Hari Setianto, MSocSc, CIA, CCSA, CFSA, CGAP, CRMA, CRMP, GRCP

President, IIA Indonesia

STAN, Birmingham University

Pekerjaan - saat ini

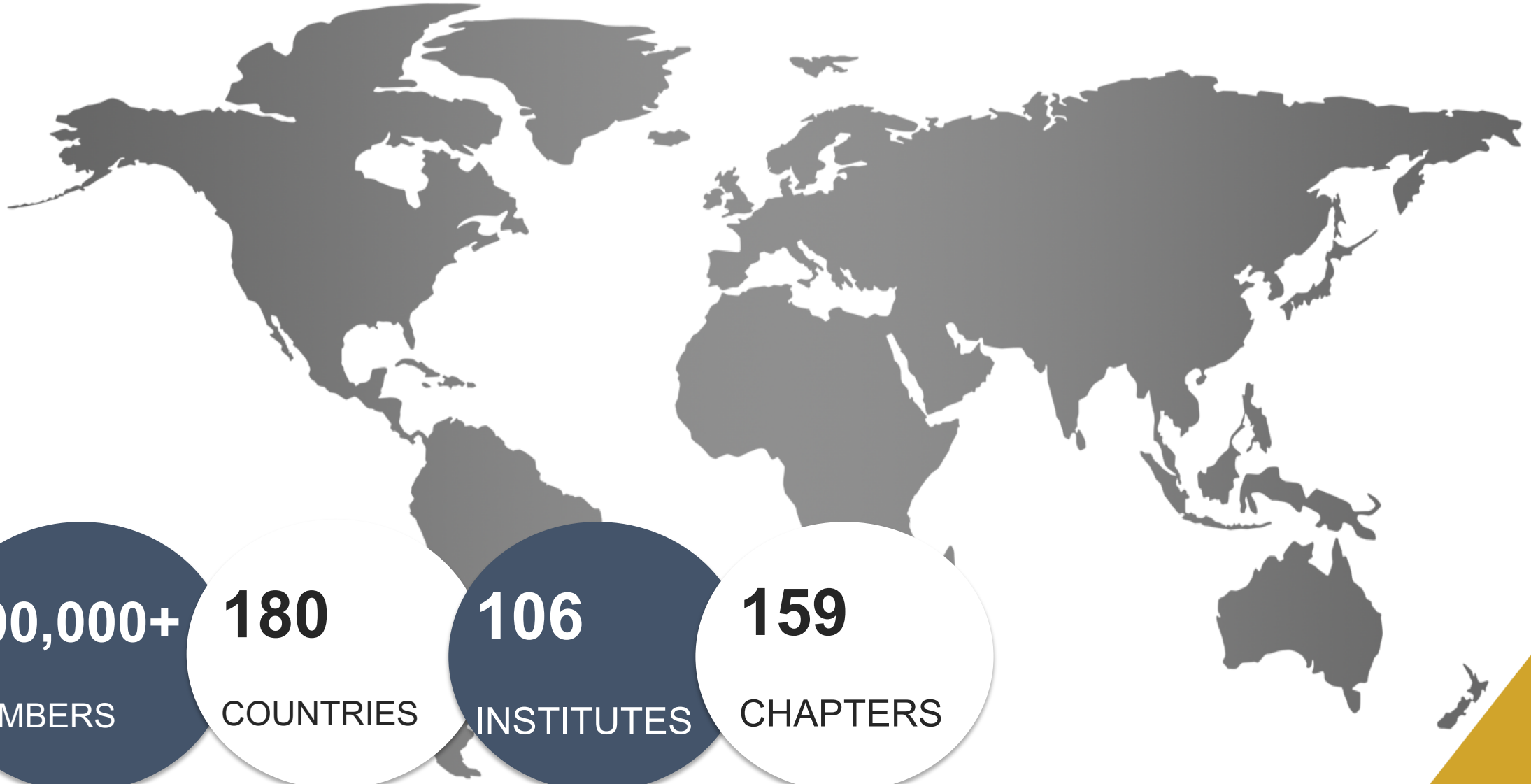
- President IIA Indonesia
- Direktur Perusahaan Tbk (Asuransi)
- Komisaris Independen Tbk (Industri Kreatif)
- Komite Audit IBST – Sinar Mas Group (Telco)
- Advisor PT. Centria Integrity Advisory (Services)

Pekerjaan - sebelumnya

- Direktur Investasi dan Keuangan PT. ASABRI (Persero)
- Direktur Akademis YPIA
- Direktur Utama PT. Bina Audita
- Komite Audit - UFJI (Subsidiary Bank BTMU)
- Komite Audit - Lotte Chemical (Lotte group)
- Komite Risiko - PT. ASABRI
- Ketua Dewan Sertifikasi QIA
- BPKP

The Institute of Internal Auditors

Signatory of: PRI Principles for Responsible Investment



200,000+ MEMBERS

180 COUNTRIES

106 INSTITUTES

159 CHAPTERS

IIA Indonesia

Signatory of:

PRI Principles for Responsible Investment

Our Mission:
To advance the profession and practice of internal auditing in Indonesia

Our Vision:
Internal audit professionals are universally recognized as indispensable to effective governance, risk management, and control

3,465

Active Member

World's IIA highest increase 49% since Jul 2018 – Jul 2019

282

CIA Holder

Or 0,0001064%
of national population

CIA CERTIFIED INTERNAL AUDITOR

CRMA CERTIFICATION IN RISK MANAGEMENT ASSURANCE

CCSA CERTIFICATION IN CONTROL SELF-ASSESSMENT

CFSA CERTIFIED FINANCIAL SERVICES AUDITOR

CGAP CERTIFIED GOVERNMENT AUDITING PROFESSIONAL

QIAL Qualification in Internal Audit Leadership

International Professional Practice Framework

Signatory of:

PRI Principles for Responsible Investment

Internal audit sebelum ‘modern’ – IIA (1941)

