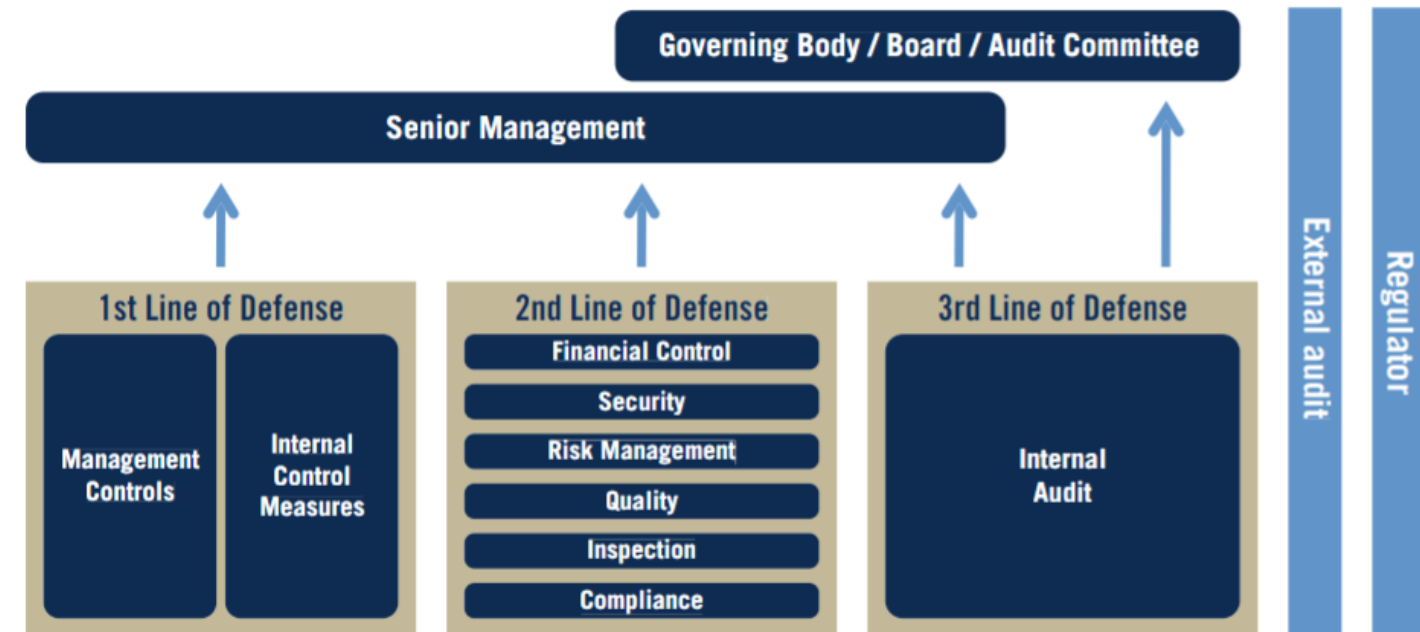
GRC Overview

The three lines

The IIA's Three Lines Model



The Three Lines of Defense Model

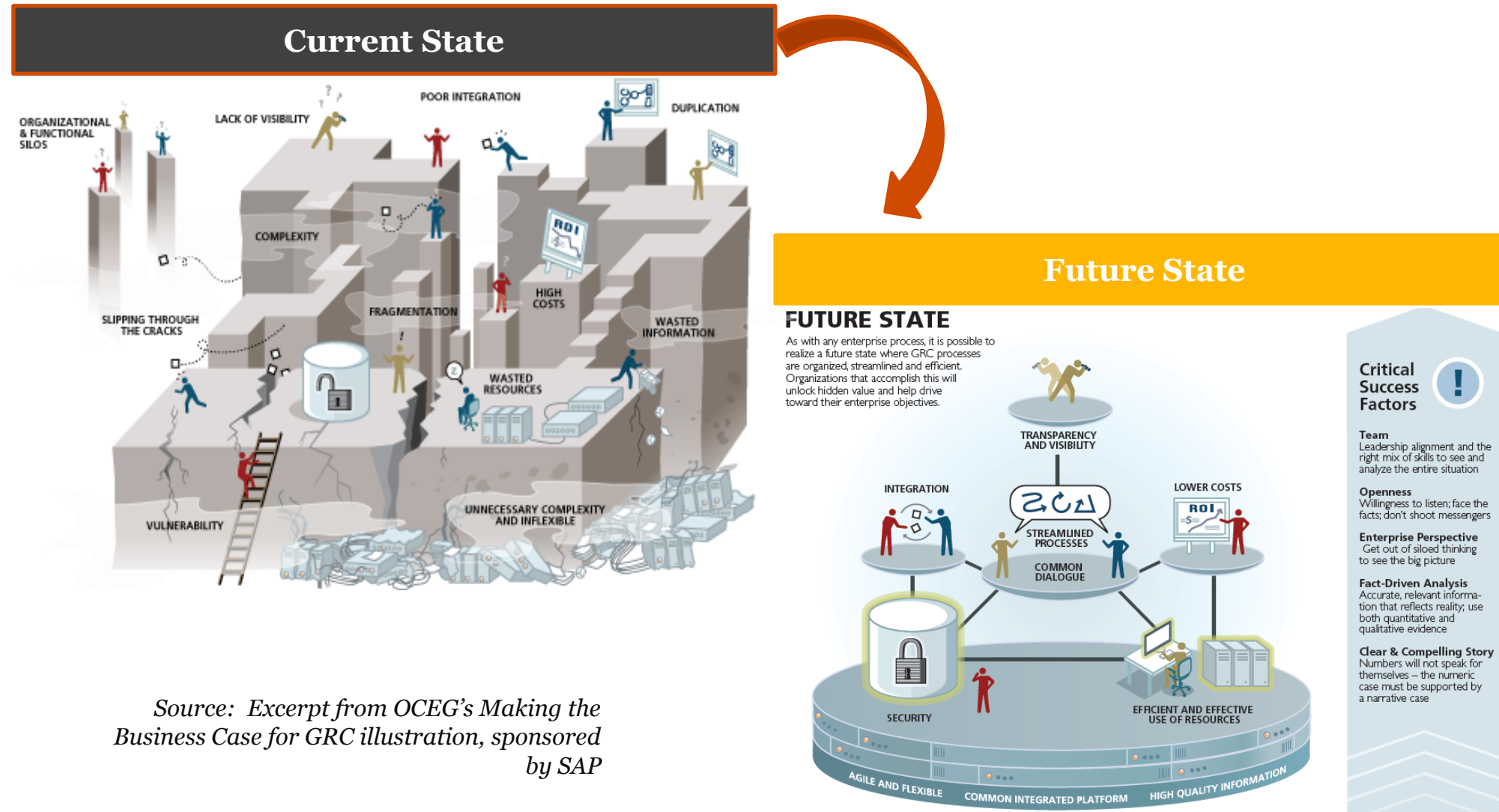


Adapted from ECIIA/FERMA *Guidance on the 8th EU Company Law Directive, article 41*

KEY: ↑ Accountability, reporting ↓ Delegation, direction, resources, oversight ↔ Alignment, communication coordination, collaboration

An integrated, structure risk management perspective

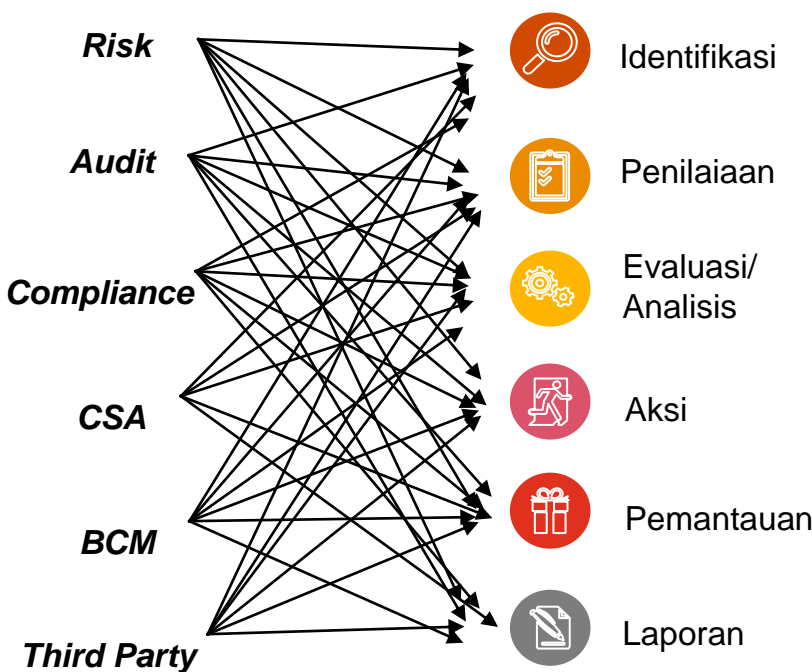
What goods look like



Source: Excerpt from OCEG's Making the Business Case for GRC illustration, sponsored by SAP

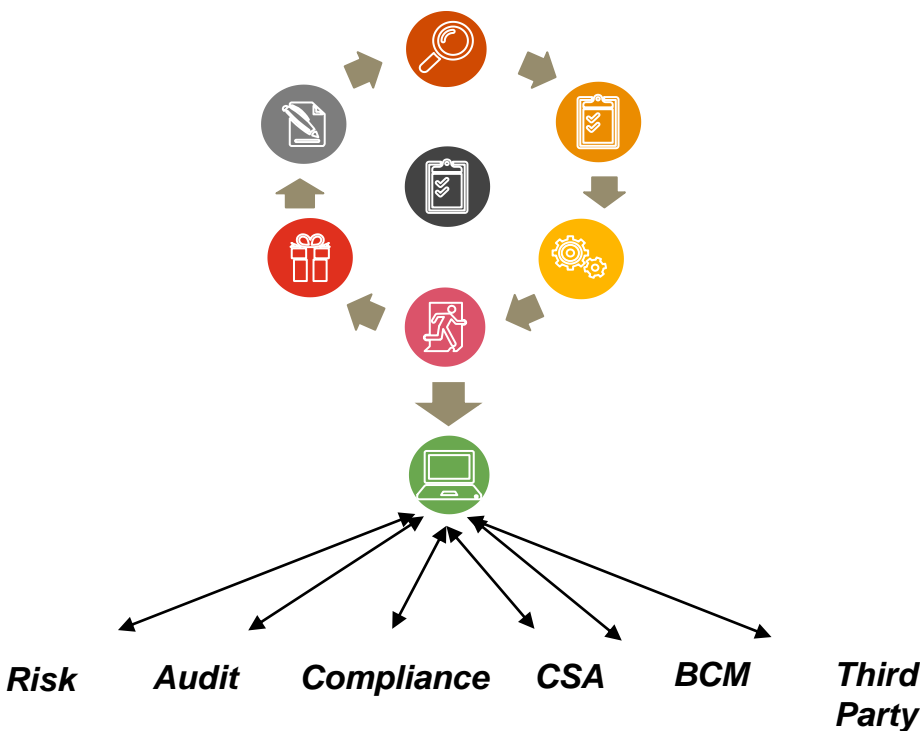
IRM yang mendukung transformasi proses bisnis

Current state



Perform many - use once

Future state



Perform once - use many

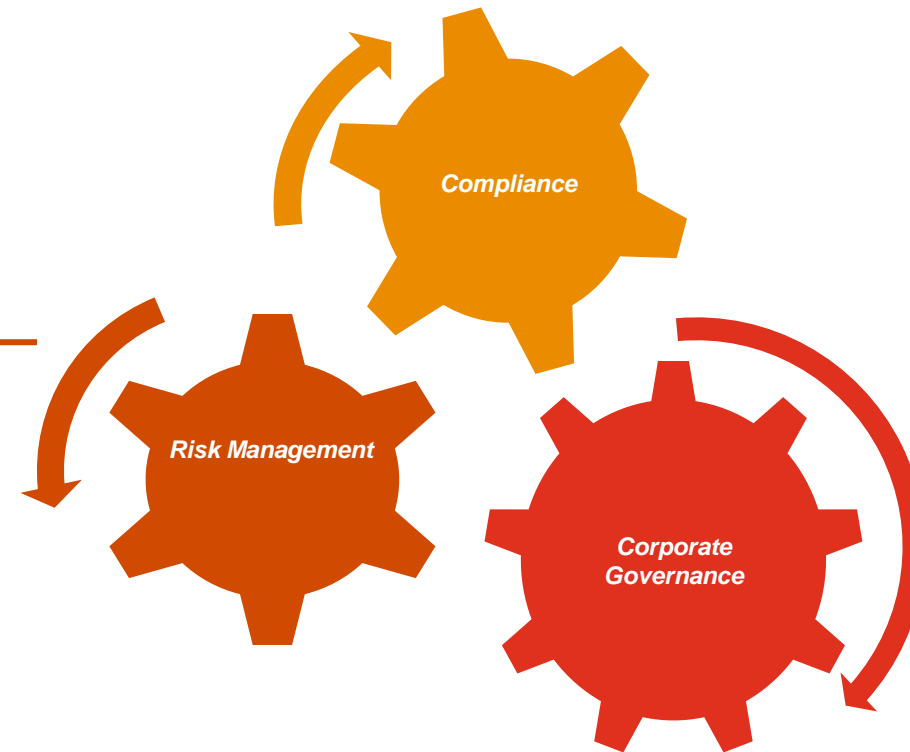
Penggunaan teknologi pada *integrated risk managed (IRM)*?

IRM adalah upaya yang terkoordinasi untuk memastikan komunikasi dan kolaborasi antar *stakeholder* dalam manajemen risiko dan kontrol pada organisasi.

Manajemen Risiko (*Risk Management*)

Kemampuan untuk secara proaktif mengidentifikasi, mengukur, memprioritaskan, dan mengelola risiko dari strategi perusahaan dan objektif bisnis.

Fungsi: Dokumentasi Proses dan Risiko, Penilaian Risiko, Analisis Risiko, Pemantauan Risiko, Agregasi, ERM *Dashboard*.



Kepatuhan (*Compliance*)

Kemampuan untuk mengelola kepatuhan dengan biaya yang lebih rendah melalui proses yang efisien agar dapat dilakukan secara berulang dan berkelanjutan.

Fungsi: Dokumentasi Proses dan Kontrol, Manajemen Kontrol, Penilaian Efektivitas Kontrol, Pengungkapan dan Sertifikasi, *Loss & Incident Management*.

Tata Kelola Perusahaan (*Corporate Governance*)

Kemampuan untuk mendefinisikan dan mengkomunikasikan strategi perusahaan, target/objektif dari kebijakan, evaluasi performa bisnis melalui pelaporan, *scorecards*, dan *dashboard* secara *real-time*.

Fungsi: Manajemen Kebijakan dan Prosedur, Audit Internal, *Board and Entity Management*, Pelaporan.

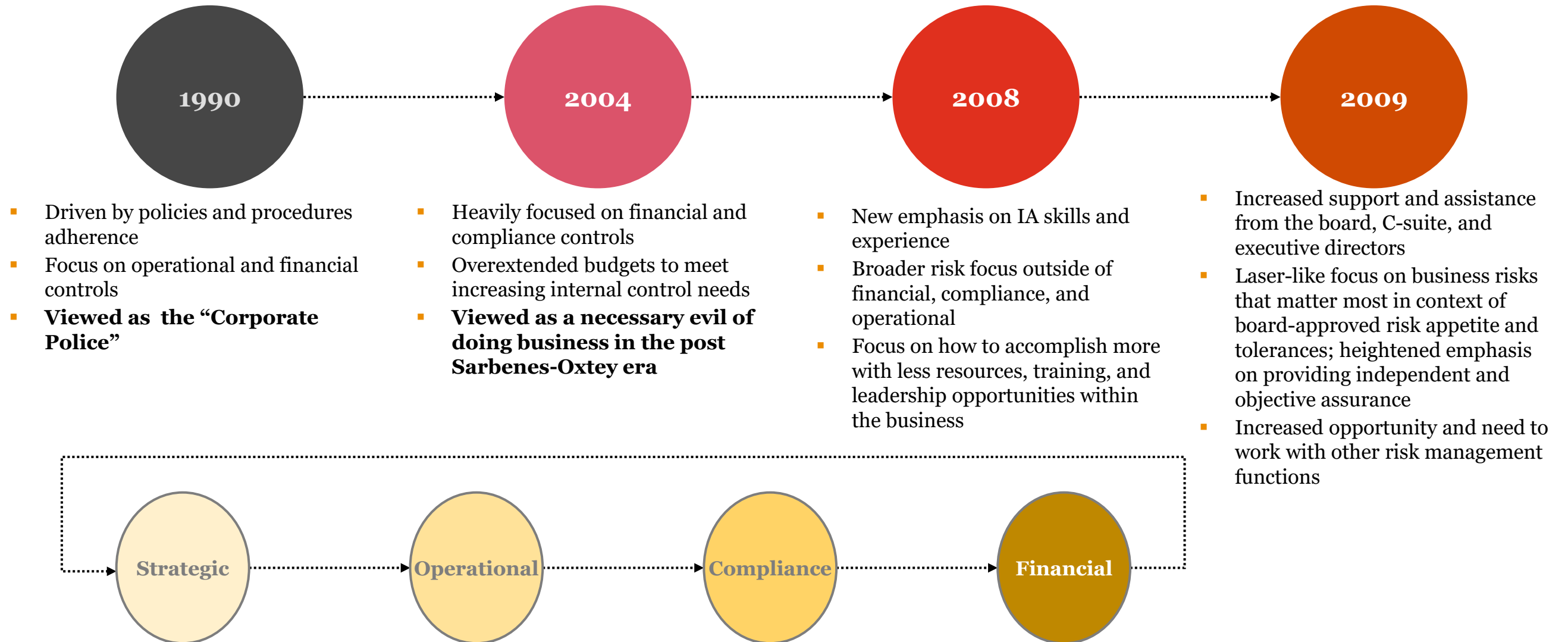
Pemberdayaan teknologi Governance, Risk & Compliance (GRC) terdiri dari sekumpulan solusi risiko dan kepatuhan yang saling **terintegrasi** untuk mengasimilasikan **informasi yang bermakna** terkait risiko dan kontrol. Hal tersebut membantu perusahaan untuk secara lebih **proaktif** mengelola risiko dan usaha serta program kepatuhan dengan lebih **efektif** dan **efisien**.



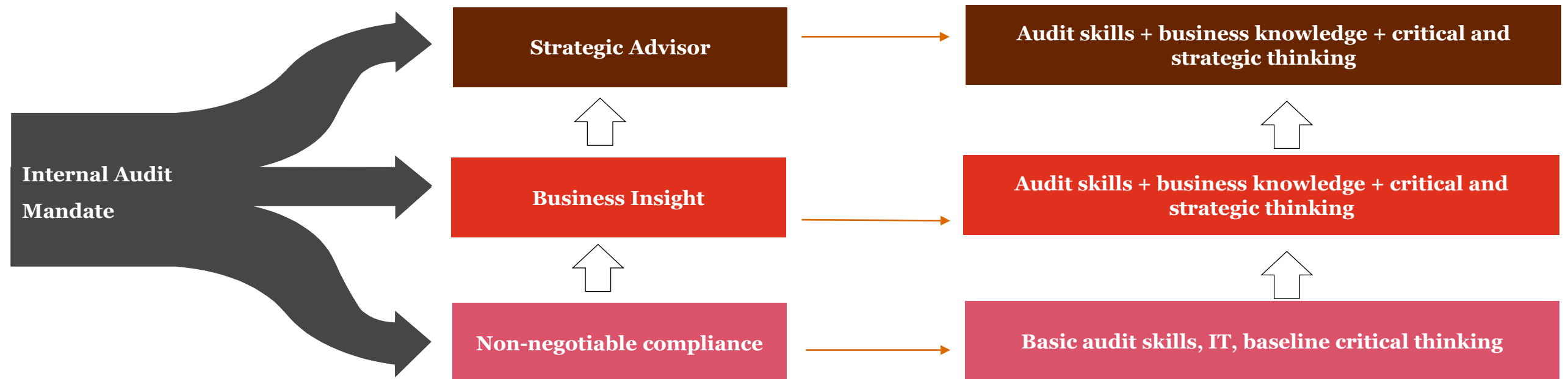
3

Roles of Internal Audit

Internal Audit Historical Trends

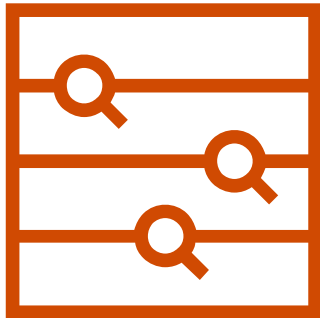


Internal Audit Mandate



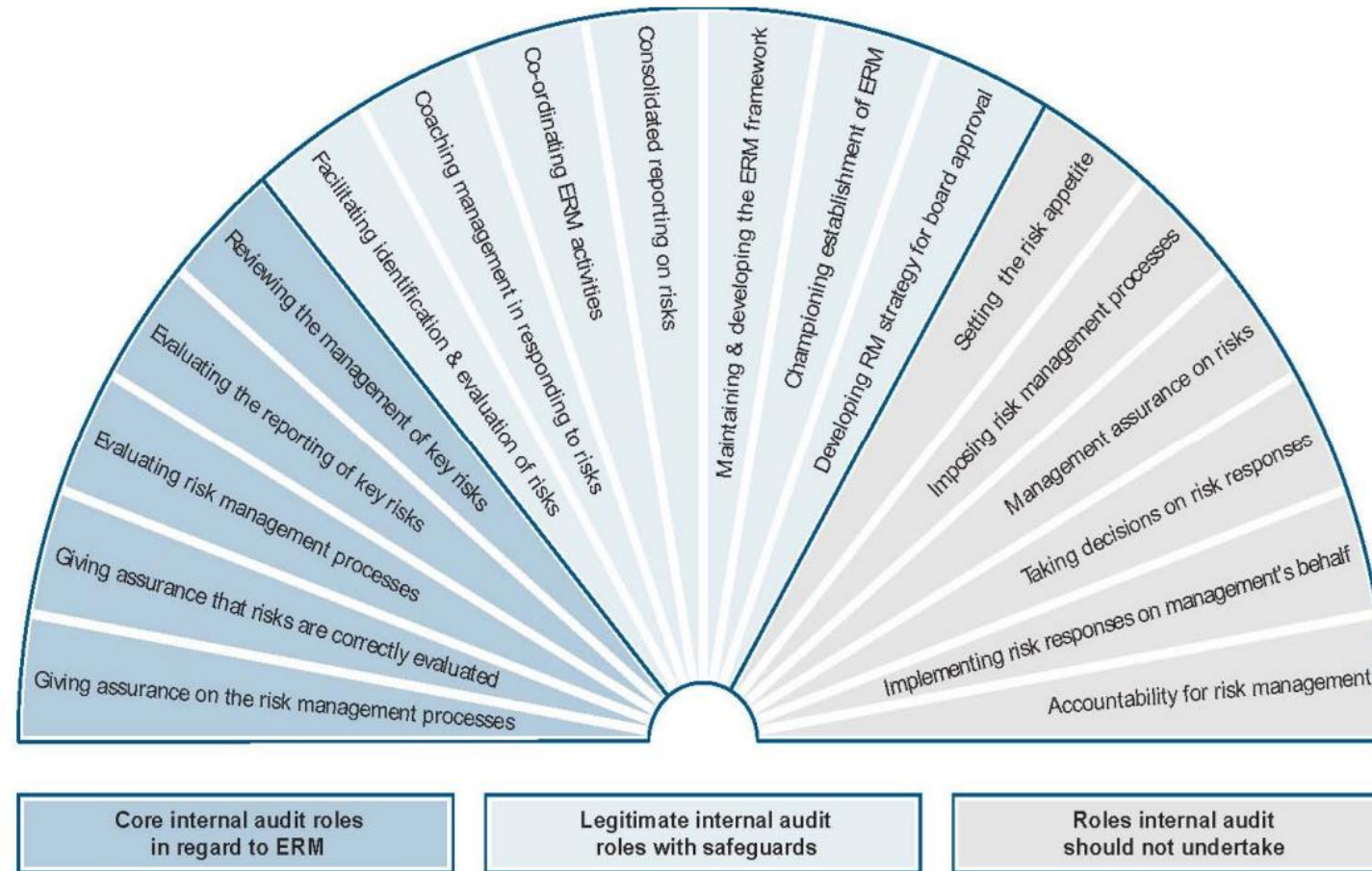
Internal Auditor Vs RCO

Perbandingan Peran IA dengan RCO



Investigative

- Interviewing
- Post-event checking
- Finding accountabilities
- Suspicious



Sumber: The Institute of Internal Auditors

Transformasi Mindset



Consultative

- Discussing
- Pre-event mitigating
- Finding solutions
- Curious
- Anticipative

Staying relevant with business goals and challenges (1/3)

The internal audit function needs to understand the future risks and issues facing the business



Several strategic objectives and risks agenda are described below for illustration: illustrated below:

- *Effectively managing and delivering the quantum of strategic, business and operational change across the organisation.*
- *Enhancing systems and IT to eliminate reliance on manual processes, facilitate effective integration and provide a scalable platform for future growth.*
- *Developing digital capability and presence.*
- *Managing the regulatory landscape and compliance*
- *Improving customer experience and refreshing distribution channels, including branches, stores*

It is important these are appropriately reflected and prioritised, as part of the planned Internal Audit activity

Staying relevant with business goals and challenges (2/3)

This is Internal Audit's moment

The business environment has changed and continues and continues to change affecting every organisation, in every market, to one degree or another. As the risk landscape expands and with it the complexity of doing the business, challenges and opportunities are being created. It is essential for organisations to be ready to respond, but it's by no means easy. Boards and senior management are being placed under unprecedented pressure to stay on top of current and emerging risks – for which they require increasingly specialised assurance. Internal Audit has emerged as a key means of giving boards the confidence to deal with demands of a dynamic market place.

Stakeholders expect Internal Audit to 'look deeper and see further', acting as a lever for change supporting an organisation's strategic agenda. The time has come for Internal Audit to be bold, courageous and innovative in order to capitalise on a growing need to provide strategic insight. Understanding this may be a daunting prospect, especially if new skills are required, but it's a challenge worth taking on. The increased comfort gained by the organisation and its wider stakeholder group will likely mean more freedom for Internal Audit to operate in a way it should and will result in greater value for money.



Championing the function

The internal audit function should recognise the responsibility to support the value of the internal audit as it evolves and transitions to meet the demands of modern business.

The internal audit should aim to play a key role in strengthening the profile, credentials and value of Internal Auditors everywhere and in doing so, help organisations meet the demands of their dynamic marketplace and an expanding risk landscape.

Boards – should expect more support and value from Internal Audit. This may include a greater role in supporting the strategic agenda.

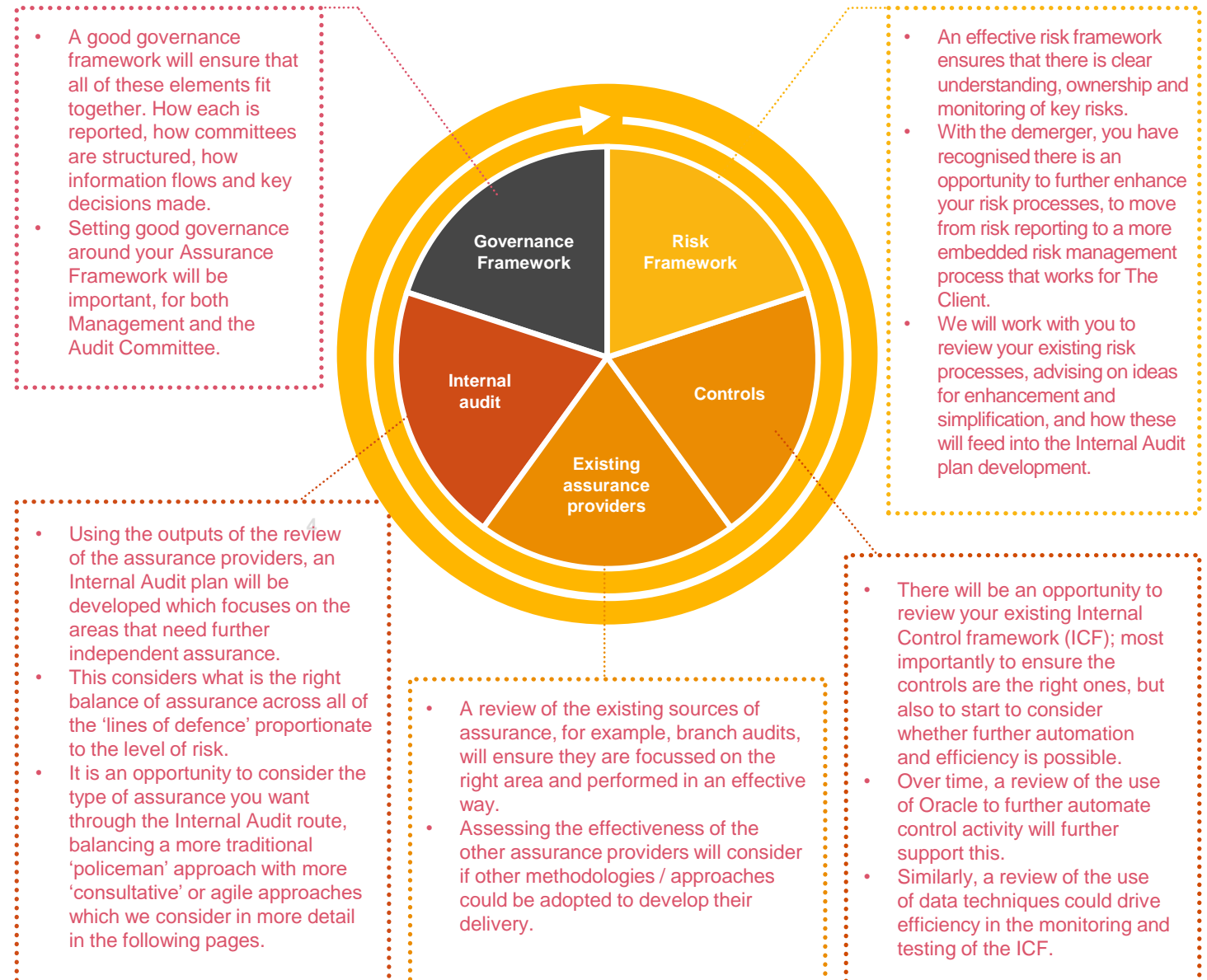
Management – should expect more agility and insight from Internal Audit. This might include assisting the business and in establishing root cause and driving positive change, leveraging its unique insight across the whole organisation.

Heads of Internal Audit – should expect greater support and investment in their Internal Audit functions. Heads of Internal Audit should also expect to be consulted on the design and implementation of new initiatives – drawing on business acumen and networks beyond the organisation.

Staying relevant with business goals and challenges (3/3)

One of the role of Internal Audit is providing assurance.

An effective Assurance Framework (refer to the diagram in the right) will ensure that all assurance activity is aligned to the key risk and controls areas, ensuring **no duplication of assurance activity** and as importantly no gaps in assurance. The key is to keep this **simple but effective**.



What good Internal Audit Looks like?

Red flagging

Telling the business something that they should be worried about and should act upon.

Horizon scanning

Predicting future areas of risk, concern and non-compliance.

Business focus

Ensuring Internal Audit's activities are focussed on areas that are most important to the business.

Insights and benchmarking

Telling the business something that they did not already know, and could not find out without Internal Audit involvement.

Business improvement

Ensuring that recommendations are practical, deliver value to the business and challenge the status quo.

Key:

- | | | | |
|-------------------|--------------------------|----------------|--------------------------|
| 1 Service culture | 3 Business focus | 5 Risk focus | 7 Stakeholder Management |
| 2 Technology | 4 Quality and innovation | 6 Talent model | 8 Cost effectiveness |

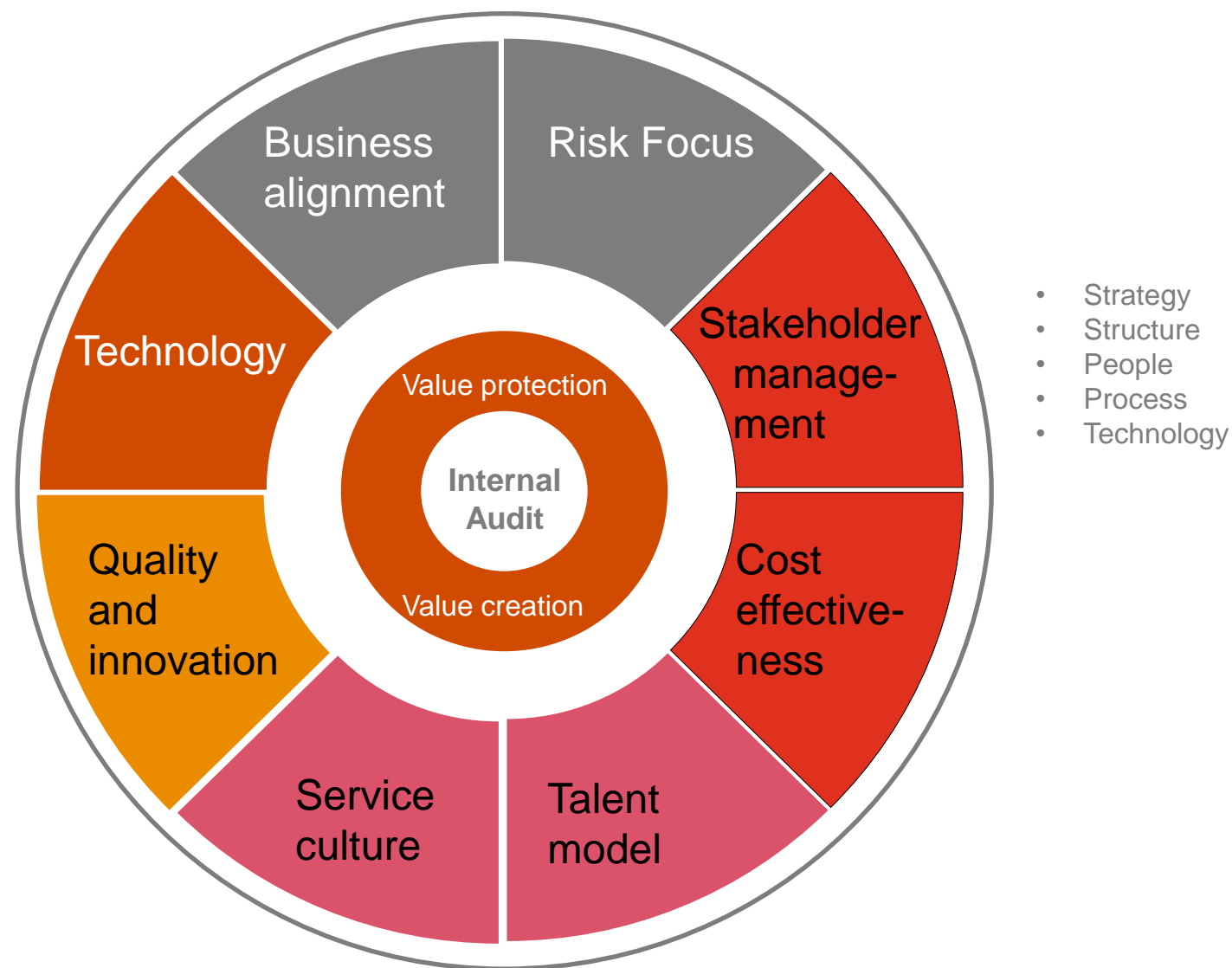


The diagram sets out the key features of what we know 'good' Internal Audit looks like, linking the 'Eight Attributes of an Effective Internal Audit function' (inner circle), with the value that Internal Audit brings to an organisation articulated around the outside.

We have a proven track record of delivering Internal Audit within this Eight Attributes model and strongly believe that this will raise the profile and create a brand for Internal Audit at The Client. For example:

- 'Business Focus' means we will align the Internal Audit effort on what matters to the business and its strategy. This means that as well as addressing risk, our recommendations will be tailored and practical, focussing on supporting the appropriate change in the business.
- 'Cost effectiveness' means that for every audit we will start by challenging the approach to find the most efficient and agile way of delivering work, getting the most out of our specialists, and bring measurable value to the business.

What we have learned - Eight key attributes across the five elements



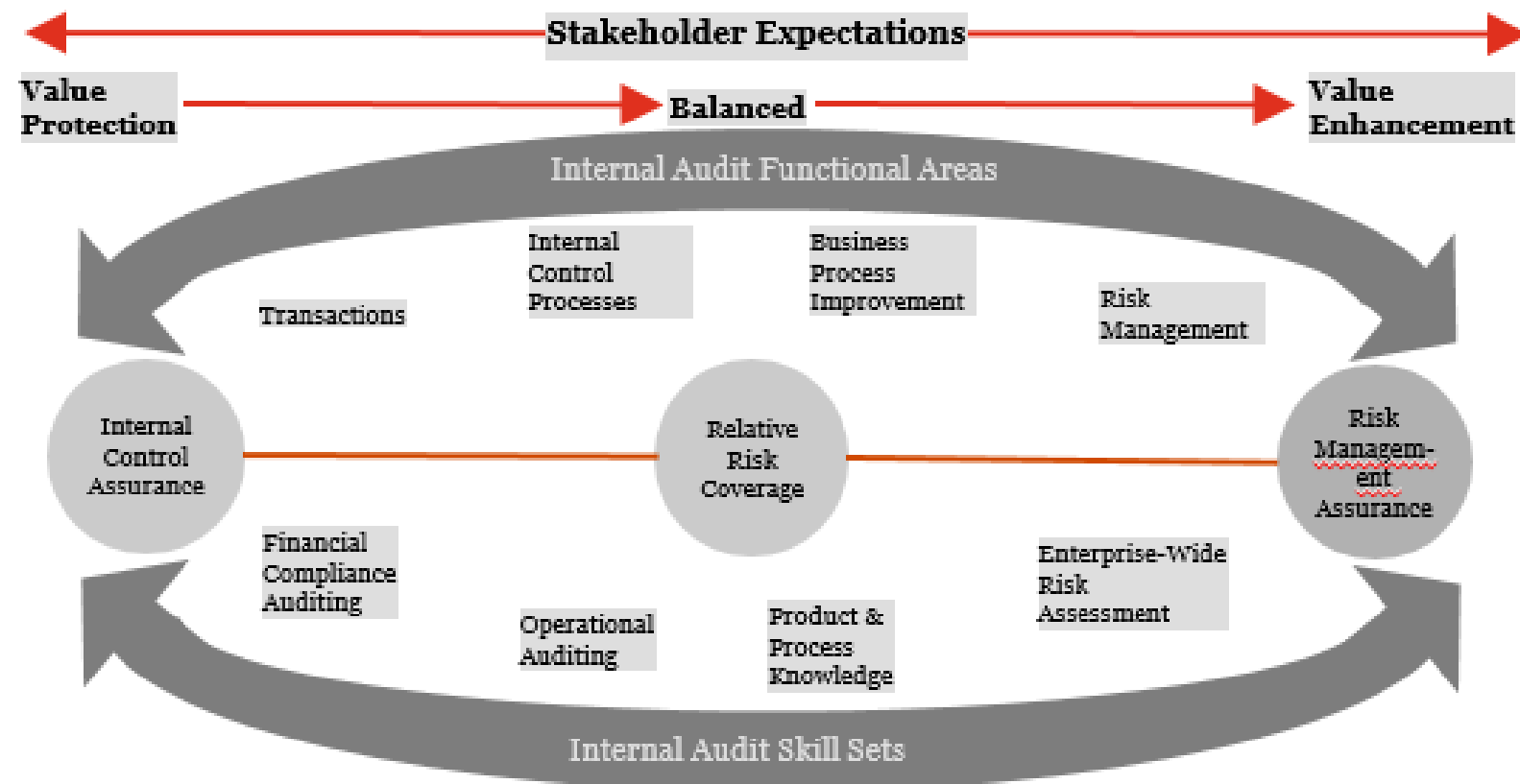
Articulating the mission of internal audit is important

A formal mission statement or charter lays out the function's goals and provides the basis to evaluate internal audit performance.

An effective mission statement delineates the function's authority and responsibilities and reflects the priorities of senior management and the audit committee. Although they vary in length and specificity, mission statements ought to address the degree to which the internal audit function will allocate resources toward traditional assurance-focused internal control activities vs. consulting activities perceived to add value to lines of business.

A mission statement that does not align clearly and directly with stakeholder expectations is of little value and can be a detriment to achieving strategic performance.

An illustration of The Internal Audit Continuum™ below depicts how internal audit's focus and skill sets may evolve as stakeholder expectations change.