- 4500 – 1940s

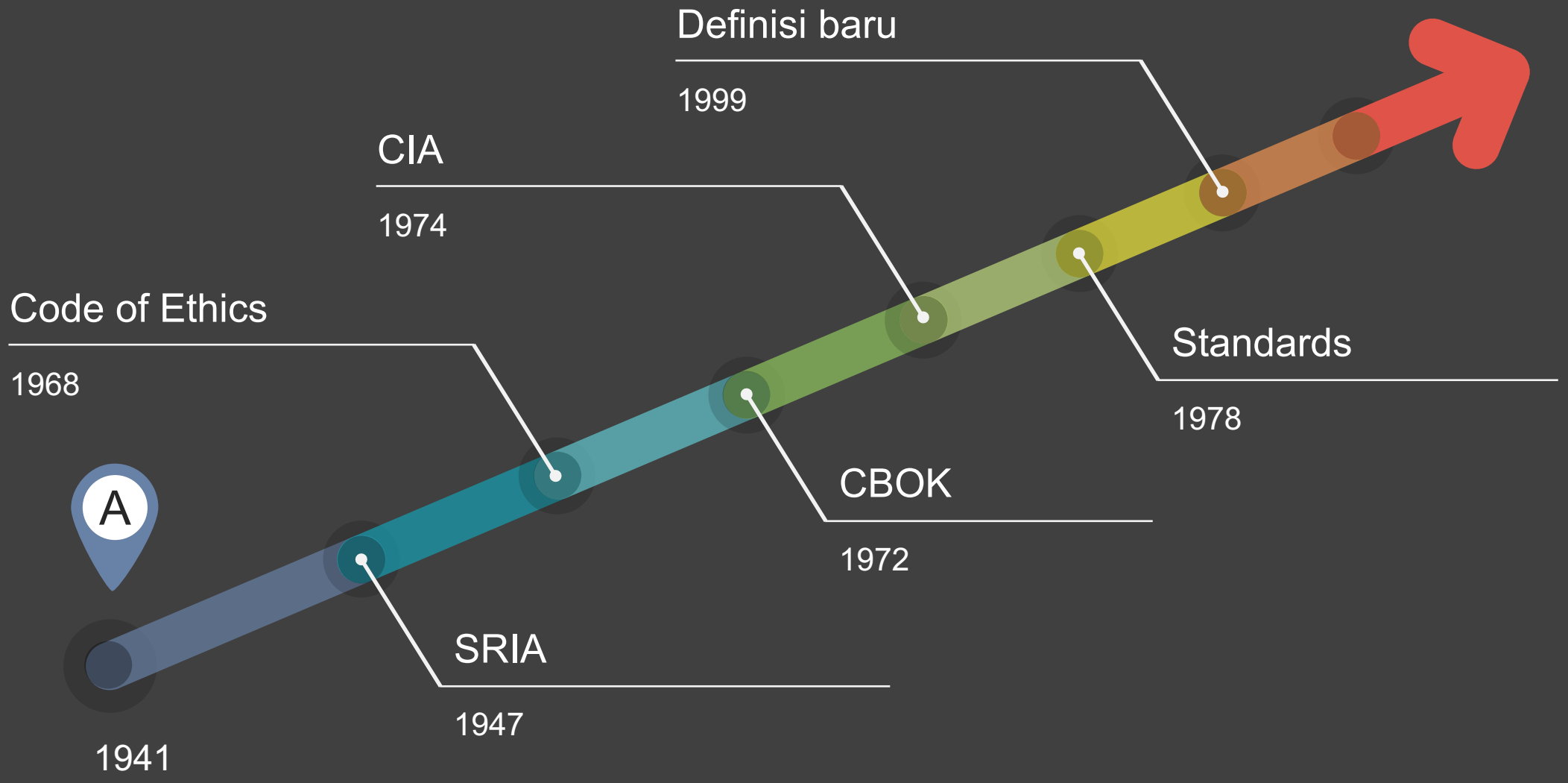
Sejak 4500 SM
Babilonia – Hamurabi
Kalifah Omar bin Khatab

2nd oldest profession
Chinese emperors

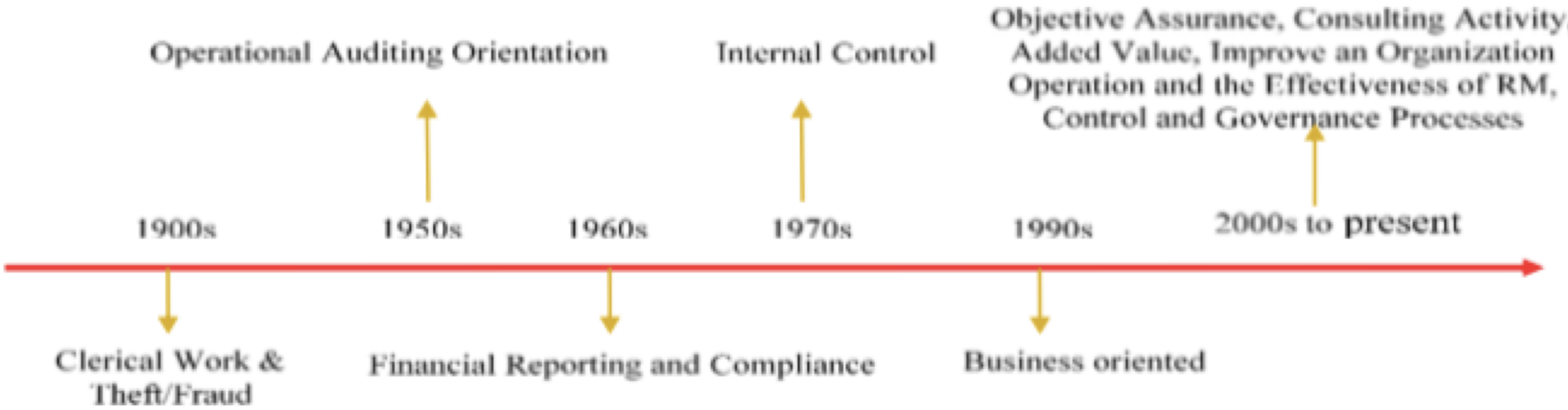
Fokus pada error,
fraud, theft, repetition

Great Depression – crash
Verification of financial records
Aids to Accounting/External auditor