The "to-be" intents should be clarified to shift the mind-set (1/2)

"We need to shift how people value the role of internal audit "

An illustration

Target Heads of Internal Audit	Up-sell to C-Suite and NEDs
Advise, co-source, outsource	Prioritise outsourcing initiatives
Focus on compliance	Focus on creating value (across the organisation)
Act as adversarial policeman	Act as collaborative connector
Look for individual risks	Help the whole business grow
Reduce costs	Identify opportunities and risks
Focus on the past and present	Be future facing

And focus on three objectives

- 1. Elevate the status of Internal Audit internally and externally.*
- 2. Increase understanding of the value of our offer internally and externally.*
- 3. Make our offer clear, comprehensive and consistent.*

The "to-be" intents should be clarified to shift the mind-set (2/2)

Common principles among Internal Audit functions that serve as 'trusted advisors'. These principles enable an Internal Audit function to be agile, yet deliver with consistent quality and innovation while optimizing cost.



Deliver with quality and innovation at an optimized cost

Our methodology is flexible to reach your optimal stride whether your function performs with high intensity intervals or at a marathon steady pace.

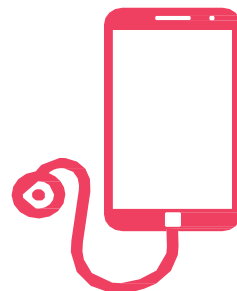
Enhance value through business alignment and risk focus

Our team will understand your organization's fitness goals and develop a program aligned to achieving Internal Audit's optimal level of performance



Embrace technology, leveraging data analytics and visualization

We recognize the important role technology now plays in monitoring performance, encouraging us to push boundaries and support us to achieve our targets. We bring you the latest thinking and tech innovation to enable you to reach your strategic goals.



Bring the right talent and provide insights

We'll bring technical and practical "coaching" support and insights in the form of both core audit skills and a wide range of specialists, to make sure you can tackle whatever challenges come your way in a dynamic and constantly changing risk environment.



Cultivate a client service culture and stakeholder management

We are continually innovating and pushing our own boundaries. We also focus on knowledge sharing with our clients and use our recovery time to evaluate progress and make necessary adjustments to ensure you achieve optimal results.

Flexible and Future-Fit

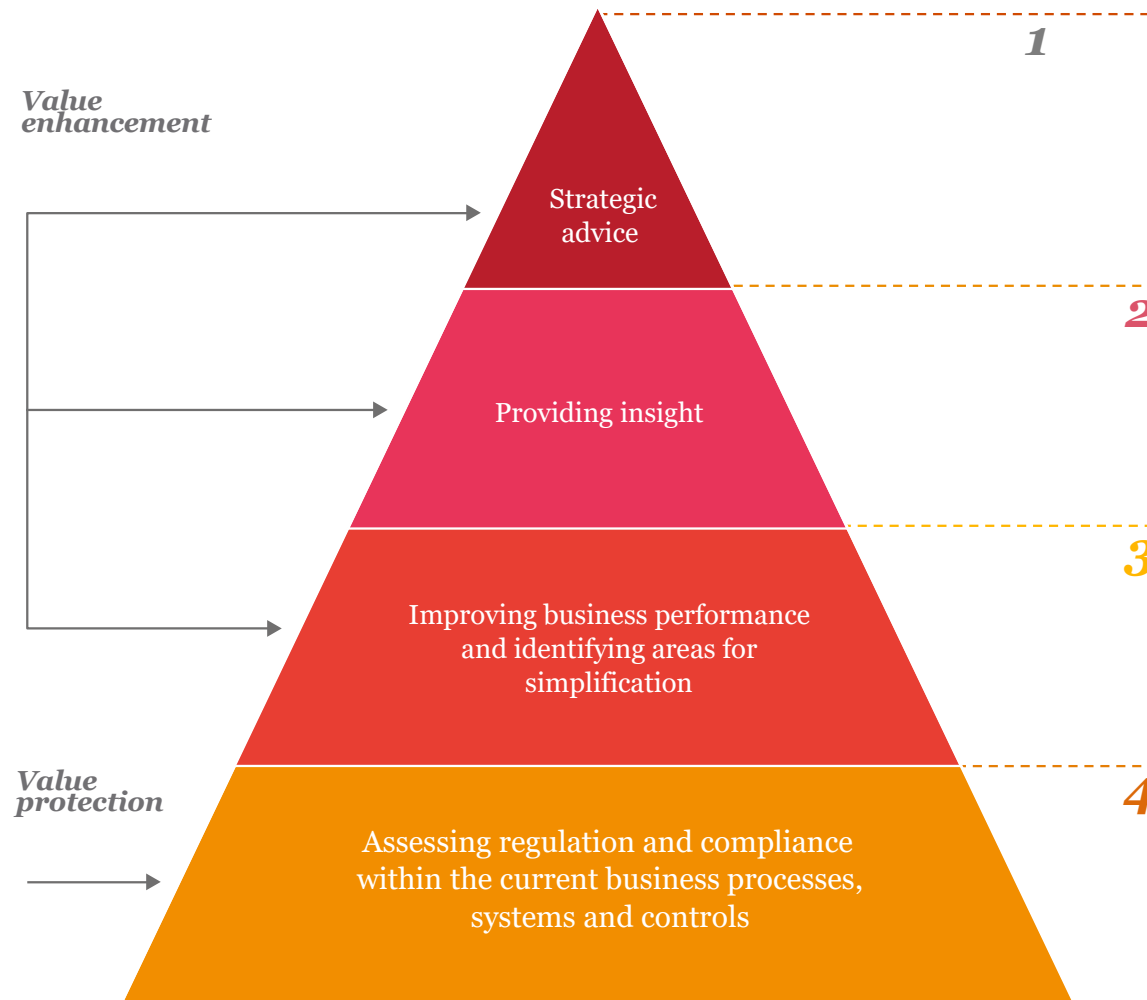
Overview of the Roles

As a trusted advisor, it is important to understand your needs and expectations of internal audit.

While internal audit's traditional role includes providing an objective point of view on governance, risk management and control processes (value protection), we also believe it should include consulting and other activities (value enhancement).

To ensure we achieve the right balance we will conduct further interviews with members of your Audit Committee, Board and management to confirm the priorities for the organisation and the areas of focus for internal audit.

Once we have a full understanding of the role you would like internal audit to play, we will formalise this and our responsibilities in the Internal Audit Charter.





4

Internal Audit Digitally fit function:
impact of technology innovation

Internal Audit of the Future:

Impact of technology innovation

Businesses today face a deluge of rapid change, driving internal audit to be more strategic

1

Increased transaction volumes

2

Groundbreaking emerging technologies

3

Business transformation

4

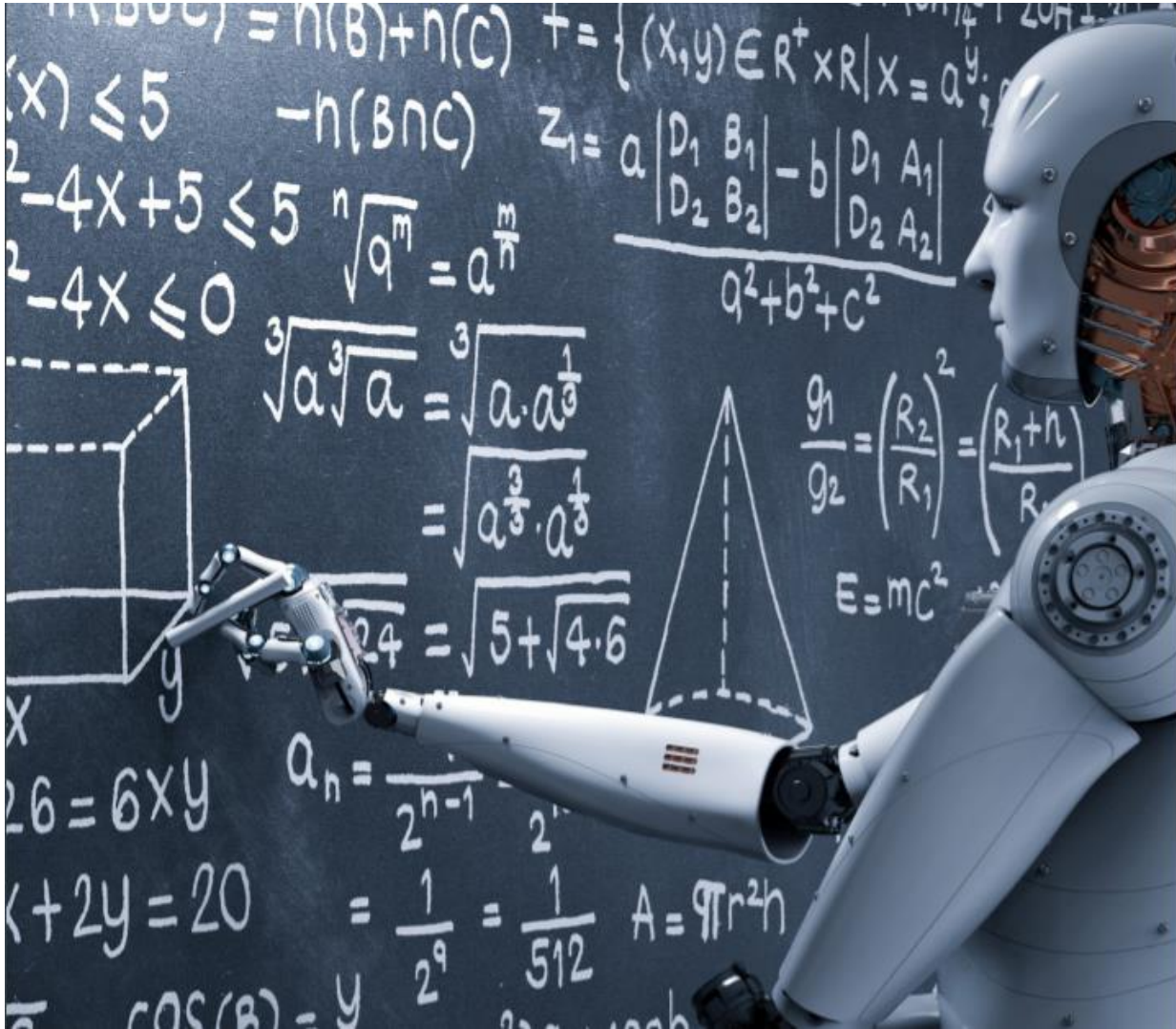
Cybersecurity and privacy

5

Regulation

Only 19% of those surveyed in PwC's 2019 State of the Internal Audit Profession Study were "digitally fit" compared to their peers, and even that minority are not fully prepared for digital disruption.

Elevating internal audit's role: The digitally fit function



Find the right
fit for emerging
technologies

Audit and advise on emerging
technologies, and use them
to streamline the function

Elevating internal audit's role: The digitally fit function

“Algorithms are in themselves their own worst enemy. I don’t know whether the algorithm that was built has been tested or whether third parties looked at it. I don’t even know whether external auditors were involved. If you use the technology tool to go through contracts and drive revenue, accounts receivable, cash, and deferred revenue, how do I know that the algorithm was correct? Who audits that? Who tests it? And importantly, how do I know it’s locked down so that someone can’t come in and change it? That’s where I get concerned.”

Vanessa C. L. Chang, Member, Audit Committee, Edison International and Sykes Enterprises

“Easy access to RPA was a warning siren about how we had to have a proper governance process in place to allow access to these digital tools but with some supervision over the operation of them...my team did a good job of getting the right governance in place balancing risk with opportunity.”

John Merino, Chief Accounting Officer, FedEx Corporation

Elevating internal audit's role: The digitally fit function



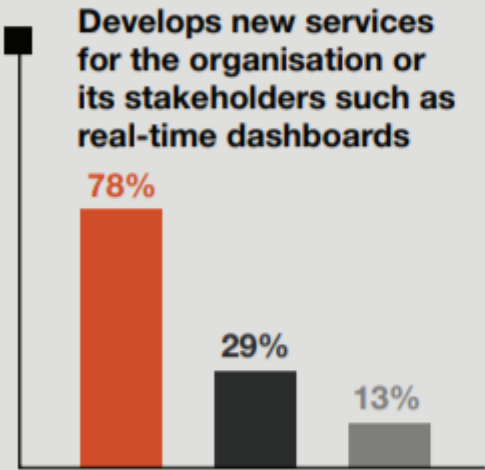
Enable the
organisation
to act on risks
in real time

Build new methods and services
to deliver assurance at the speed
the organisation requires

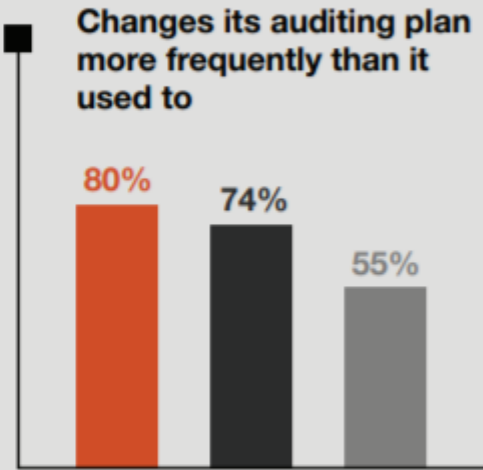
Elevating internal audit’s role: The digitally fit function

Dynamics are using data and technology to develop more-powerful insights

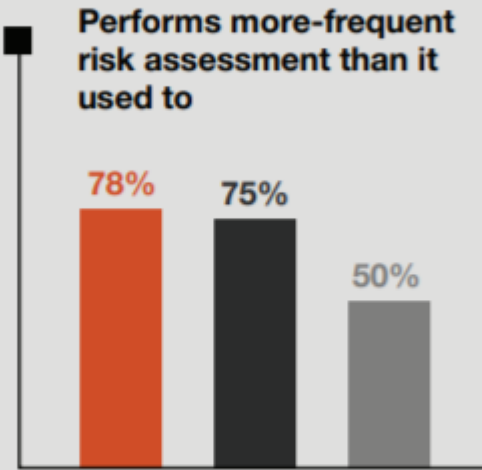
My function...



Q. Is your internal audit function doing or planning to do the following service-related activities based on the availability of digital technologies? (Responses are 'Doing now')
Base: 98 Dynamics; 140 Actives; 271 Beginners



Q. Please rate your level of agreement with the following statements about your internal audit function. (Responses are 'Agree' or 'Strongly agree')
Base: 98 Dynamics; 140 Actives; 271 Beginners



Elevating internal audit's role: The digitally fit function

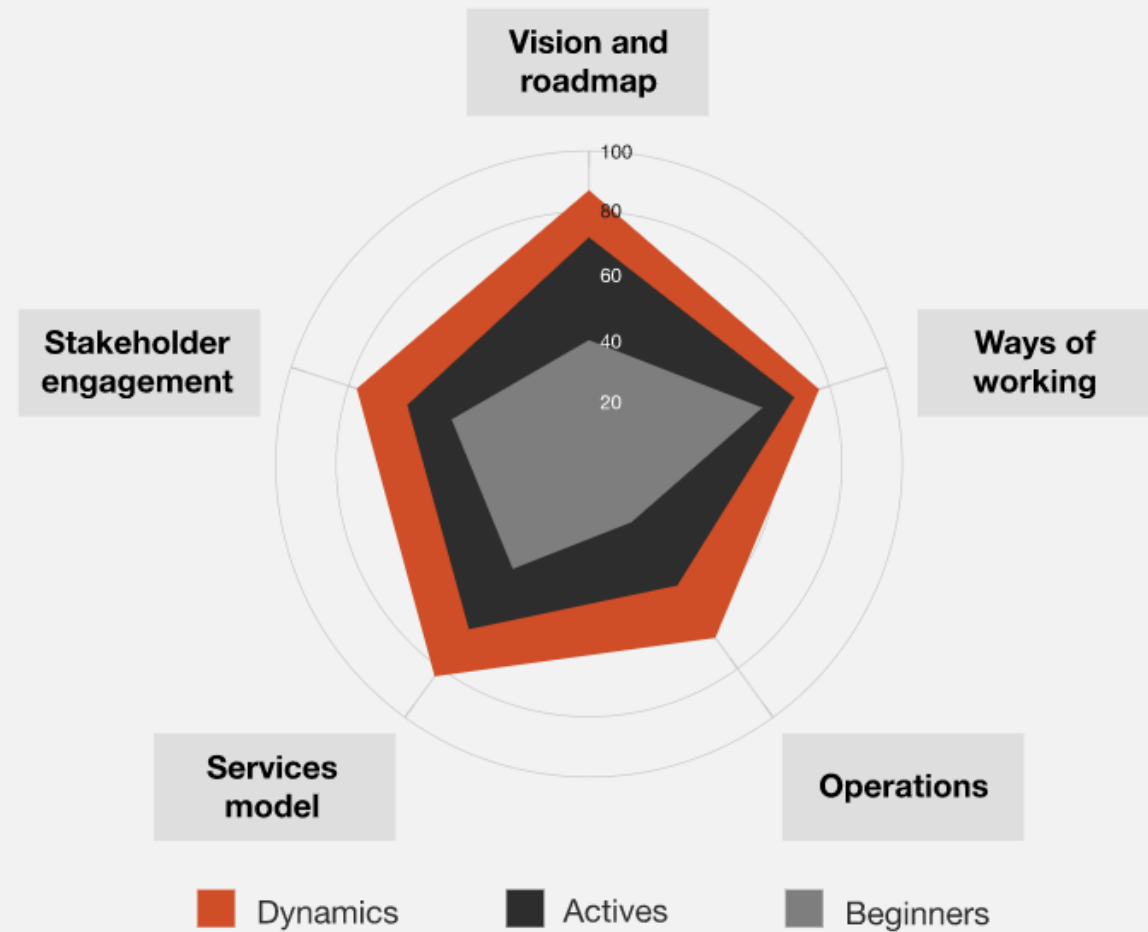
Organisations are rapidly rolling out digital initiatives in an arena defined by more data, more automation, sophisticated cyberattacks, and constantly evolving customer expectations. In some ways—for internal audit functions—the situation is not new: technology risks and controls have already been on their agendas for decades, and most can reliably deliver a technology audit.

- **Artificial Intelligence for such tasks as full population testing, controls or risk modelling**
- **Robotic process automation for monitoring or routine tasks such as data retrieval and audit testing**

Elevating internal audit's role: The digitally fit function

Where digitally fit internal audit functions stand out

Digital fitness in each dimension



Digital maturity score on a scale of 0 to 100 based on PwC analysis and index calculation.
Base: 98 Dynamics; 140 Actives; 271 Beginners

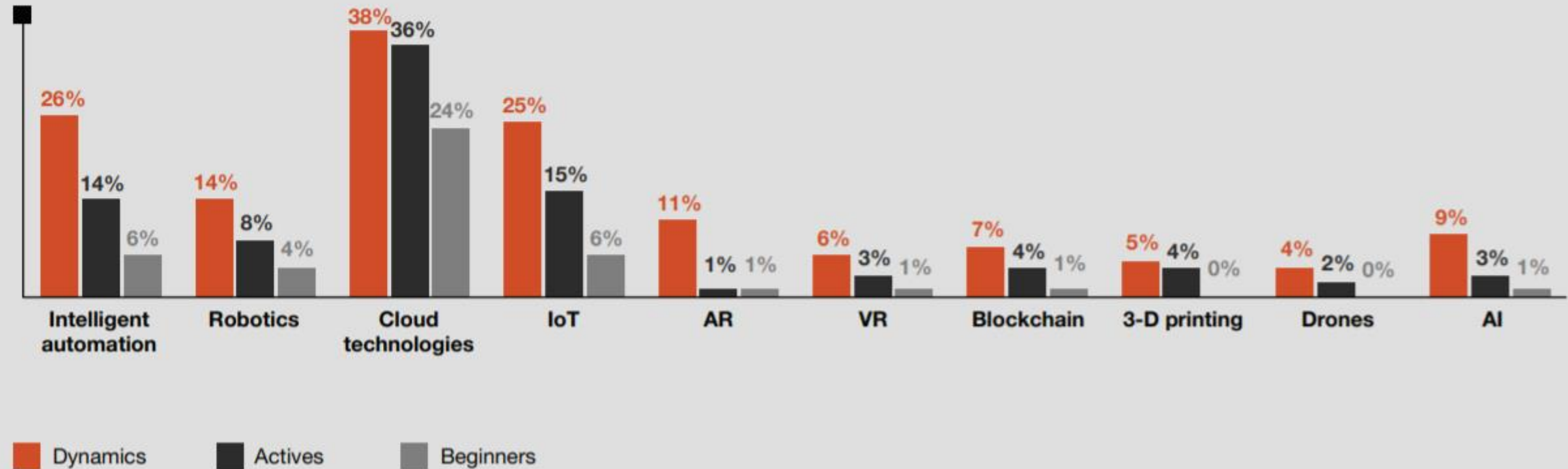
Six habits of dynamic internal audit functions

- 01 Go all-in on the organisation's digital plan
- 02 Upskill and inject new talent to move at the speed of the organisation
- 03 Find the right fit for emerging technologies
- 04 Enable the organisation to act on risks in real time
- 05 Actively engage decision makers of key digital initiatives
- 06 Collaborate and align to provide a consolidated view of risks

Elevating internal audit's role: The digitally fit function

Dynamics are preparing to audit emerging technologies

My internal audit function is fully staffed and capable of auditing or in the past 12 months has audited an area that uses this technology.

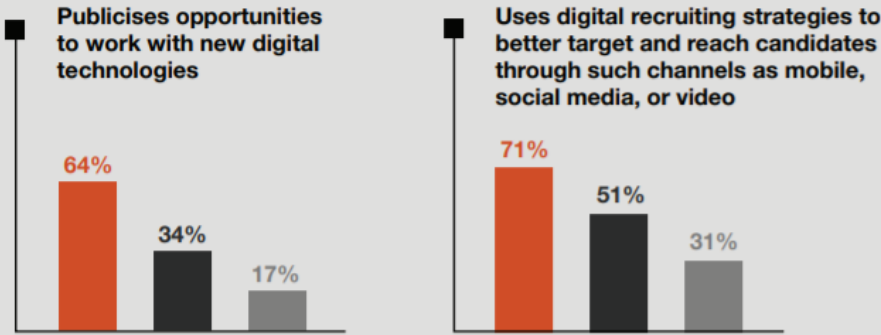


Q. Which of the following best describes your current preparedness to audit each of the following new technologies?
Base: 98 Dynamics; 140 Actives; 271 Beginners

Elevating internal audit's role: The digitally fit function

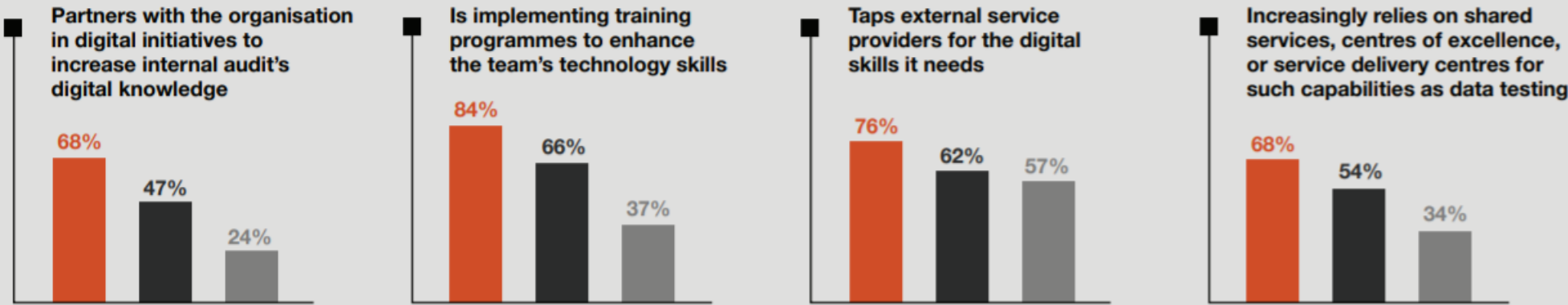
Dynamics put digital first in recruiting

My function...



Dynamics use multiple strategies for building digital skills

My function...

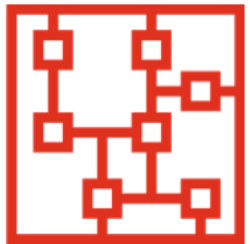


Four considerations to help facilitate your journey toward emerging technology internal assurance



Intelligent Automation and AI

Companies are using intelligent automation and AI to reduce costs and increase efficiency. As AI tools get “smarter,” they can help drive better decision-making, as long as the potential risks are understood.



Blockchain

If implemented correctly, blockchain can enable the creation of transaction processing systems with much higher-than-standard levels of trust. It may not be the answer to every challenge internal assurance faces, however. There is a need to establish industry standards and ways to audit blockchain systems.



Cyber Resilience

While cybersecurity awareness has grown, the overall rise in cyberattacks underscores the importance of continuously improving cyber resilience, agile defense and recovery capabilities.



Continuous Auditing

Continuous auditing can be an important mechanism for aligning internal audit activities more closely with the actual pace of transaction processing. Companies that implement continuous auditing have been able to redirect internal auditors' focus so they can serve as business consultants—identifying trends, investigating exceptions, and guiding strategy.

Robotic Process Automation (RPA): A primer for internal audit professionals

Five key risk areas to consider when implementing an RPA program

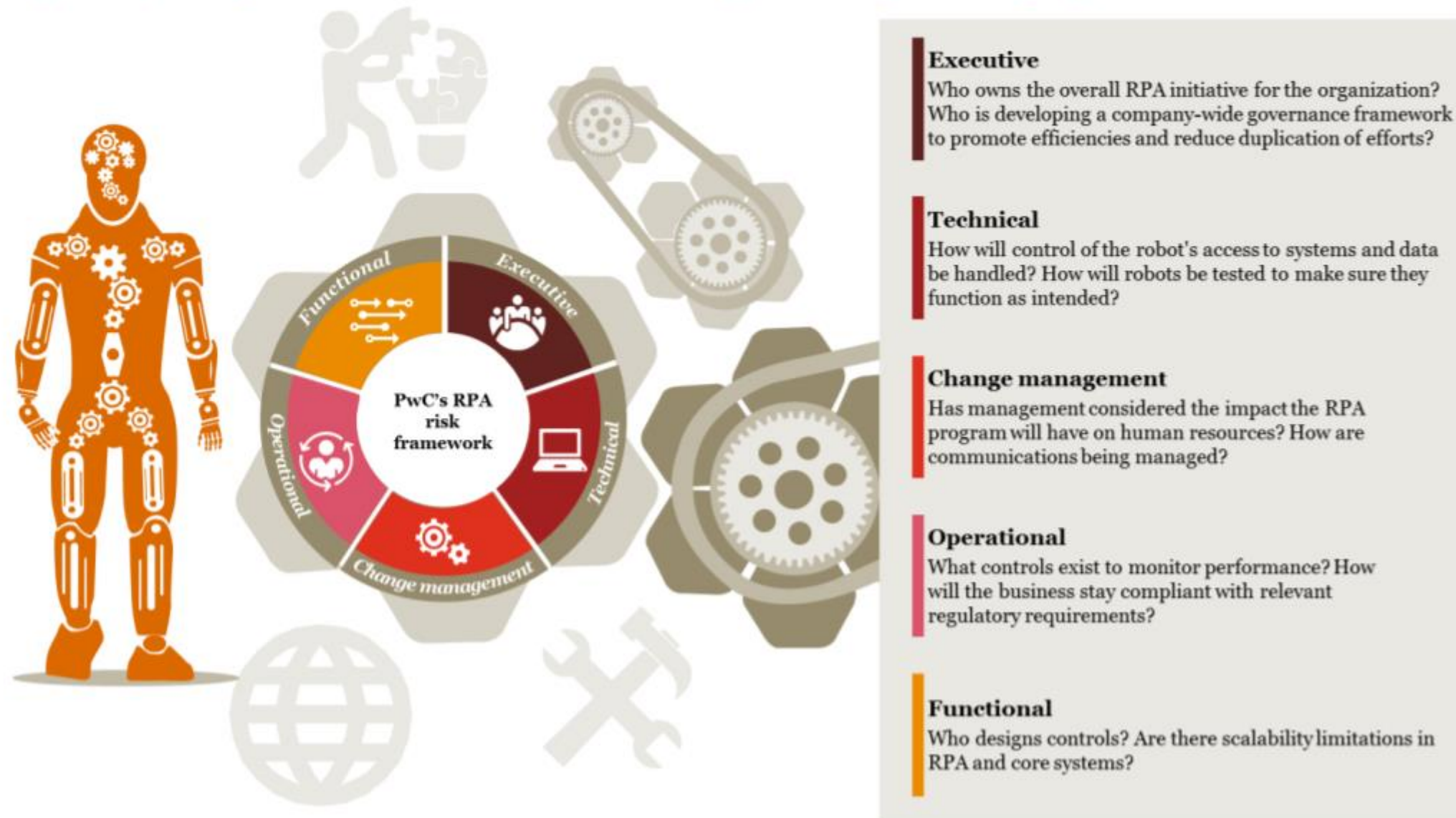


PwC estimates that 45% of work activities can be automated, and this automation would save \$2 trillion in global workforce costs¹.

Internal audit's early involvement in an RPA initiative ensures a balanced discussion, risk assessment and agreement on the overall governance framework and process design.

Robotic Process Automation (RPA): A primer for internal audit professionals

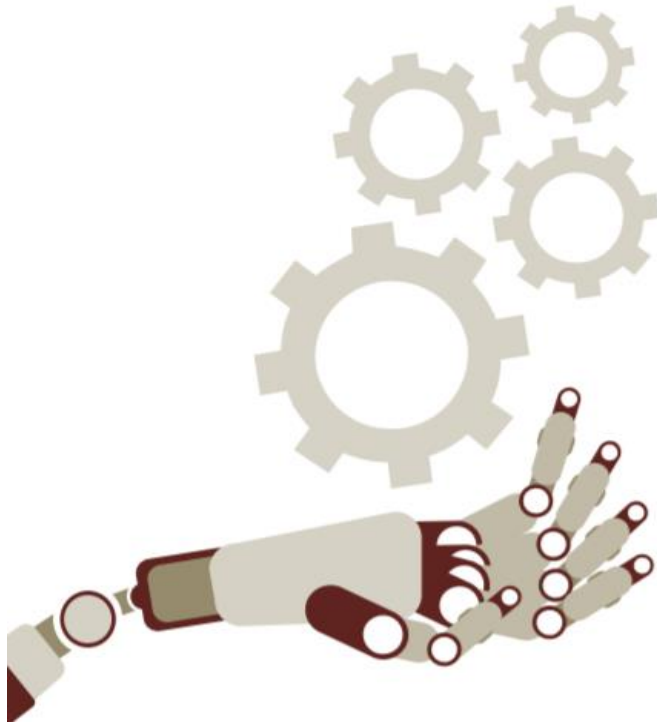
Figure 1: 5 categories of risk to consider when implementing an RPA program



Robotic Process Automation (RPA): A primer for internal audit professionals

Automating control performance, controls testing and other internal tasks

Through automated testing, internal audit can test full populations of data rather than sampling and management can have greater confidence that controls are designed and operating effectively.



Beyond the automation of controls testing, RPA offers significant potential to change how internal audit works. For example, some of the tasks that RPA could automate include:

- Identifying open items, sending emails to responsible parties, conducting follow-up when due dates are not met and documenting remediation status
- Tracking progress against the annual audit plan or tracking and monitoring key risk indicators (KRIs)
- Automating reporting and dashboarding activities, including populating audit committee and management report templates or internal audit's balanced scorecard
- Evaluating data quality in any system, such as in master data files, checking for completeness of fields, duplicates and validation

Robotic Process Automation (RPA): A primer for internal audit professionals

Questions CAEs should consider



Have we inventoried our Internal Audit processes and identified repetitive, mundane or undifferentiated tasks done by humans that could be carried out by robots?



Have we considered if there are processes that could be simplified to then become automated (challenging the status quo)?



Have we connected with the business or functional leaders to learn where they are or could be using RPA and to coordinate RPA initiatives?



5

Why do we need
Internal Audit transformation?

Avoiding change is not an option. Why the time to transform internal audit is now

There are **5.9 million businesses**¹ in corporate America employing **127 million people**². Estimates predict **40% of jobs**³ could be affected by automation in the next 10 years. The balance of jobs will significantly change in nature, requiring new skill sets.

As technology takes a front seat, here's what's happening in the business ecosystem:

Customers and shareholders are just as focused on trust, integrity and privacy as they have been on quality, relationships and price

Employees are embracing new technology tools across the entire spectrum of employee experience from onboarding and teaming, to mentorship and customer relationships

Regulators and standard setters are moving into previously unknown territory, such as privacy and operational resiliency, to uncover new and risky behaviors that may affect customers

Communities and advocacy groups are both stakeholders and watchdogs, identifying potential issues before they become known to the business

Channel partners are an integrally connected extension of the business, leveraging publicly available data to make vendor and channel partner decisions

Avoiding change is not an option. Why the time to transform internal audit is now

When nothing in the internal or external environment is status quo, isn't it time to think differently about internal audit?

Real ways internal audit teams are transforming now:

- By using unsupervised learning in the form of artificial intelligence, one team can detect anomalies and correlations that wouldn't otherwise be detected
- Another team identifies high risk transactions with channel partners, real time, to fundamentally change the scope and approach of the audit
- A third team is so in sync with business strategy that it used data-enabled auditing to free up approximately 40% its of annual budget to respond to risks associated with a new service launch
- Another internal audit team has created risk indicators and data analysis tools now used by other lines of defense for continuous monitoring of controls
- And, another hosts digital upskilling sessions to ensure teams can adjust to the changing technology and risk landscape



Avoiding change is not an option. Why the time to transform internal audit is now



How to get started?

Internal audit has an opportunity to re-envision the impact it can make for the organization and reframe the approach it takes to add value and keep pace with business change. Some areas to consider before starting your journey:



Assemble a strong team that's ready and excited to get started on your journey



Discover new capabilities and ideas for internal audit to drive value like never before



Choose ideas that would drive immediate impact with limited/no additional budget



Explore alternative models for sourcing talent and technology—run some pilots



Socialize and celebrate your successes. Every small win builds momentum!



Develop a roadmap for people-led, data-driven transformation

Avoiding change is not an option. Why the time to transform internal audit is now

NextGen IA professional profile

Internal audit acumen

- Deep auditing skills
- Professional skepticism focused on business value



Business acumen

- Industry knowledge
- Deep regulatory and compliance knowledge



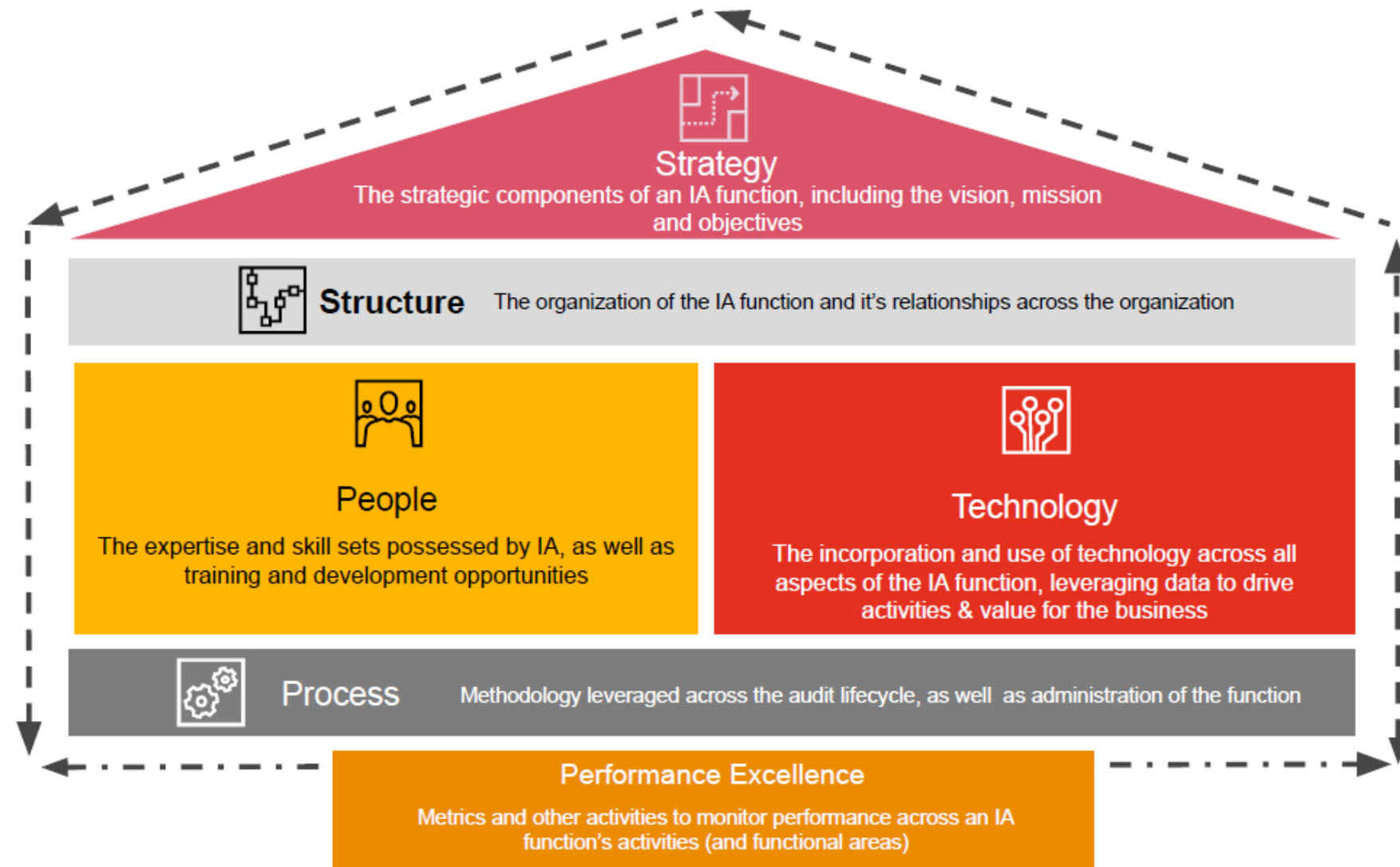
Digital and data acumen

- Understanding of data sources, data quality, insights, and analytics capabilities
- Knowledge of ERP, Cybersecurity, Cloud, and as automations



Areas of Internal Audit Transformation

The IA Transformation framework is applied to each of the internal audit functional areas based on the current vision and baseline of the organization, and performance excellence is considered throughout





6

Transforming the value proposition of internal audit

There is a clear gap in how Internal Audit (IA) meets the needs of its stakeholders...

Contents

77%

Of board members believe Internal Audit's current level of involvement in risk is not sufficient

>50%

Of management believe Internal Audit does NOT contribute significant value to the organization

46%

Of stakeholders view Internal Audit as a Significant value provider.

... and now more than ever there are opportunities for IA to react and evolve



Digital transformation,
Speed of change &
Data availability



Impacts of
COVID-19
“New Normal”



Dynamic and complex
business models

Has internal audit been keeping up?

Contents

While IA has made incremental strides...

- Periodic risk assessment
- Rolling audit plan
- Workflow tools
- Basic analytics
- Leverage subject matter resources
- Guest auditors
- Agile execution approach
- Better dashboards



...challenges remain!

- Qualitative risk assessment discussions seem too high level
- Technology adoption rate is increasing
- Duplicative control testing activities across the 3 lines
- Sample approach for audit work seems antiquated
- Stakeholder expectations continue to increase, while budget pressures remain
- **How do we upskill, attract and retain NextGen talent?**
- **How do we audit differently?**



While IA has made incremental strides over the past few decades, it is now time for Internal Audit to evolve. Let's transform IA...