Milestones profesi sampai 1999



Signatory of:
PRI Principles for Responsible Investment



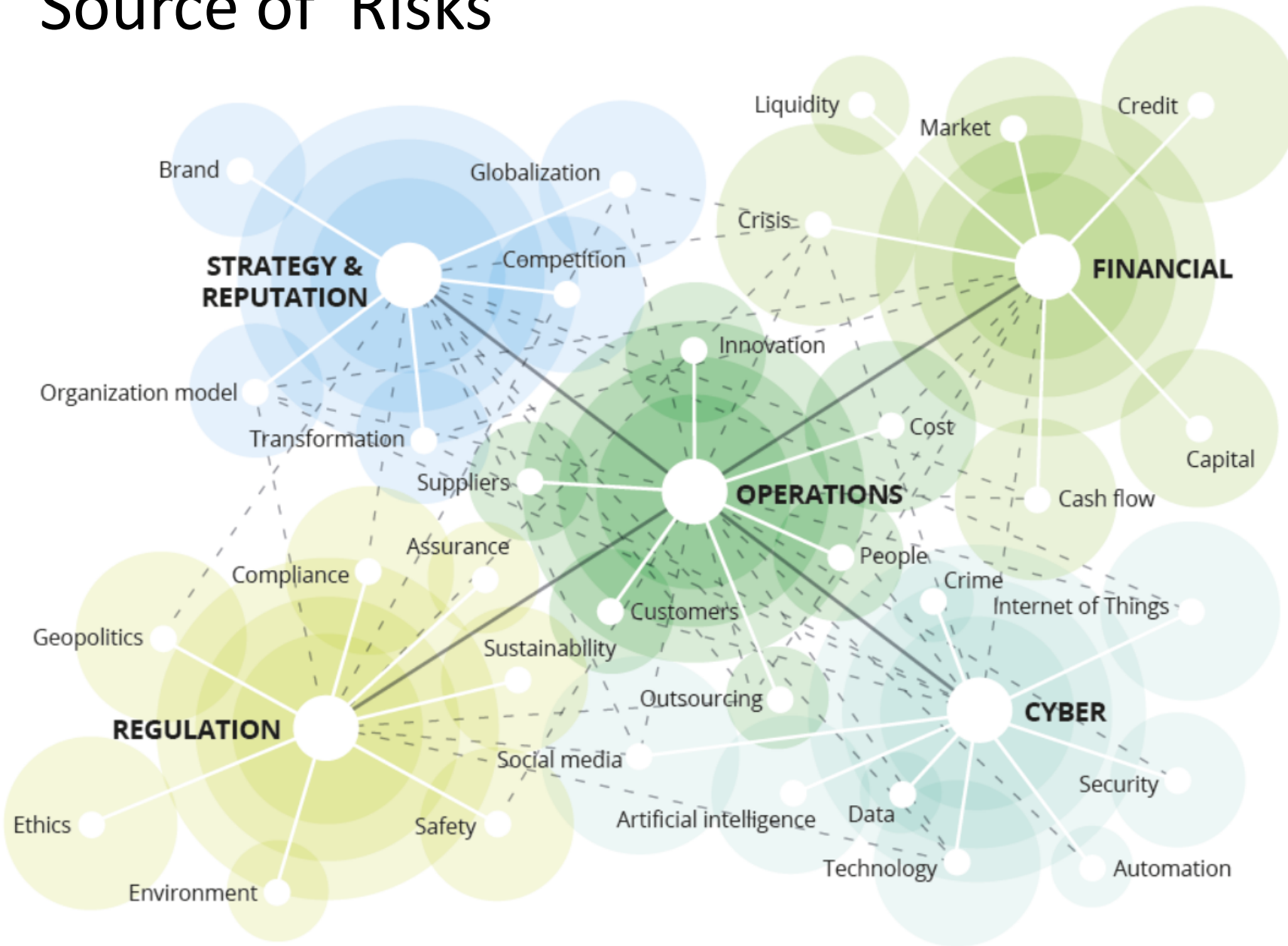
KEY MILESTONES

IA Set to Emerge as a Profession
1941-Formation of the IIA
1947-Issued the Statement of the Responsibilities of the IA (Revised in 1957, 1971, 1976, 1981, and 1990)

IA Began as a Profession
1968-Issued the Code of Ethics
1972-Published the CBOK
1974-Created the Professional Certification for IA
1976-Formation of the IIA Research Foundation
1977-Created a Professional Magazine for IA
1978-Issued the Standards

Advances & Strengthening of IA Profession
1999-Issued Current Definition of IA
2000-Revised the Code of Ethics
2002-Issued a New IA Standards
2006-The Standards has been Recognized Globally
2007-Issued a New IA Framework- the IPPF*
2015-Issued a New Enhancement of the IPPF
*The IPPF is subject to update once in every 2 years

Source of Risks



Organisasi menghadapi meningkatnya ketidakpastian dari berbagai sumber

Source: Internal Audit 3.0 (2018) Deloitte

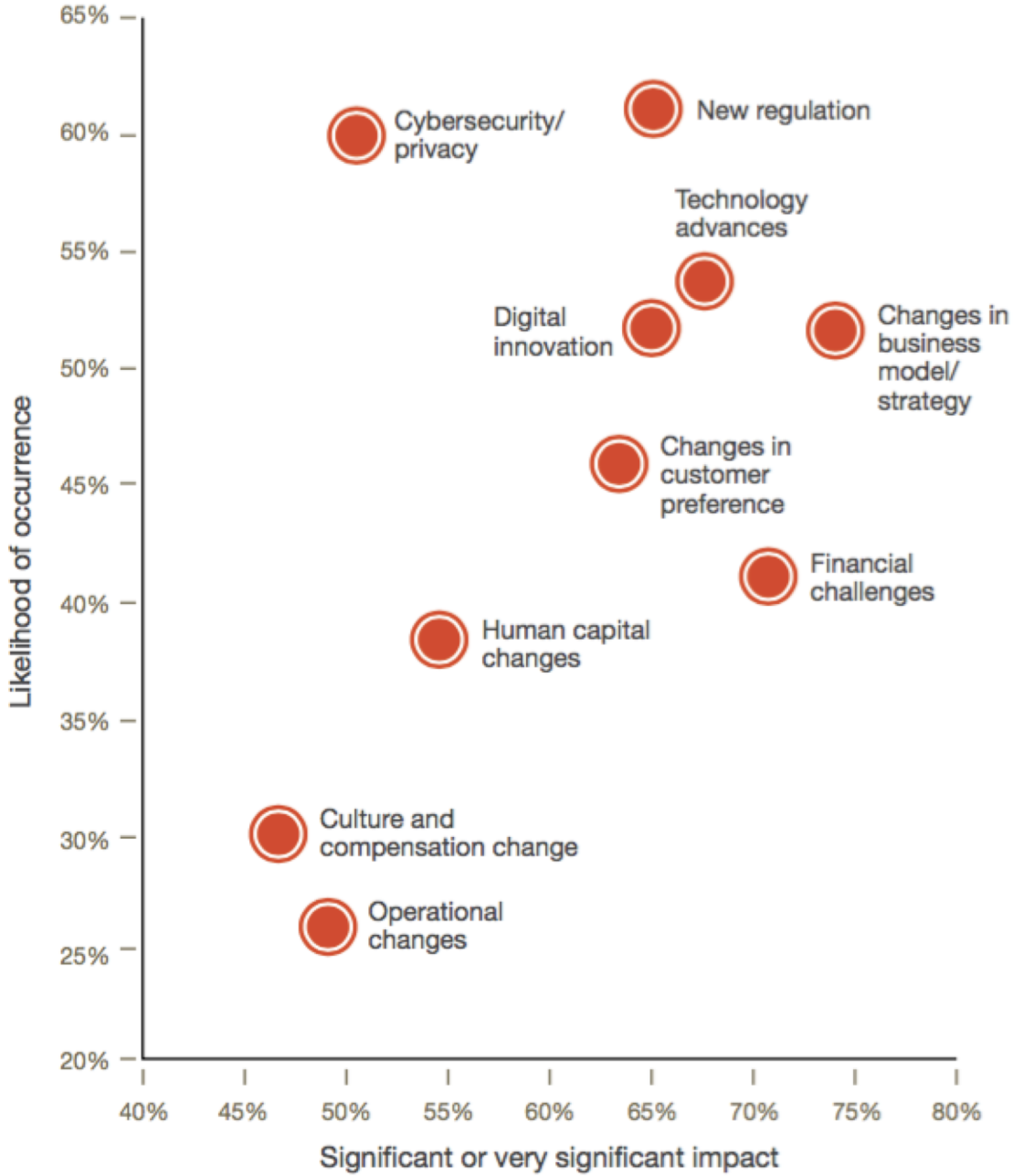


Figure 2: Top five disruptions

pwc

CYBERSECURITY: The growing sophistication and variety of cyberattacks continue to wreak havoc on organizations' brands and reputations, often resulting in disastrous financial impacts. This risk examines whether organizations are sufficiently prepared to manage cyber threats that could cause disruption and reputational harm.

DATA PROTECTION: Beyond regulatory compliance, data privacy concerns are growing as investors and the general public demand greater control and increased security over personal data. This risk examines how organizations protect sensitive data in their care.

REGULATORY CHANGE: A variety of regulatory issues, from tariffs to new data privacy laws, drive interest in this risk. This risk examines the challenges organizations face in a dynamic and sometimes volatile regulatory environment.

BUSINESS CONTINUITY/CRISIS RESPONSE: Organizations face significant existential challenges, from cyber breaches and natural disasters to reputational scandals and succession planning. This risk examines organizations' abilities to prepare, react, respond, and recover.

DATA AND NEW TECHNOLOGY: Organizations face significant disruption driven by the accelerating pace of technology and the growing ease of mass data collection. Consider traditional versus born-digital business models. This risk examines organizations' abilities to leverage data and new technology to thrive in the fourth industrial revolution.

THIRD PARTY: Increasing reliance on third parties for services, especially around IT, demands greater oversight and improved processes. This risk examines organizations' abilities to select and monitor third-party contracts.

TALENT MANAGEMENT: Historically low unemployment, a growing gig economy, and the continuing impact of digitalization are redefining how work gets done. This risk examines challenges organizations face in identifying, acquiring, and retaining the right talent to achieve their objectives.

CULTURE: "The way things get done around here" has been at the core of a number of corporate scandals. This risk examines whether organizations understand, monitor, and manage the tone, incentives, and actions that drive behavior.

BOARD INFORMATION: As regulators, investors, and the public demand stronger board oversight, boards place greater reliance on the information they are provided for decision-making. This risk examines whether boards are receiving complete, timely, transparent, accurate, and relevant information.

DATA ETHICS: Sophistication of the collection, analysis, and use of data is expanding exponentially, complicated by artificial intelligence. This risk examines organizational conduct and the potential associated reputational and financial damages for failure to establish proper data governance.

SUSTAINABILITY: The growth of environmental, social, and governance (ESG) awareness increasingly influences organizational decision-making. This risk examines organizations' abilities to establish strategies to address long-term sustainability issues.

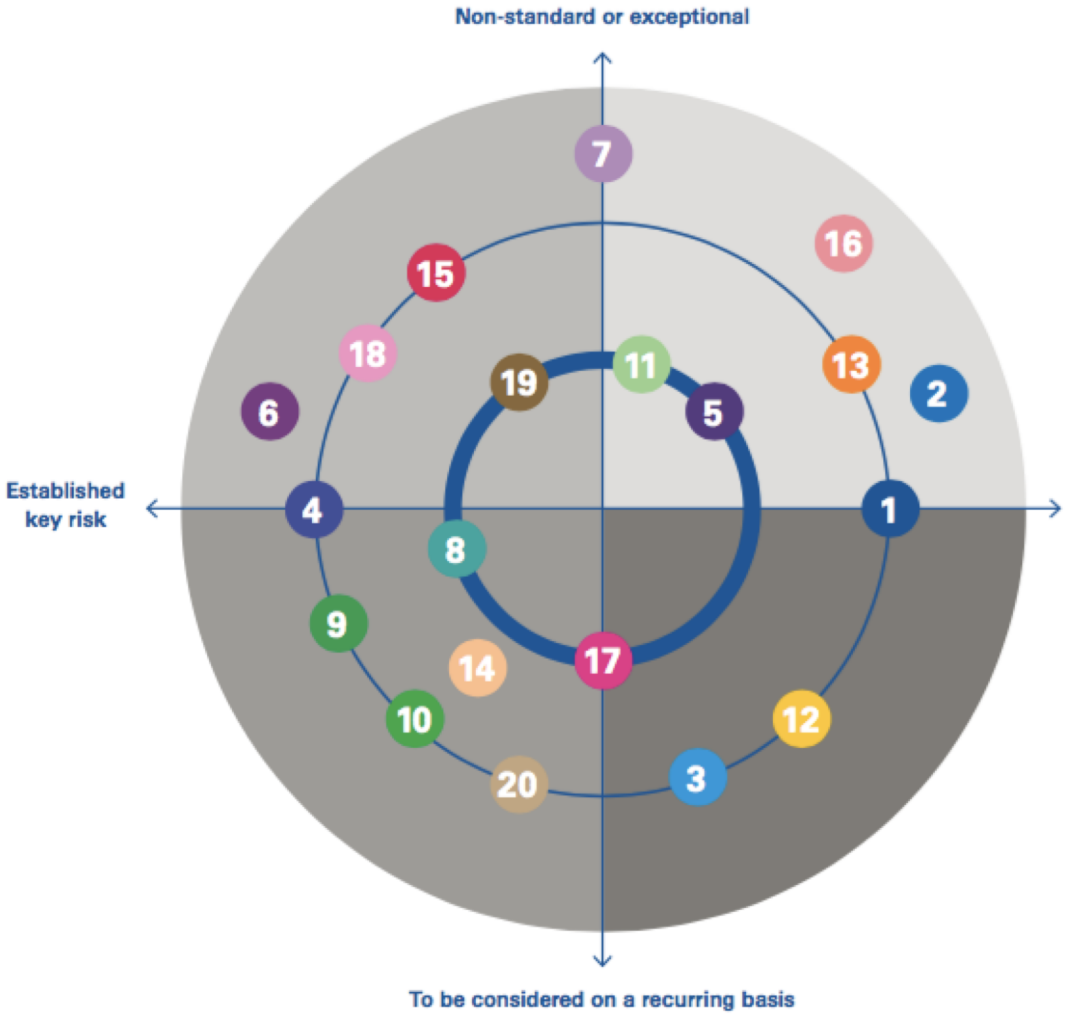
2020

1. Cybersecurity & data privacy: rising expectations of internal audit
2. The increasing regulatory burden
3. Digitalisation & business model disruption
4. Looking beyond third parties
5. Business resilience, brand value & reputation
6. Financial risks: from low returns to rising debt
7. Geopolitical instability & the macroeconomy
8. Human capital: the organisation of the future
9. Governance, ethics & culture: the exemplary organisation
10. Climate change: risk vs opportunity