Adapting to today's new world

Contents

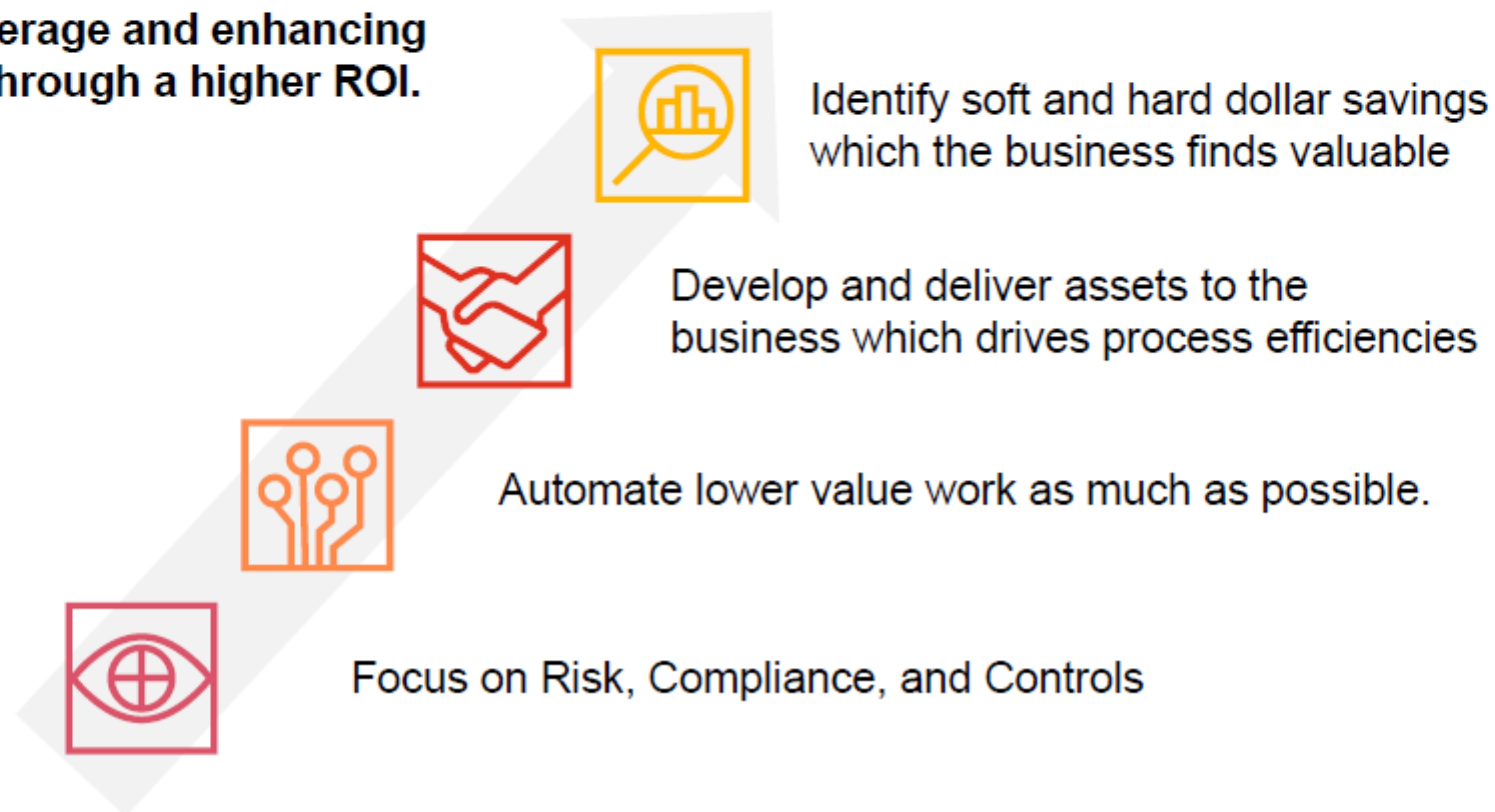
As we pivot from COVID-19 response to adopting a 'new normal'; it's critical to ask..

What have we learned?... Have expectations changed?

The 'new normal' demands adjustments to business processes with technology and data at the center of it; the data is waiting to be untapped. Internal Audit is uniquely positioned to provide insights across corporate functions because of their access to data.

Transforming the IA value proposition:

Providing greater risk coverage and enhancing its value to stakeholders through a higher ROI.



Discovering what's possible

Contents

Now IA functions can...



Identify blind spots, previously humanly impossible



Provide greater coverage across organization without increasing audit resources



Uncover human behavioral patterns through machine learning and regression



Scope and execute audits virtually, with a data driven and risk based targeted precision



Influence the strengthening of first and second line defenses through digital collaboration and continuous monitoring



...some have already started



Leveraged machine learning on 500,000 images to **identify potential fraud in under 10 minutes**

Impact: Created a data enabled approach to monitoring the \$1.6 Billion Marketing Fund.



Conducted IP leakage audits for **specific product types, location & targeted employee types** flagged by deep learning algorithms

Impact: Detected evidence of counterfeiting of products in the vicinity of several overseas factories.



Used modeling to **identify HR team wrongfully delayed termination** of employees in the system to receive quarterly retention bonuses

Impact: Magnified deviations from expected throughput time and determined the root cause of these cases



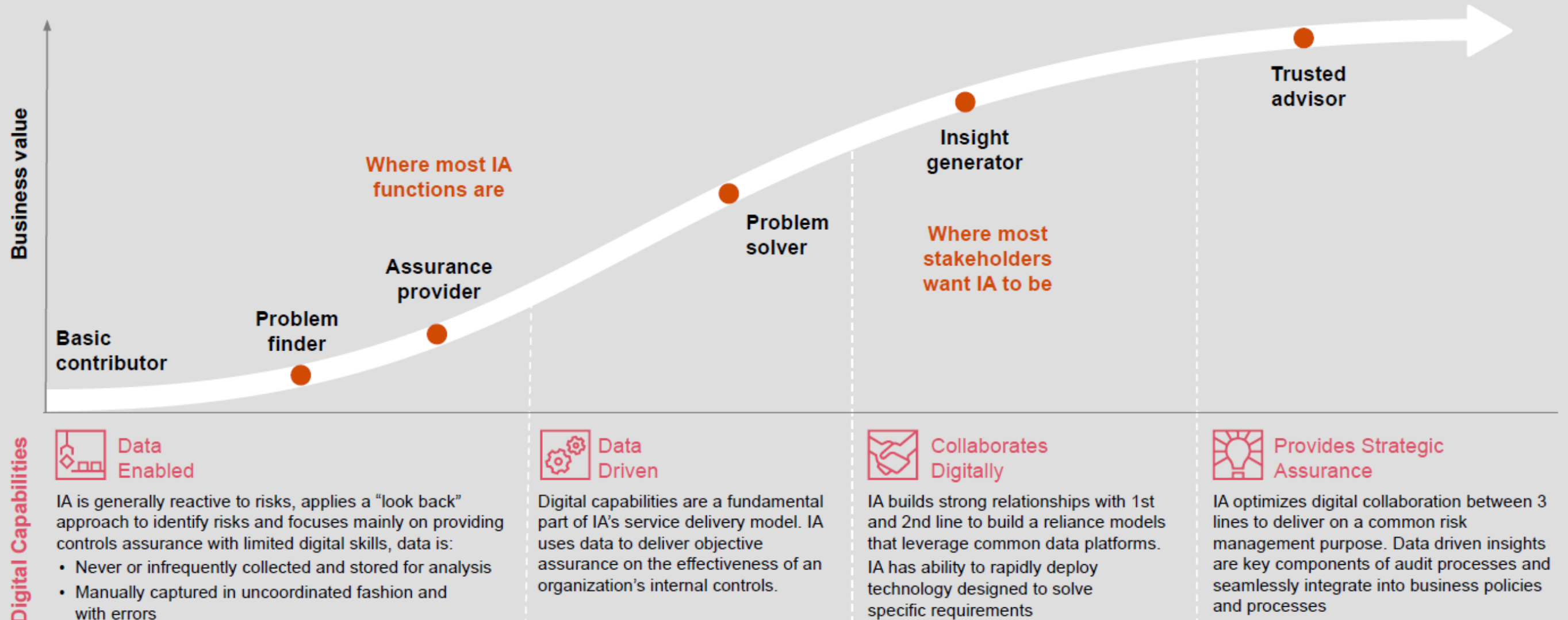
Built third party risk monitoring dashboards using data from the web and **transitioned to second line for ownership**

Impact: Improved management and ongoing monitoring of workforce utilization against internal benchmarks

Recalibrating the IA maturity curve

Digital capabilities are essential to driving value beyond an assurance provider

[Contents](#)



How can Internal Audit move up the maturity curve?

Contents



Strategy	<ul style="list-style-type: none"> • Migration away from control-centric to risk-thematic view 	<ul style="list-style-type: none"> • Assurance over risks that are of strategic value 	<ul style="list-style-type: none"> • Common sense of purpose for all risk management activities
Structure	<ul style="list-style-type: none"> • Teaming structure based on risk themes • Leverage existing risk management activities 	<ul style="list-style-type: none"> • Aligned assurance maps / reliance models • Real-time, role-based engagement with business and 2nd line of defense. 	<ul style="list-style-type: none"> • Real-time, role-based engagement with stakeholders • Proactive engagement with business
People	<ul style="list-style-type: none"> • Personalized Learning by Role 	<ul style="list-style-type: none"> • Deep learning for Digital Accelerators • Data-driven and issue-focused mindset 	<ul style="list-style-type: none"> • Digitally upskilled profiles & deployment • Crowdsource innovation
Technology	<ul style="list-style-type: none"> • Analytics for IA and others lines of business • Automation for repetitive / standardized areas — i.e data gathering activities 	<ul style="list-style-type: none"> • Robotics and automation • Use of unstructured and structured data sources for auditing 	<ul style="list-style-type: none"> • Artificial intelligence (AI) and machine learning — software to automate testing • Continuous monitoring & auditing
Process	<ul style="list-style-type: none"> • Common risk taxonomy, defined metrics, and measures (KPIs, KRIs) 	<ul style="list-style-type: none"> • Dynamic risk identification and monitoring based on leading and lagging indicators • Broad set of agile audit activities 	<ul style="list-style-type: none"> • Insights on blind spots: pattern analysis and behavioral insights by “connecting the dots”

Benefits - Why does Internal Audit need to transform?

Contents

When Internal Audit...



Assess its brand and buy into shared vision of risk with a focused on business value **(Strategy)**



Invest in partnership across risk functions **(Structure)**



Upskill and inject new talent **(People)**



Embrace the use of data and digital tools **(Technology)**



Redefine Internal Audit agility, speed, and scalability **(Process)**



The organization gains a...

Strategic business partner; identify strategic insights and enhanced value through actionable cost savings recommendations

Risk Resiliency Leader; remove possible redundancies in risk management and drive consistent messaging to business

Leadership talent incubator; Creates future leaders with emerging technologies proficiency coupled with functional business acumen.

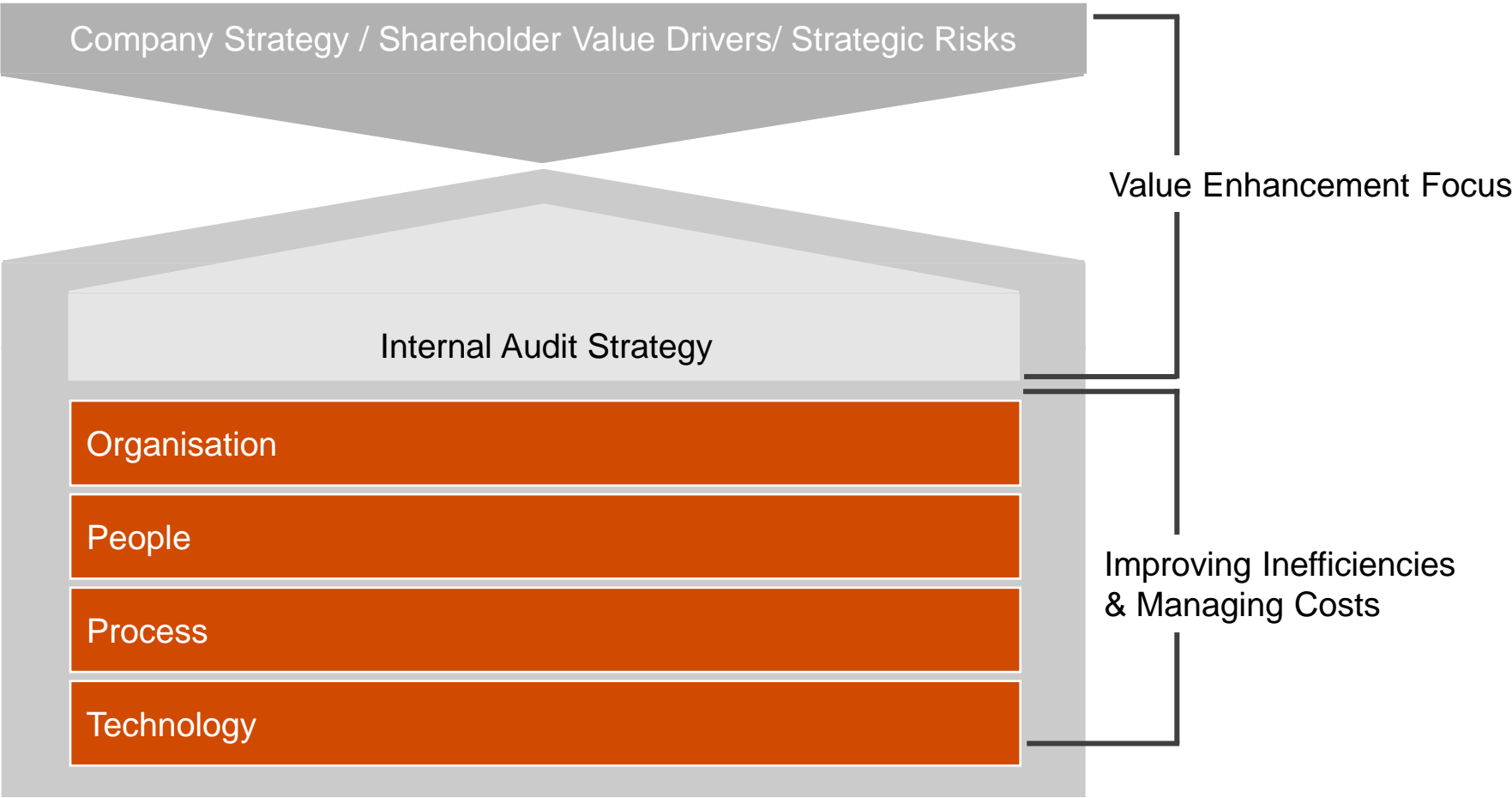
Risk Tools Catalyst; Create common tools and transferable assets for cross functional risk identification

Trusted Advisor; Obtain wider risk coverage across the organization and a more targeted scope for cost optimization.



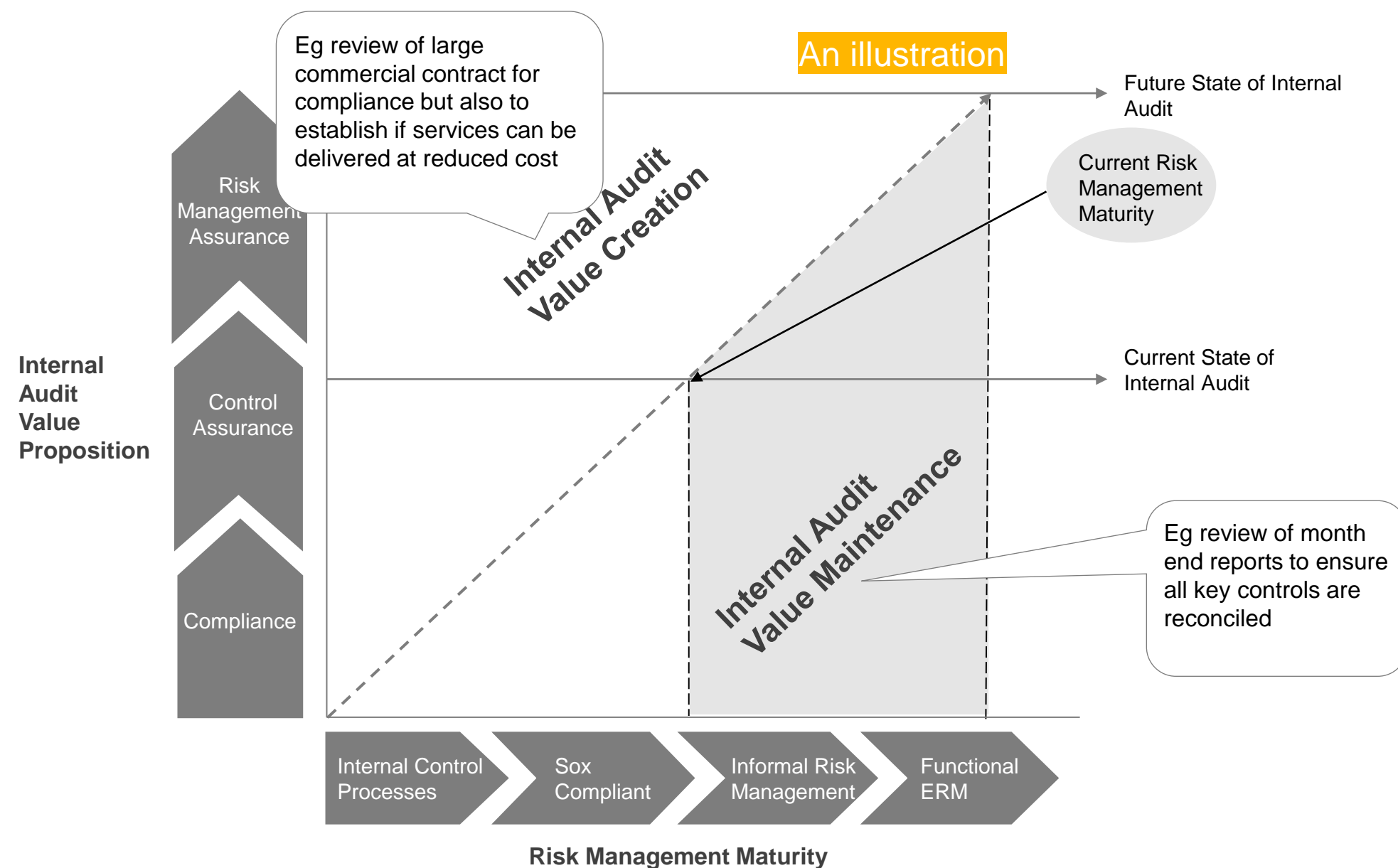
General approach in transforming internal audit function

Balancing between value maintenance and value enhancement



General approach in transforming internal audit function

Balancing between value maintenance and value enhancement



Method of Internal Audit Transformation

Implementation of Data Analytics

Through capitalizing the new data-driven business available from business activities and external sources, Internal Audit can apply new techniques by embedding data analytics during audit process. Therefore, Internal Audit can provide the management with new insights that cannot be captured with the traditional method. Following are the benefits on implementing Data Analytics during audit process:



Increase audit scope

Audit process can now capture 100% of populations, rather than selected samples



Increased efficiency

Manual audit procedures can be reduced



New analysis method

Usage of data visualization to analyse trends in the data



Continuous Monitoring

Monitoring process can be done continuously through data



Reduce Cost

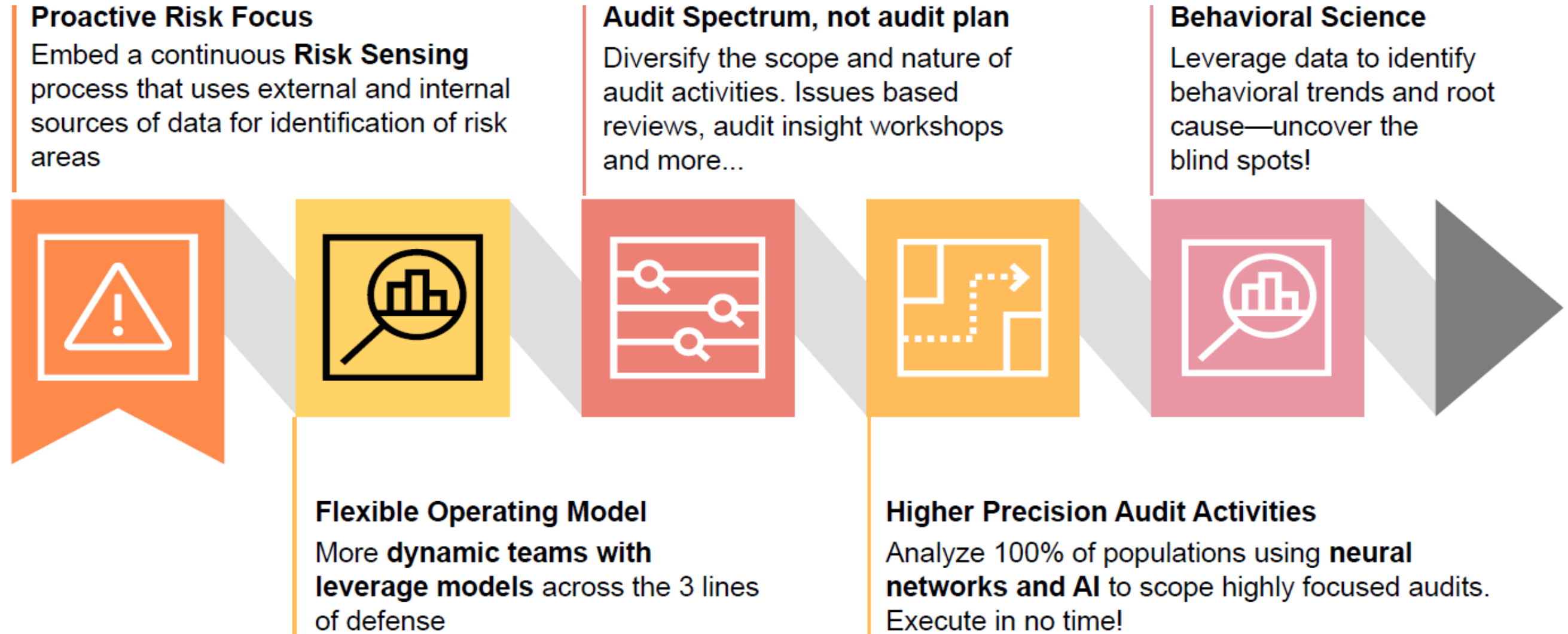
Lower operational cost by maximizing data driven procedures



7

Expected outcome of
Internal Audit Transformation

What does a transformed IA function look like?



Internal Audit of the Future



Are you ready to:

- Identify blind spots, previously humanly impossible
- Influence the strengthening of first and second line defenses through digital collaboration and continuous monitoring
- Provide greater coverage without increasing audit resources
- Conduct audits with surgical precision
- Uncover human behavioral patterns through machine learning and regression



8

Anti-fraud Management

Fraud is more than financial losses

Maximize positive user experience and retention of stakeholders (customers, vendors, employees, business partners);
Minimize inconvenience to stakeholders.

Maximize efficiency of anti-fraud controls and operations
Minimize total operational cost of fraud controls.

Enable the business to achieve growth goals by finding solutions to risk problems; have scalable controls;; Minimize business disruptions.

Maximize reliability and trust with direct and indirect stakeholders;
Minimize mistrust, which will hurt the brand.

Minimize real hard-dollar fraud losses and maximize recoveries, for the client and their stakeholders and customers.

Meet compliance obligations and as appropriate lead industry in finding innovative solutions to do so; Minimize regulatory penalty.



Several factors are on the rise across sectors promoting the heightened risk of fraud

Availability of data

Mass data breaches continue to cause major disruption, flooding the dark web with PII and compromised credentials for sale at a premium

Use of sophisticated tools and techniques

Organizations are struggling to keep up with the shifting nature of fraudsters and the sophistication of methods they use, such as device/IP/ID spoofing, advanced malware, bot armies and social engineering

Unintended consequences of Digital and payment transformation

New and faster payment networks and accelerated deployment of new digital products introduce elevated fraud risk. Fraudsters leverage new channels as entry points.

Exploitation of weak control environment

As businesses look to stay ahead of the competition, fraudsters continue to target the path of least resistance – taking advantage of control vulnerabilities and over reliance on technology without the right operational infrastructure support

Complex treasury payment processes

Payment and treasury systems have gotten more complicated over time. These systems are vulnerable to both internal and external frauds.

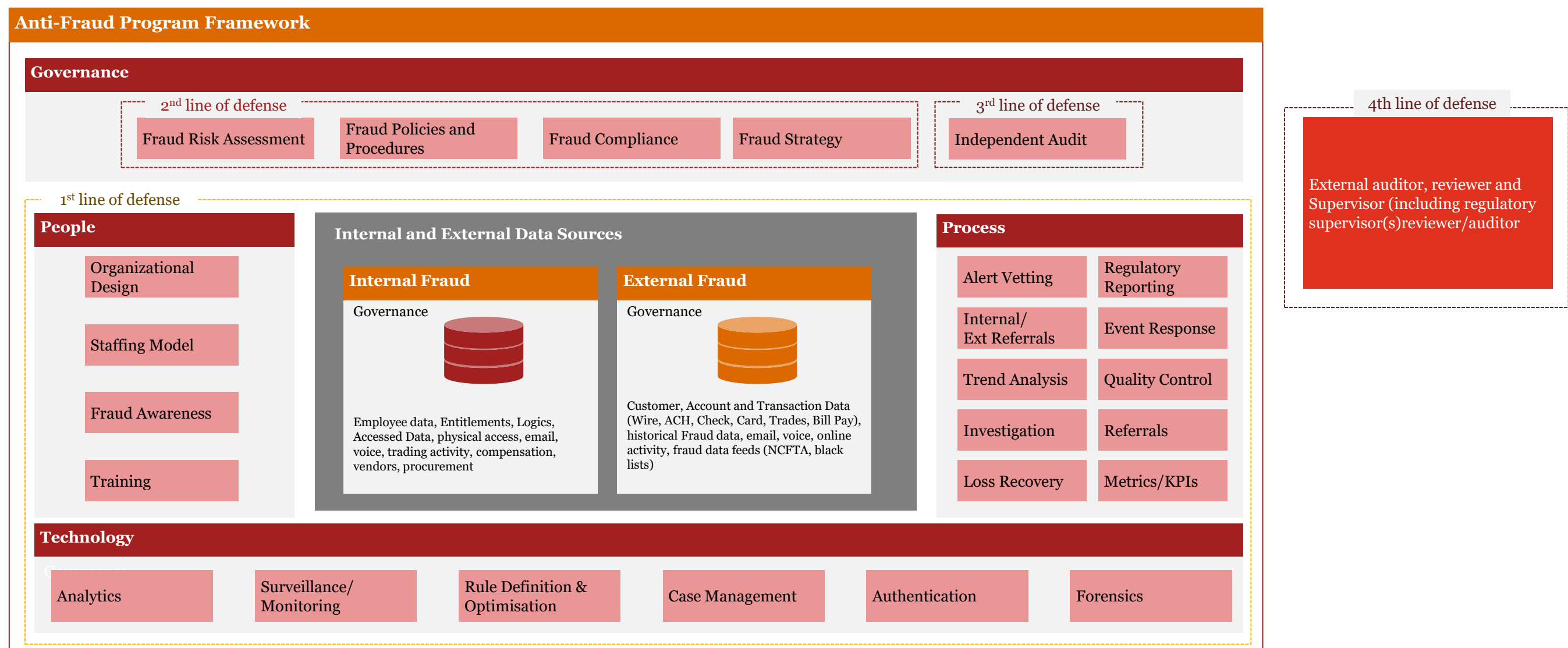
Convergence of sectors

Increasingly lines are blurred between traditional sectors and channels to market (e.g. digitization) which creates complexity and presents opportunities for fraudsters (e.g. creating more attack surface)

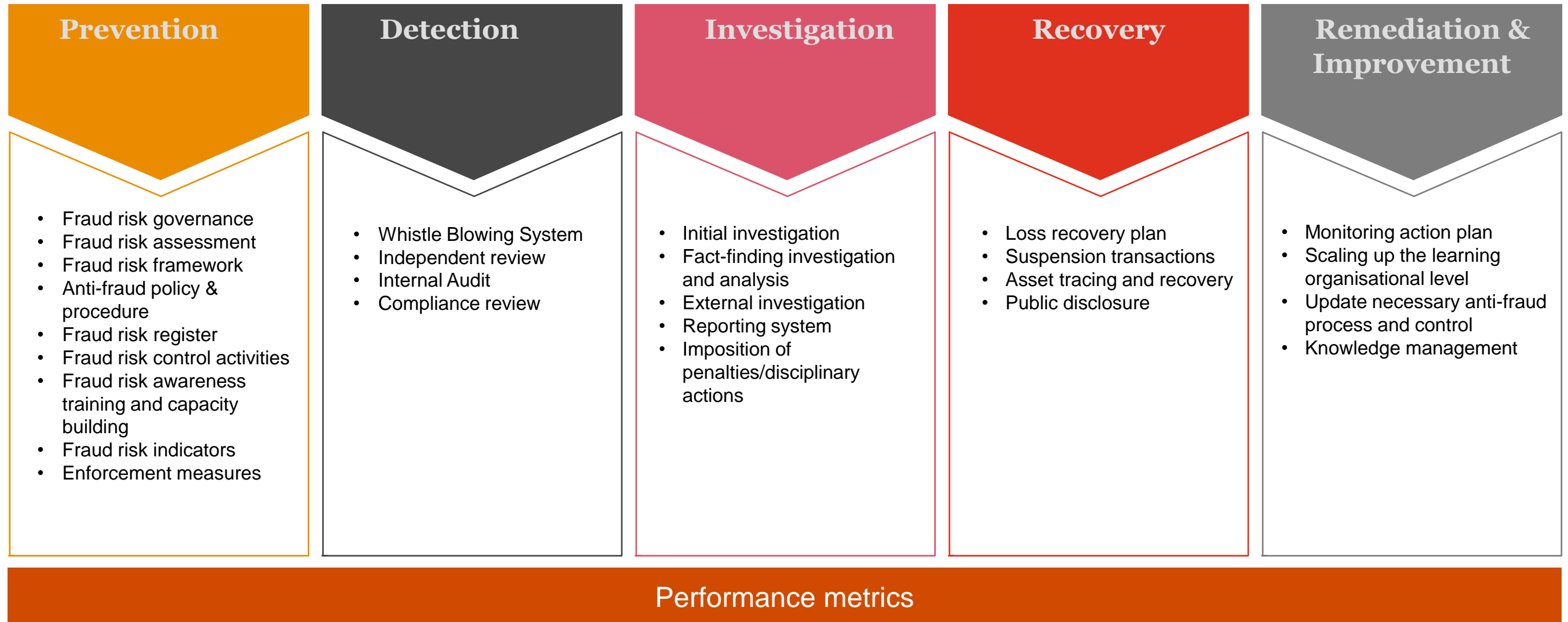
Managing fraud risks are becoming more important than ever before

Anti-Fraud Program Framework

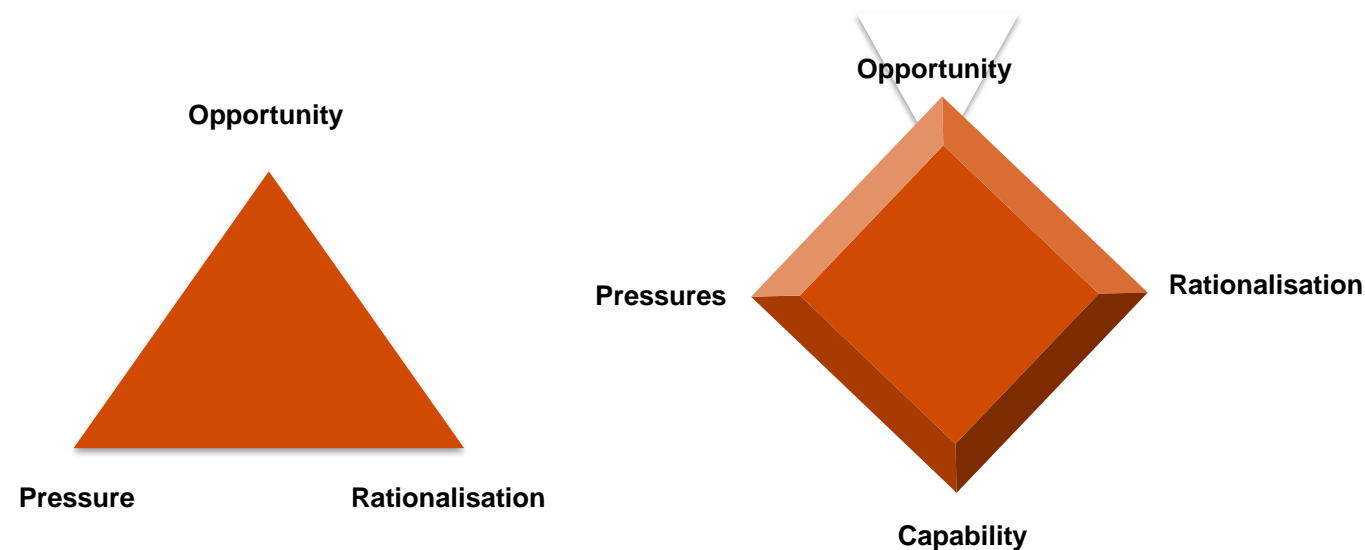
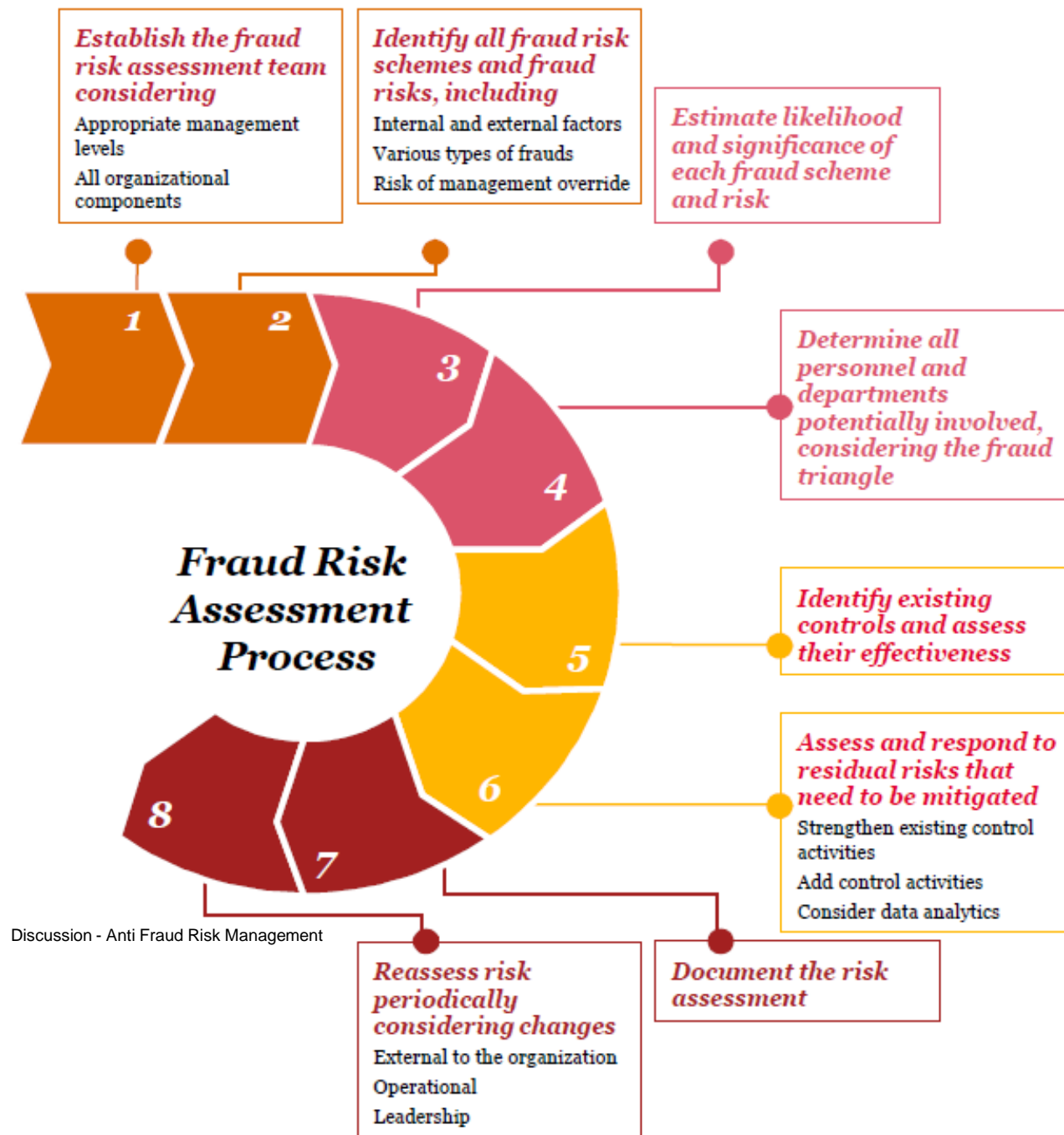
Companies seek to minimise their risk of fraud through implementation of anti-fraud programs. The diagram below illustrates components which may form part of such a program.



PwC Anti-Fraud Management Cycle

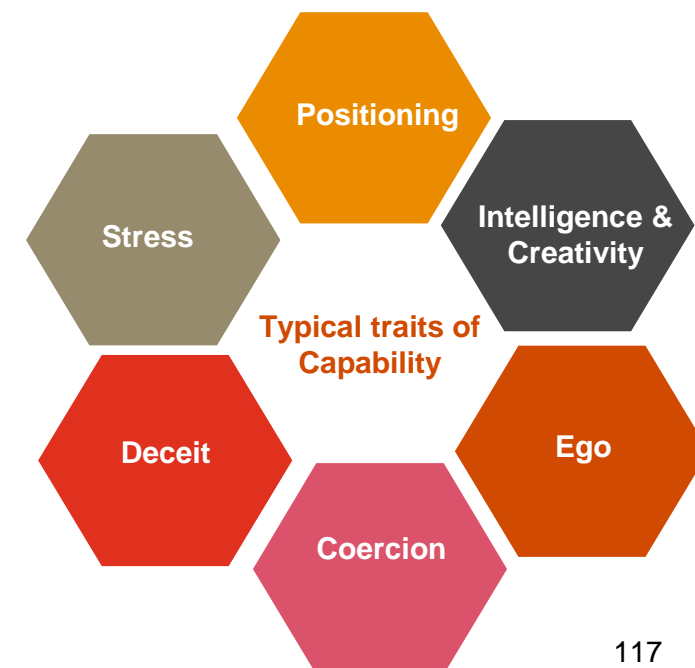


Incorporating the Fraud Diamond in the assessment



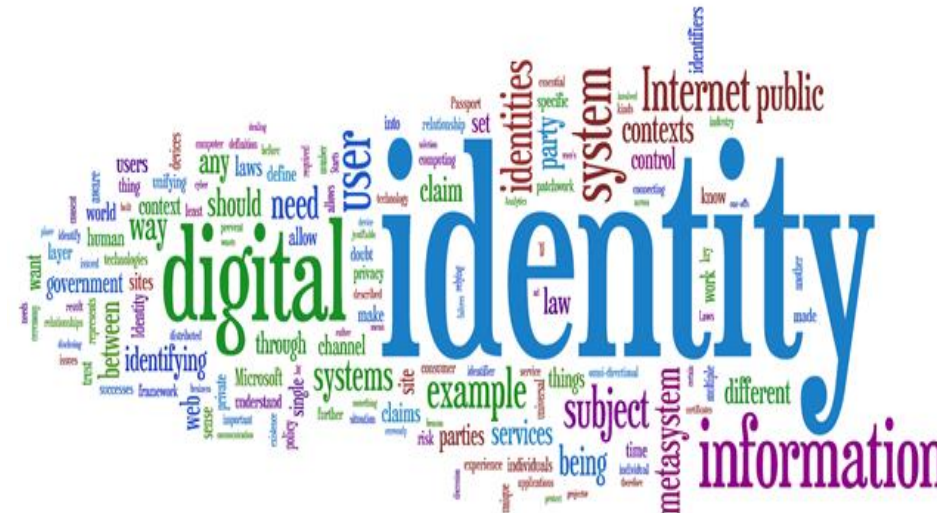
When we identify processes, consideration all relevant points of focus and opportunities, incentives/pressures and attitudes/rationalization will be considered...