RISK	CURRENT	FUTURE	CHANGE
CYBERSECURITY	86%	90%	+4 ↑
DATA PROTECTION	78%	85%	+7 ↑
REGULATORY CHANGE	66%	64%	-2 ↓
BUSINESS CONTINUITY	65%	67%	+2 ↑
DATA AND NEW TECHNOLOGY	64%	82%	+18 ↑
THIRD PARTY	60%	66%	+6 ↑
TALENT MANAGEMENT	58%	65%	+7 ↑
CULTURE	57%	58%	+1 ↑
BOARD INFORMATION	54%	51%	-3 ↓
DATA ETHICS	51%	66%	+15 ↑
SUSTAINABILITY (ESG)	30%	45%	+15 ↑

Figure 10: *Risk Relevance for 11 Risks*

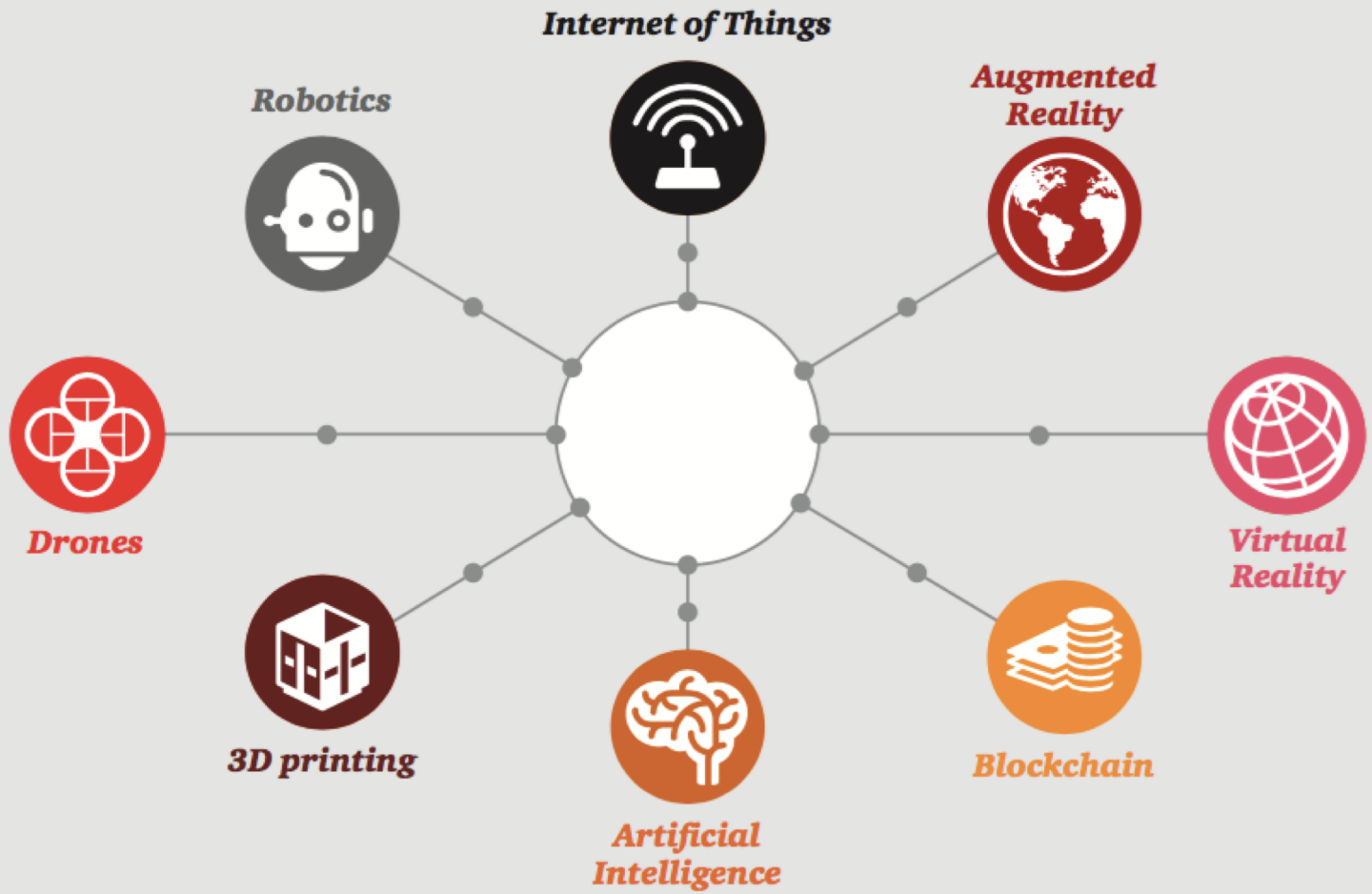
Top 20 risks before 2020



1. Digitalization, Industry 4.0 & the Internet of Things
2. Cloud computing
3. EU General Data Protection Regulation (EU-GDPR)
4. Cyber security
5. Business continuity and crisis response
6. Net working capital management
7. Non-GAAP financial measures
8. Data analytics and mass data usage
9. Treasury management
10. Organization-wide initiatives/projects
11. Effective talent management
12. Trade environment and customs
13. Alignment of operations to organization's strategy and objectives
14. Compliance Management Systems (CMS), auditing organization culture and ethics
15. Effectiveness and efficiency of operational processes
16. Mergers, acquisitions, and divestitures
17. Integrated enterprise risk management and monitoring
18. IT governance
19. Outsourcing and managing third-party relationships
20. Tax compliance

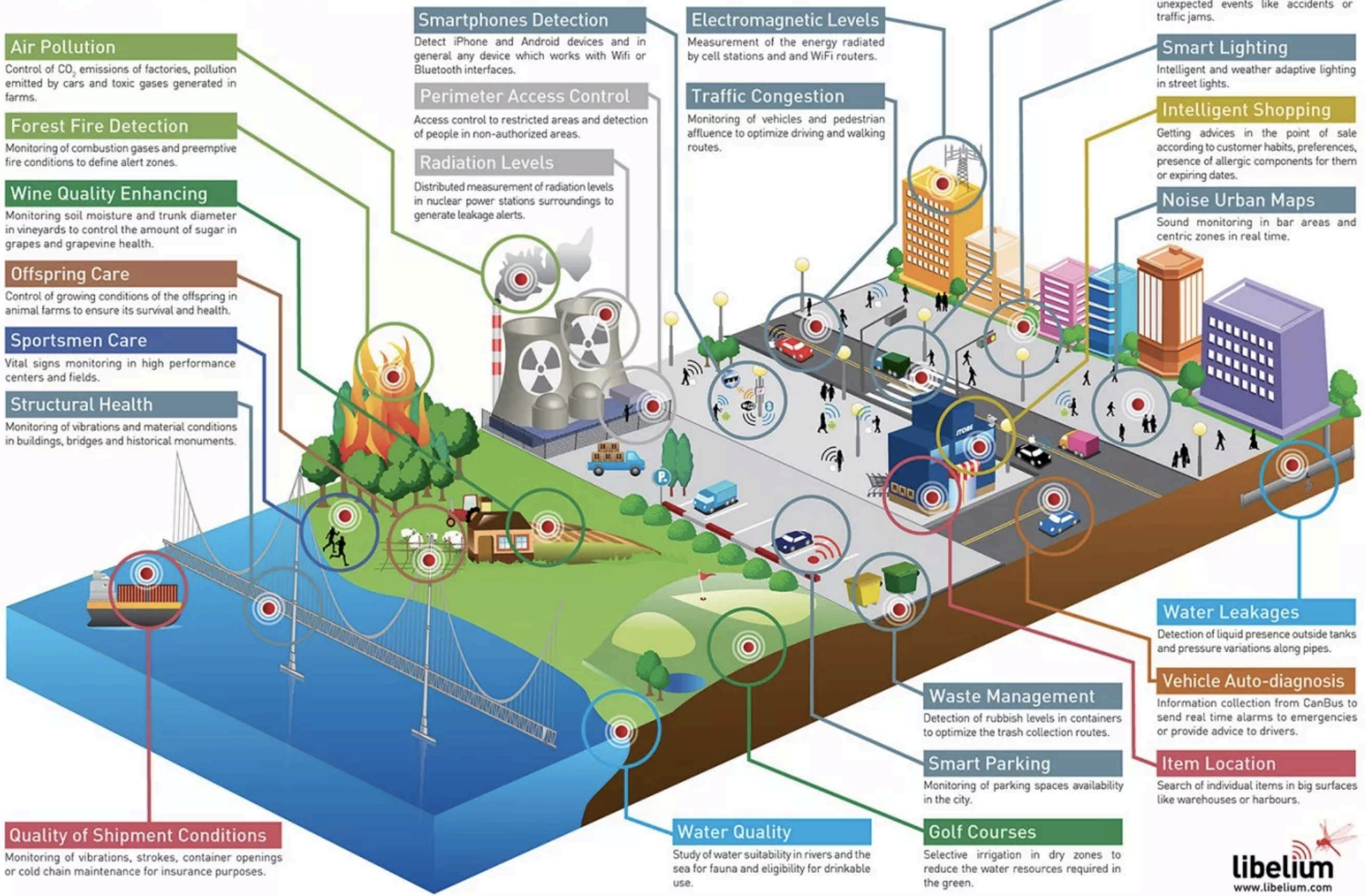
Sumber: '20 Key Risks' (KPMG, 2018)

Figure 1: The essential eight emerging technologies



Source: PwC, "How can boards tackle the Essential Eight and other emerging technologies?", June 2017

Libelium Smart World



Air Pollution
Control of CO_2 emissions of factories, pollution emitted by cars and toxic gases generated in farms.

Forest Fire Detection
Monitoring of combustion gases and preemptive fire conditions to define alert zones.

Wine Quality Enhancing
Monitoring soil moisture and trunk diameter in vineyards to control the amount of sugar in grapes and grapevine health.

Offspring Care
Control of growing conditions of the offspring in animal farms to ensure its survival and health.

Sportsmen Care
Vital signs monitoring in high performance centers and fields.

Structural Health
Monitoring of vibrations and material conditions in buildings, bridges and historical monuments.

Quality of Shipment Conditions
Monitoring of vibrations, strokes, container openings or cold chain maintenance for insurance purposes.

Smartphones Detection
Detect iPhone and Android devices and in general any device which works with Wifi or Bluetooth interfaces.

Perimeter Access Control
Access control to restricted areas and detection of people in non-authorized areas.

Radiation Levels
Distributed measurement of radiation levels in nuclear power stations surroundings to generate leakage alerts.

Electromagnetic Levels
Measurement of the energy radiated by cell stations and and WiFi routers.

Traffic Congestion
Monitoring of vehicles and pedestrian affluence to optimize driving and walking routes.

Water Quality
Study of water suitability in rivers and the sea for fauna and eligibility for drinkable use.

Smart Roads
Warning messages and diversions according to climate conditions and unexpected events like accidents or traffic jams.

Smart Lighting
Intelligent and weather adaptive lighting in street lights.

Intelligent Shopping
Getting advices in the point of sale according to customer habits, preferences, presence of allergic components for them or expiring dates.

Noise Urban Maps
Sound monitoring in bar areas and centric zones in real time.

Water Leakages
Detection of liquid presence outside tanks and pressure variations along pipes.

Vehicle Auto-diagnosis
Information collection from CanBus to send real time alarms to emergencies or provide advice to drivers.

Item Location
Search of individual items in big surfaces like warehouses or harbours.

Waste Management
Detection of rubbish levels in containers to optimize the trash collection routes.