...and expanded into adding the element of capability into the "fraud diamond"

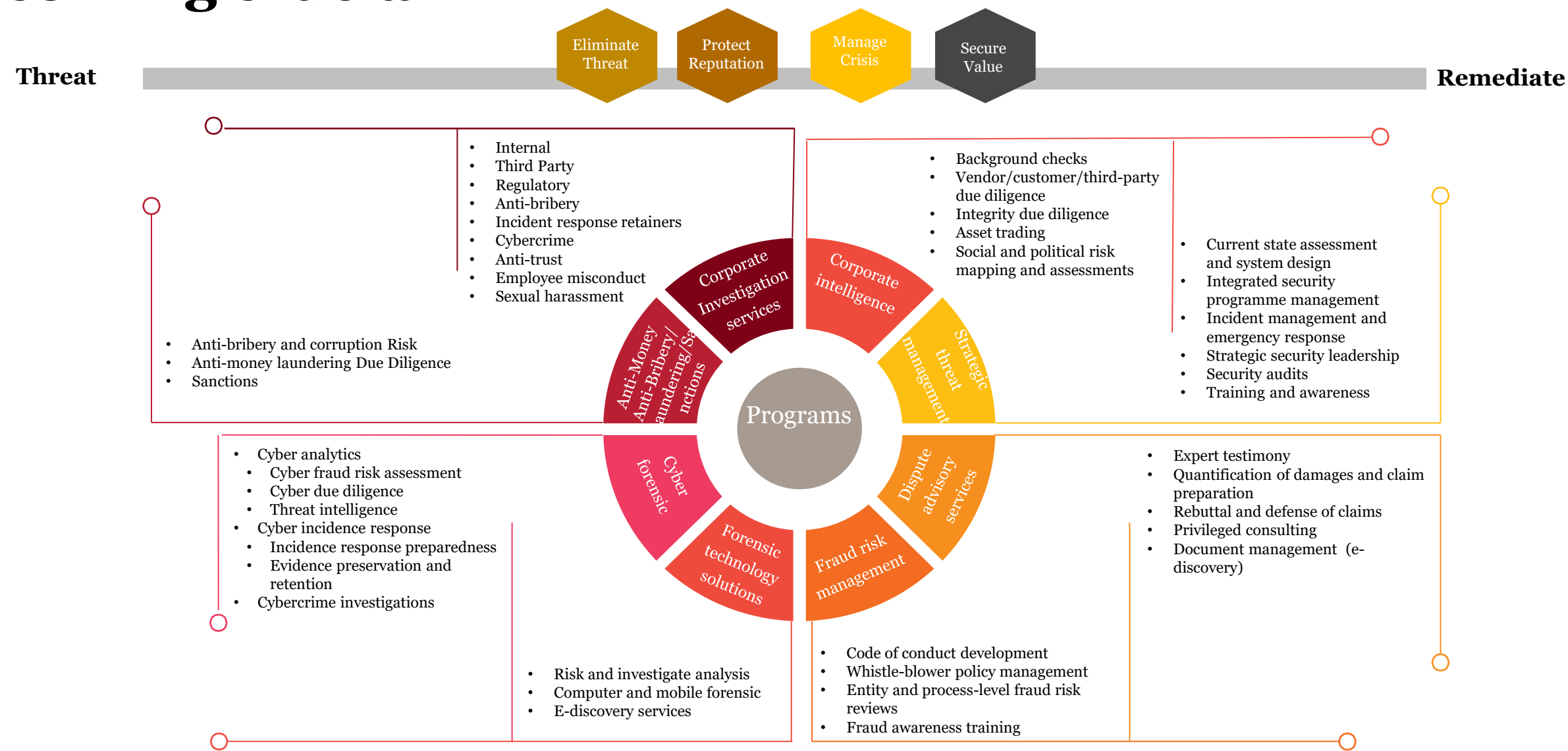


Fraud Risk Management Program: *Why does it “fail”?*

- 1 Failure to capture emerging risks
- 2 Tick-the-box exercise focus
- 3 Unclear and inconsistent risk appetite (cost vs benefits)
- 4 Inadequate information system
- 5 Ineffective monitoring
- 6 Silos
- 7 Unclear consequences if fails
- 8 Crisis management
- 9 Low understanding of fraud risk

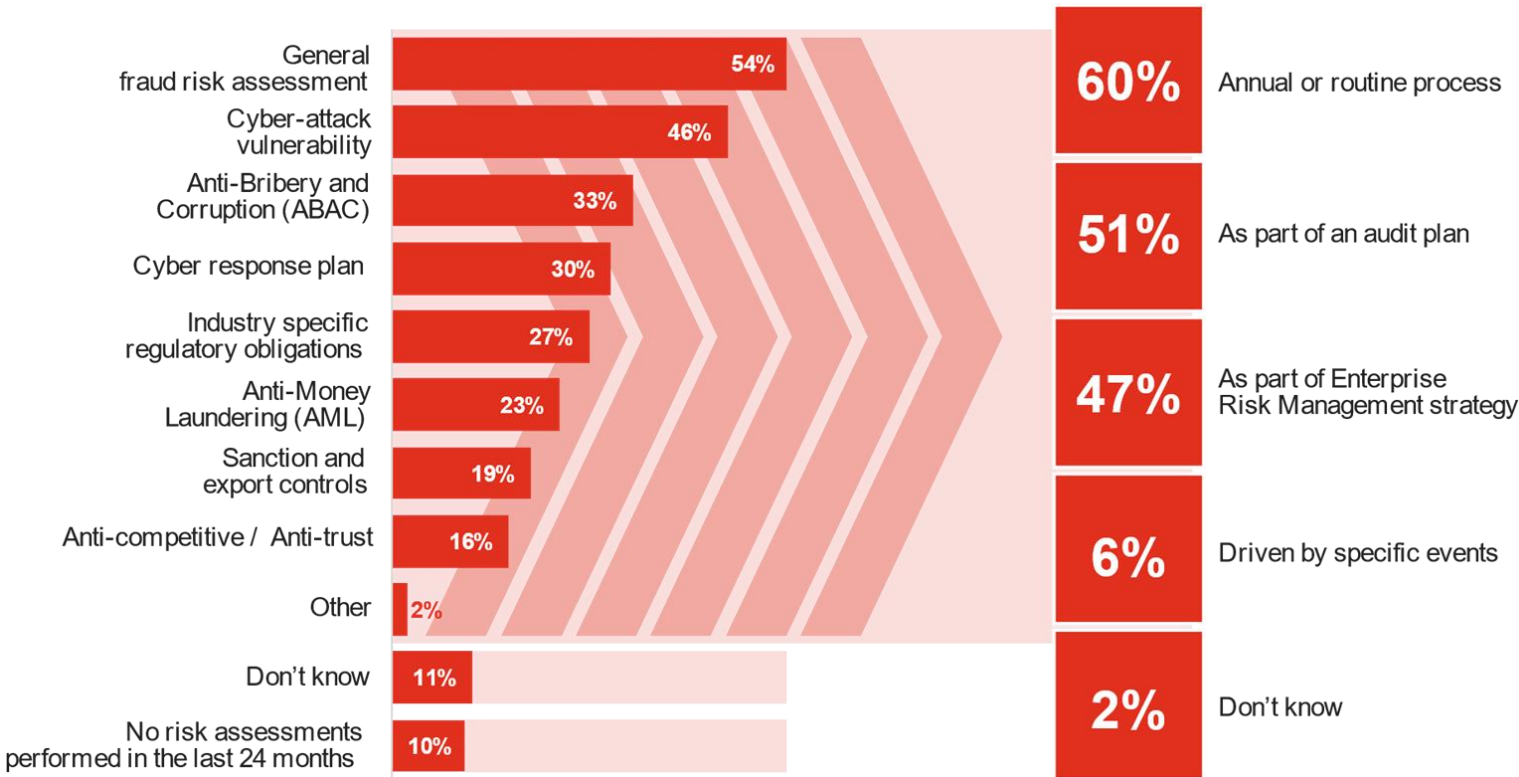


Developing an integrated financial crime management is becoming crucial



Organisations need to perform comprehensive and targeted fraud risk assessments...

Q. Less than half of all organisation have performed targeted risk assessments in the last 2 years



Source: PwC's 2018 Global Economic Crime and Fraud Survey

Q. What anti-fraud controls are the most common in the Asia-Pacific region?

Control	Percent of cases
External audit of financial statements	93%
Code of conduct	88%
Internal audit department	84%
Management certification of financial statements	80%
Management review	78%
External audit of internal controls over financial reporting	75%
Hotline	72%
Independent audit committee	71%
Fraud training for employees	64%
Fraud training for managers/executives	62%
Anti-fraud policy	59%
Employee support programs	50%
Dedicated fraud department, function, or team	50%
Formal fraud risk assessments	45%
Proactive data monitoring/analysis	43%
Surprise audits	36%
Job rotation/mandatory vacation	32%
Rewards for whistleblowers	15%

When to conduct a fraud risk assessment and approach how to deliver

Regular Fraud Risk Assessments

When there is a substantial change in business strategy, entity's structure, functions or activities.

Substantial changes can include:

- changes to service delivery models (such as the introduction of new technologies or the transitioning into the digital delivery of services),
- design and delivery of new programs (such as eligibility payments and grant-based programs);
- or responses to urgent or emergency events (such as natural disasters and COVID pandemic).

Enterprise Risk Management

It is important that fraud risk assessments are considered in the broader context of an entity's enterprise-wide risks. For example, there is often considerable overlap between fraud, physical security and cyber security risks. This overlapping of enterprise risks means that controls and countermeasures may often intersect



Both Global and Indonesian respondents reported similar responses with regards to remediating the incidents

“ How did your organisation remediate the incident?

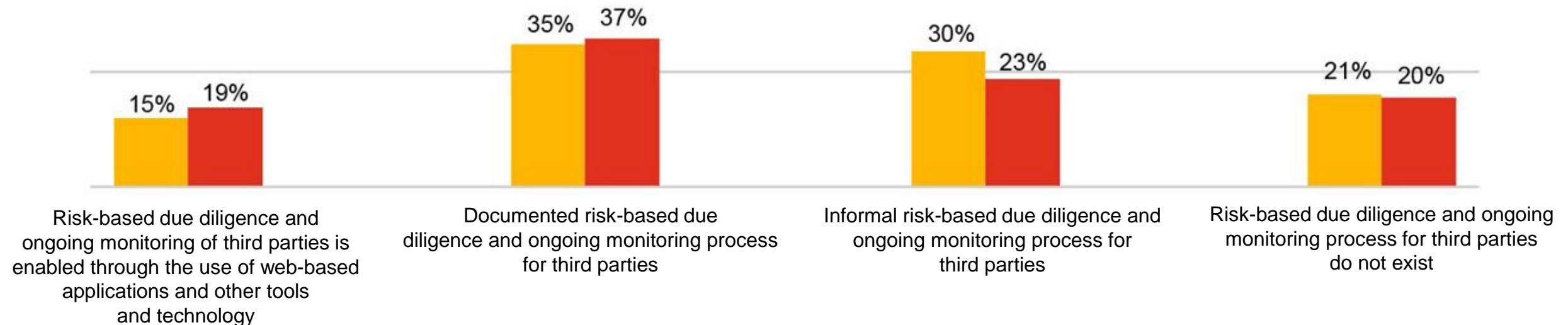


Implemented / enhanced policies and procedures, internal controls, and disciplined / terminated employees are the top three responses

More and more, companies are outsourcing non– core competencies, but these business partners can be fraught with risk – a risk many companies have not formally addressed



Which option best describes the key elements of your overall fraud programme in relation to third party management?



One in five respondents cited that they do not have risk-based due diligence and ongoing monitoring process for third parties.



Managing Fraud Risk in a Connected World - *The extended enterprise*

Do you rely on third party business relationships for the success of your business?

Does your business struggle to manage a large population of global third parties?

Do you know where the risks lie in these relationships?

How do you make sure that the risks are being continuously monitored and managed?

In today's interconnected world, a business operates with an intricate chain of relationships— be it vendors, contractors, customers. These relationships, even in organizations with a strong risk focus, frequently reside at the edge of — or outside — the risk umbrella.



<https://telecom.economictimes.indiatimes.com/tele-talk/the-importance-of-extended-enterprise-risk-management-in-telecom-companies/3330>

Fraud Risk – the general taxonomy

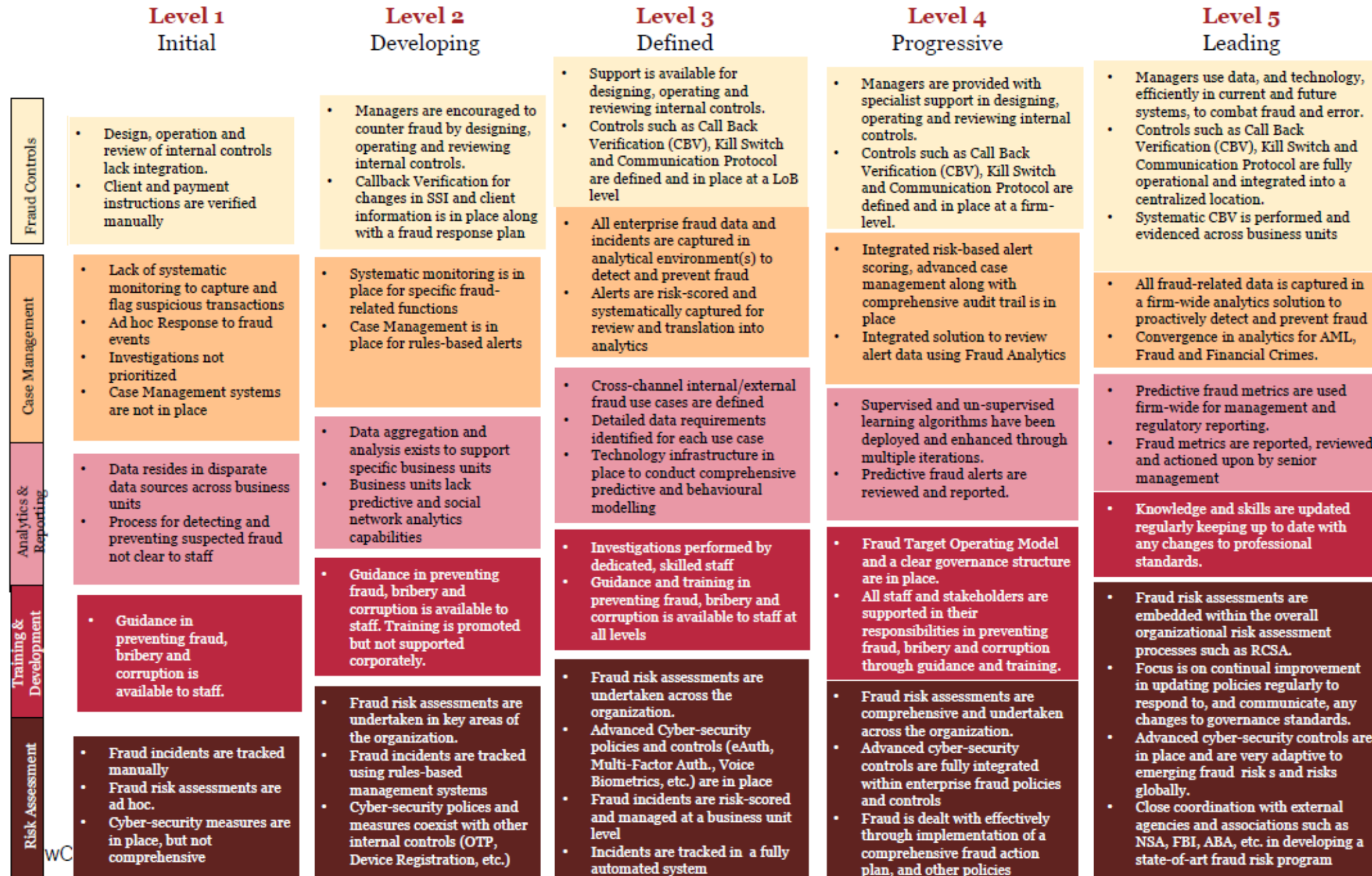
Fraud is an intentional misrepresentation of the truth; wrongful or criminal deception intended to result in financial or personal gain.

The following is our general **Fraud Taxonomy** which is used to classify different types of fraud by perpetrator and vector.

Internal fraud				External fraud			
Financial Statement Fraud	Bribery and Corruption	Asset Misappropriation	Market Abuse	Fraud Ring Attacks Against Customer or Company Accounts	Fraud Committed by Customers	Fraud Committed by Resellers & Agents	Fraud Committed by Vendors & 3rd Parties
Asset/Revenue Overstatement	Illegal Gratuities	Cash & Payments	Insider Trading	New Account/Digital Identity	Credit/Bust Out	Fraudulent Reseller/Agent	Fraudulent Vendors/3 rd Parties
Asset/Revenue Understatement	Conflicts of Interest – Sales Practices - Internal	Credit & Margin	Unauthorized Trading	Account Takeover & Transactions	Payment Fraud	Conflicts of Interest – Sales Practices - External	Vendor Collusion & Corruption
	Conflicts of Interest - Purchases	Inventory & Other Assets	Market Manipulation	Transaction Fraud without Account Takeover	Fraudulent Claims	Revenue Share & Royalty	Vendor Service/Product
	Economic Extortion	Data & Information	Anti-Competitive Behavior	Victim Initiated Transactions	Returns & Refund	Bribery & Corruption - Agents	Vendor Invoice & Discount
	Bribery		Product & Service Misrepresentation		Abuses of Terms & Conditions of Sale		Upstream Supply Chain
					Loyalty & Incentive Program Abuses		Counterfeit Product/Intellectual Property Theft

The maturity scale framework in assessing the anti-fraud strategy

For Illustration only



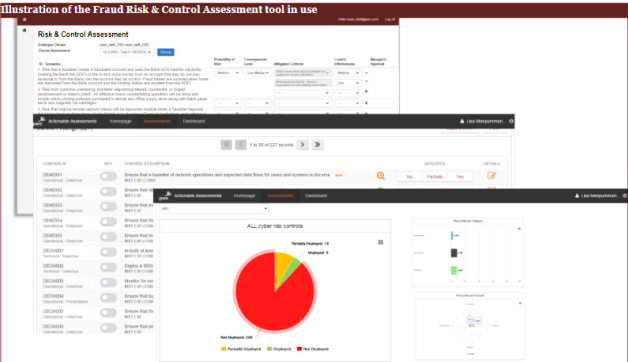
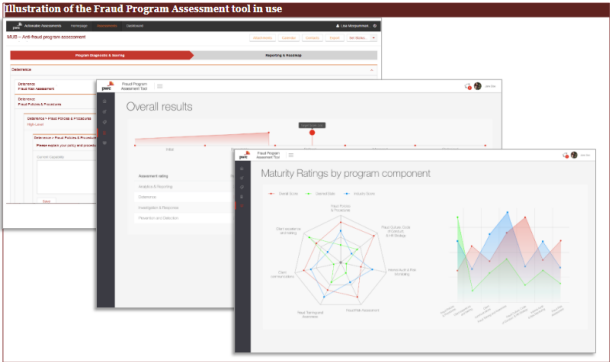
Traditional fraud program and risk assessments

- Collection of information is manual in nature
- Relies on few subject matter experts' knowledge of leading practices for analysis leading to inefficiencies and inconsistencies
- Difficult to compare across business units and over different time periods
- Lacks peer comparison data that provides insights for fraud program optimization across business enablement, losses, costs and customer experience

Fraud Risk Rating												
ID Number	Business Unit	Fraud Risk Category	Fraud Risk Description				Likelihood	Impact	Inherent Risk Rating			
CC-1	Call Center	Unauthorized Activity	Activity on an account that is not at the known or willing direction of the legitimate customer, enabling future fraudulent activity.				4	3	4			
Control Activities Matrix												
ID Number	Fraud Risk Category	Fraud Risk Score	Fraud Risk - Business Unit	Control Category	Control type	Control Name	Control Detail	Control Business Unit	Responsible Person(s)	Design Effectiveness	Friction	Efficiency
CC-1	Unauthorized Activity	4	Call Center	Authentication	KBA - Static	Customer	Owner's name, Contract number, last 4 digits of SSN Exception: If contract number is unknown, full SSN and date of birth.	Call Center		4	2	2
CC-1	Unauthorized Activity	12	Call Center	Authentication	KBA - Static	Power of Attorney (POA)	POA's name, the contract Owner's name, contract number and last 4 digits of Owner's SSN Exception: If contract number is unknown, Owner's full SSN and date of birth.	Call Center		4	2	2
CC-3	Unauthorized Activity	12	Call Center	Authentication	KBA - Static	Producer	Producer's name, Broker Dealer, Customer's Contract Number, and Customer's name Exception: If contract number not known, can provide the Customer's SSN; if the information is not known, the Producer can provide their SSN and their full book of business can be located.	Call Center		4	2	2
CC-4	Unauthorized Activity	12	Call Center	Fraud Detection	Red Flag Monitoring - Manual	Suspicious Activity	Throughout customer / Producer interactions, Customer Service Representatives assess the call for red flags that may be indicative of suspicious activity	Call Center		3	1	4
Fraud Risk Assessment as of Q1 - 2016												
ID Number	Business Unit	Fraud Risk Category	Likelihood	Impact	Inherent Risk Rating	Existing Anti-Fraud Controls		Effectiveness Assessment	Friction	Efficiency	Residual Risks	Fraud Risk Response
CC-1	Call Center	Unauthorized Activity	4	3	4	CC-1 - Authentication KBA - Static Customer CC-2 - Authentication KBA - Static Power of Attorney (POA) CC-3 - Authentication KBA - Static Producer CC-4 Fraud Detection Red Flag Monitoring - Manual Suspicious Activity		4	2	2	4 - High	RR-1: Implement enhanced customer authentication (e.g., voice biometrics, out-of-band authentication) for incoming customer requests.