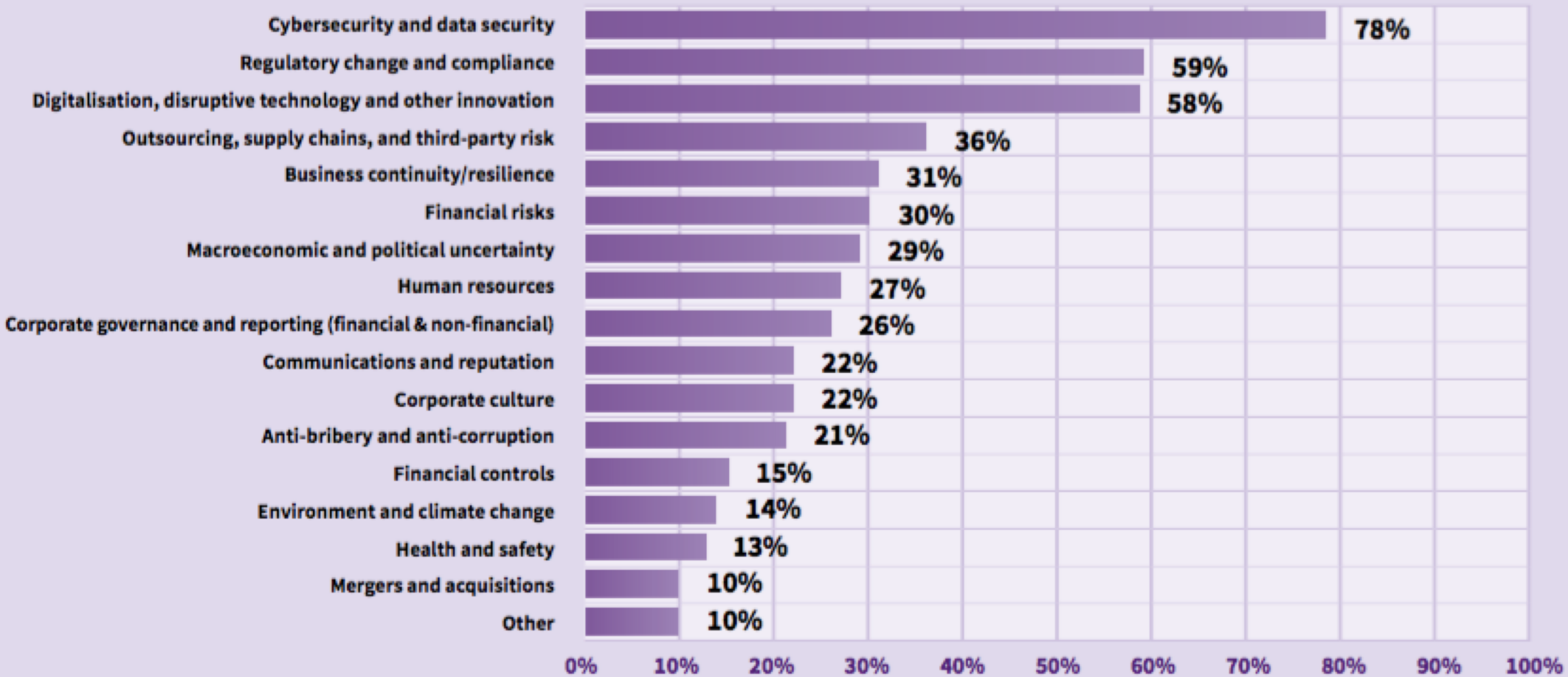
Smart Parking
Monitoring of parking spaces availability in the city.

Golf Courses
Selective irrigation in dry zones to reduce the water resources required in the green.