Digitally enabled fraud program and risk assessment

- Automate the process with PwC's Digital Assessment Tool
- Increase efficiency of information collection through standardized questionnaires
- Increase consistency in the assessment of program and controls by leveraging built-in fraud program and control leading practices
- Gain powerful insights by comparing your program maturity and control ratings across business units, over time and with your peers
- Leverage peer comparison data to optimize your program and controls across business enablement, losses, costs and customer experience business drivers



Enable detection rules

Pre-delivered content : **Examples**

Illustration Only



Vendor &
Service Provider

Frequent changes in the master data of a vendor
Vendor located in high-risk country



Payments

Smurfing on outgoing payments (split invoices)
Irregularities in payments to vendors



Customer

Customer located in high risk country
Bank account and Address in different countries
List Screening (e.g. PEP lists)



Accounting

Accounting documents posted on exceptional dates



Purchasing

Address screening
Conflicts of interest
Irregularities in purchase orders



Invoices

Irregularities in invoices
High-value keyword search



Travel Expenses

Irregularities in Travel Expenses



Compliance

Foreign Corrupt Practices Act
Anti Bribery Act

Cases of red flags to identify suspicious transactions within organizations

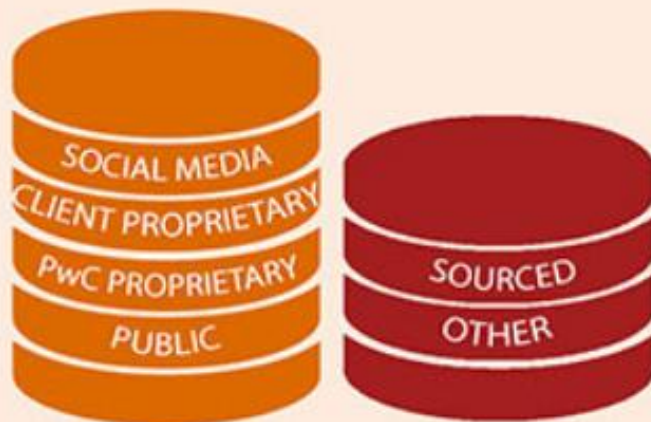
Indicators		Red Flags	Fraud Risk
1	Finance & Accounting	Invoice Transactions – Same Vendor, Invoice, Amount & Posting Date	Overbilling, cost mischarging, shell company, unauthorized supplier
		Vendors paid within zero days [invoice date vs payment date]	Improper payments or payments not inline with agreement
		Supplier with Received Quantity greater than Ordered Quantity	Payments to supplier for additional units of products which are unnecessary
2	Procurement	Invalid address in Supplier Masterfile	Fictitious suppliers, suppliers controlled or linked to employees (former and current), suppliers part of the same group of companies, etc.
		Vendor Set Up and Invoice Transaction Posted by Same Employee	Conflict of interest, improper payments
3	Employee	Personnel number duplication in Employee Masterfile	Ghost employees, employees still paid despite having departed from the company, system login issues, etc.
		Sudden wealth display from employee (e.g pays down debts, or lives beyond his means)	Fraudulent payment received by employee

The use of technology to detect

Manage data to information

Phase 1

Collecting, consolidating and cleaning relevant data.



Increasing amounts of data from new and existing sources, new BI and analytics technologies and processes to create information.

Perform analytics

Phase 2

Applying intelligent techniques to uncover insight from the relevant data.



Predictive, descriptive and prescriptive analytics.

Create visual event output

Phase 3

Converting the data into a more comprehensible and user-friendly format.



Tableau and QlikView, Java Application or event through digital platform.

Harness insight

Phase 4

Applying the insight into more effective decision-making.



Improved risk and compliance management. Increased margins, productivity, growth and innovation.

The use of technology to detect

Key features			
• Lightweight footprint but still generates heavy processing power	• Basic database server and client application to process tens of millions of rows	• Data aggregation from various sources, including databases and flat files (Excel, extracts)	• Rapid development cycles facilitate iterative prototyping of screens and analytics

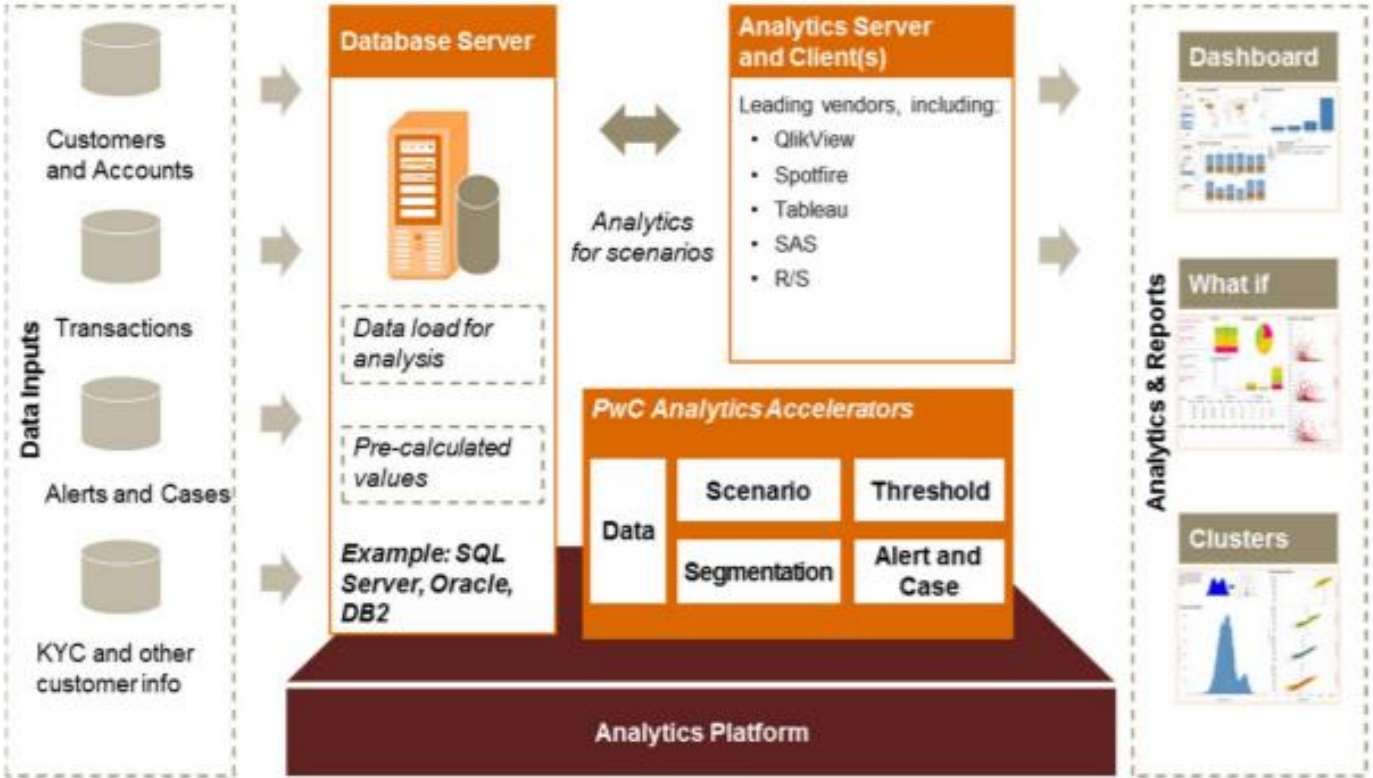
Leading practices and PwC Accelerators

Dashboards	Segmentation	Scenario Typology	Thresholds	Risk Scoring
• Dashboards to track financial crime risk KPIs • Heat maps to identify higher risk areas	• Segmentation cluster tests • Segmentation dashboards with KPIs to monitor model metrics • Outlier dashboards	• Scenario library for parallel run or independent testing • Typology analytics to determine fit for purpose	• Statistics and metrics dashboards • What-if and scenario analytics for hypothesis testing	• Statistical models to predict risk of alerts or cases

A new platform for a new environment

Built relatively easily despite their advanced capabilities, the next wave of data analytics programmes can provide a holistic — yet intuitive — view of risks across businesses and geographies.

Indicative “next wave” analytics sandbox



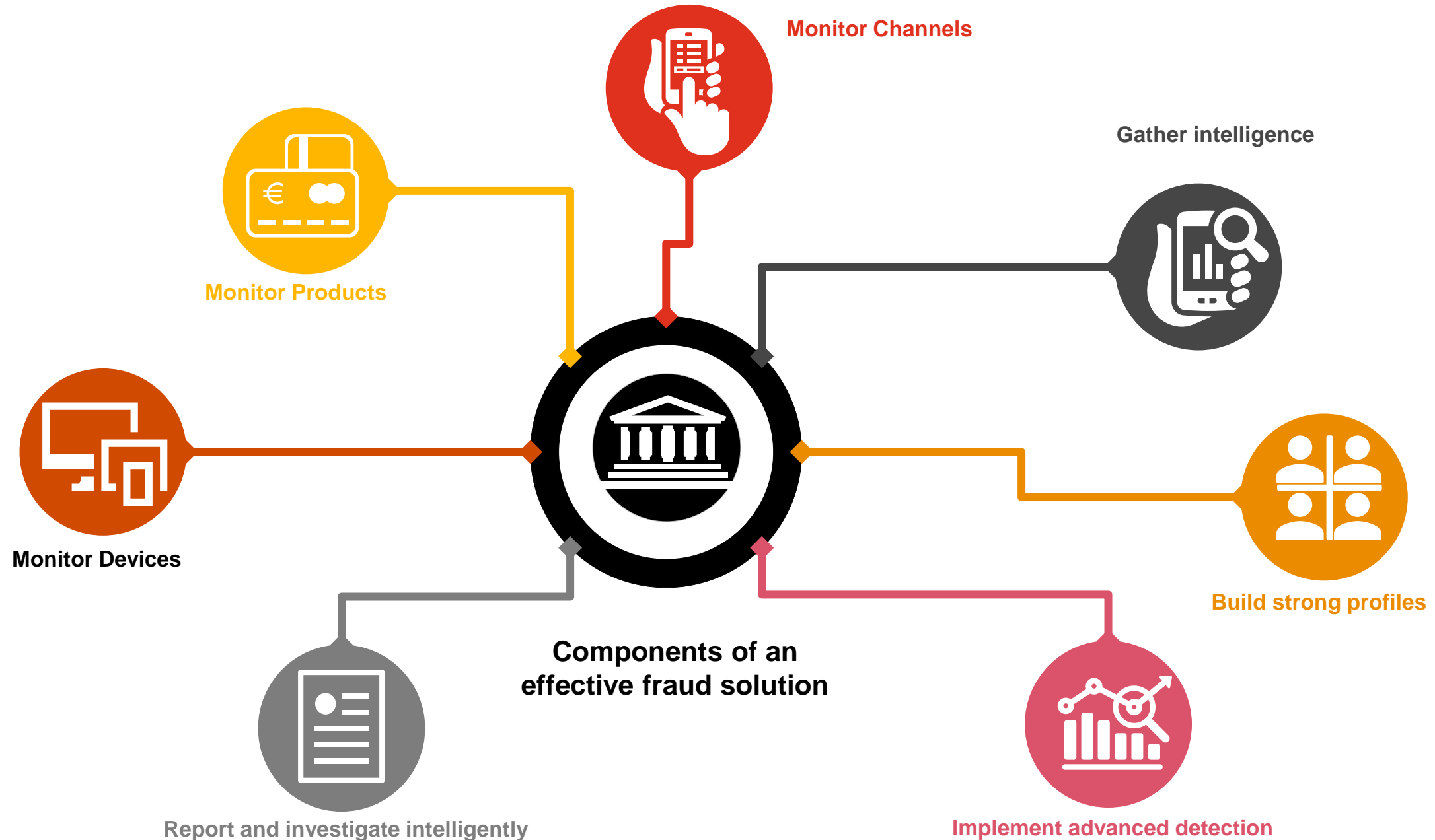
Key features			
• Lightweight footprint but still generates heavy processing power	• Basic database server and client application to process tens of millions of rows	• Data aggregation from various sources, including databases and flat files (Excel, extracts)	• Rapid development cycles facilitate iterative prototyping of screens and analytics

Leading practices and PwC Accelerators

Dashboards	Segmentation	Scenario Typology	Thresholds	Risk Scoring
• Dashboards to track financial crime risk KPIs • Heat maps to identify higher risk areas	• Segmentation cluster tests • Segmentation dashboards with KPIs to monitor model metrics • Outlier dashboards	• Scenario library for parallel run or independent testing • Typology analytics to determine fit for purpose	• Statistics and metrics dashboards • What-if and scenario analytics for hypothesis testing	• Statistical models to predict risk of alerts or cases

Technology for Fraud detection and prevention

Given the plethora of fraud technology offerings currently available, banks need to identify the most effective combination for solving specific problems



Technology for Fraud detection and prevention: Products



Banks need to monitor the products operated by them to reduce risks of fraud and ensure monitoring from all perspectives

Anomaly detection

Monitor product behaviour over time to identify unintended use or anomalous activity

Product evaluation: Use of natural language

Make use of ML models utilising natural language processing to analyse product features and programmatically identify weaknesses



Automated risk assessment

Analyse changes in product Terms & Conditions and assess the inherent and residual risk exposure

Real-time contextual risk assessments

Continuously update fraud risk assessment with risk indicators identified from transaction behaviour

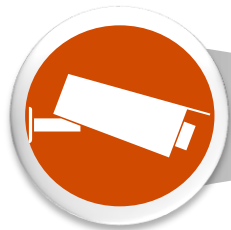
Technology for Fraud detection and prevention: Transaction processing and Accounting Systems

Machine learning can be leveraged for tracking and monitoring transaction and accounting systems for fraud indicators. Often these are the target of internal / employee conducted fraud



Transaction processing and accounting systems are susceptible to fraud via:

- Rogue employees make entries into General Ledgers, journals, customer details etc.
- Fake identification details used to create fraudulent accounts and transactions
- Malicious code implementations which utilise inherent vulnerabilities in certain systems allowing for unauthorized deployments



Employee technology surveillance

Banks, have never been more vulnerable to catastrophic losses caused by dishonest employees and employees duped by dishonest third parties. Thereby, necessitating the need to monitor employee digital footprint and traffic.

Banks should compare traffic and employees within similar segments to check for anomalous activity



Background checks

Automate background checks and verify employee and customer background data using cognitive RPA, thereby updating customer and employee risk over time



Code changes

Identify unauthorized system and code base modifications which could compromise the system and increase fraud susceptibility.

Systems should be continuously monitored for any modifications

Track firmware identifiers, code/utility versions and audit logs and automated regular assess systems for unauthorized code changes

A Pulse Check

How well do you understand your fraud risk?

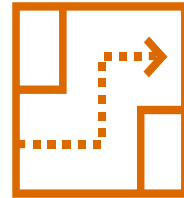
Does your digital business build trust?

Where do you place your investment against fraud?



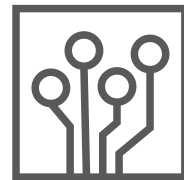
People

- 41% of global and 45% of Indonesian respondents said they have received formal fraud training, but only 18% (ID: 25%) said that mandatory training is tracked.
- 11% of global and 8% of Indonesian respondents have received no fraud training or communication at all.
- 9% of global and 16% of Indonesian respondents said that they lack sufficient expertise / resources in digital skills.



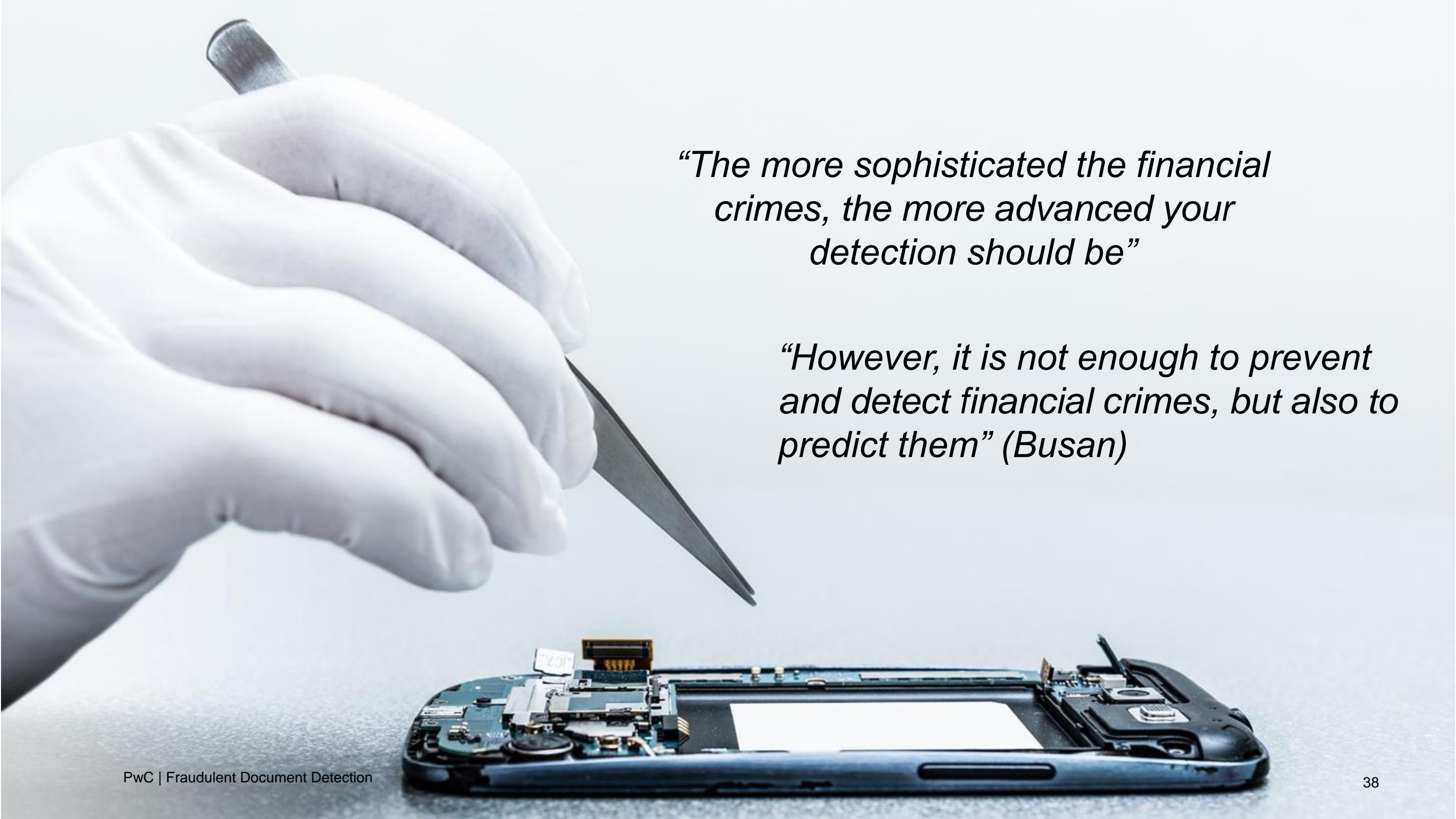
Process

Compliance programs must be risk-based, appropriately sized, and categorised between operational frauds and situational frauds. **Operational frauds** are mainly activity-driven and transactional in nature. The methods are monitoring of suspicious activity, AI and data analytics. **Situational frauds** make the accomplishment of programmatic ROI difficult. These are mostly behaviour-driven, such as corruption and accounting frauds. The most effective tools to combat frauds are culture and people-based, including due diligence, monitoring and investigations.



Technology

Technology requires a nuanced response and finding the right balance is challenging. Start by seeking to extract optimal value from the technology you already have, and measure its effectiveness. This can be a starting point for making your case to invest in new tools.

A close-up photograph showing a hand wearing a white nitrile glove. The hand is holding a thin, metal pick tool, which is positioned to lift a small, rectangular electronic component from the internal circuitry of a disassembled smartphone. The phone's internal components, including the battery, logic board, and various connectors, are visible. The background is a plain, light-colored surface.

“The more sophisticated the financial crimes, the more advanced your detection should be”

“However, it is not enough to prevent and detect financial crimes, but also to predict them” (Busan)

Thank you

Budi Santoso SE, Ak, MForAccy, PGCS, CA, CFE, CPA (Aust.)

Director Risk Consulting & Financial Crime Territory Leader

Email: budi.santoso@pwc.com

Mobile: +62 813 9915 4114

pwc.com



Yayasan Pendidikan Internal Audit
L'Avenue Office Tower Lt.17 F
Jl. Raya Pasar Minggu Kav. 16, Pancoran-Jakarta Selatan
Telp: 021-7985555
(Mitha) 0812-1912-1158, Hary (0812-1001-7321), Yasmin (0878-7218-3943)
Email: marketingypia@gmail.com, registrasi.snia@ypia.co.id
website: www.ypia.co.id