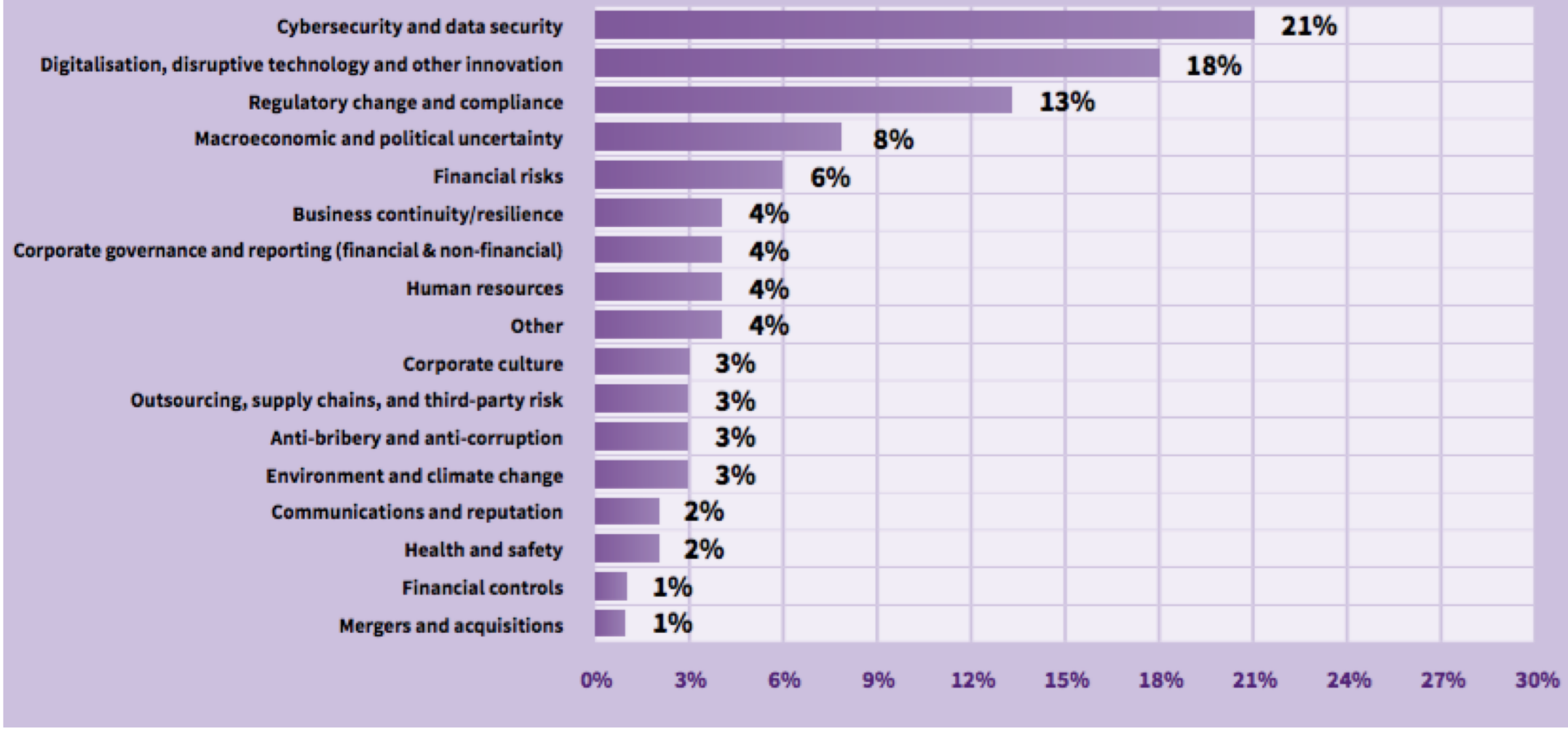
libelium
www.libelium.com

IMTS
2014
STRATI

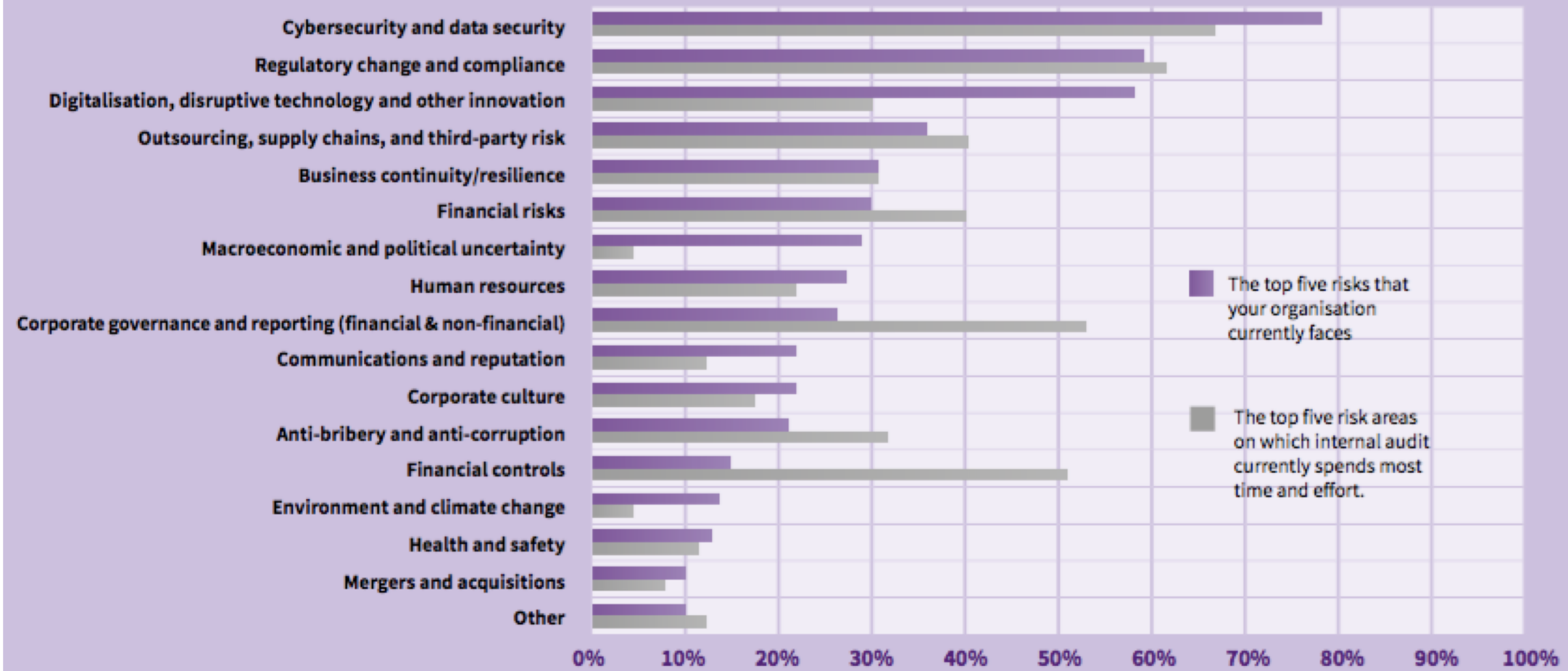
What are the top five risks to your organisation?



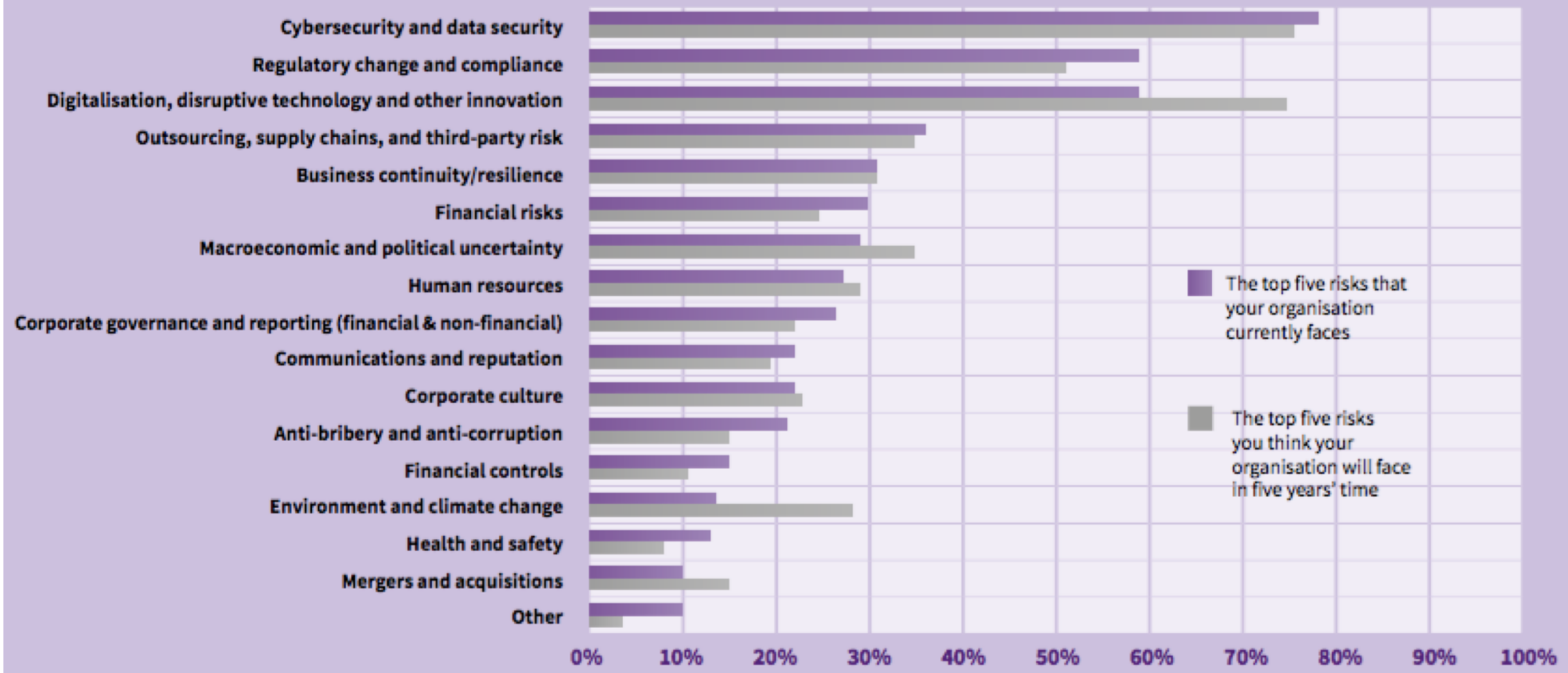
What is the single biggest risk to your organisation?



The top five risks that your organisation currently faces vs the top five risk areas on which internal audit currently spends most time and effort:



The top five risks that your organisation currently faces vs the top five risks you think your organisation will face in five years' time:



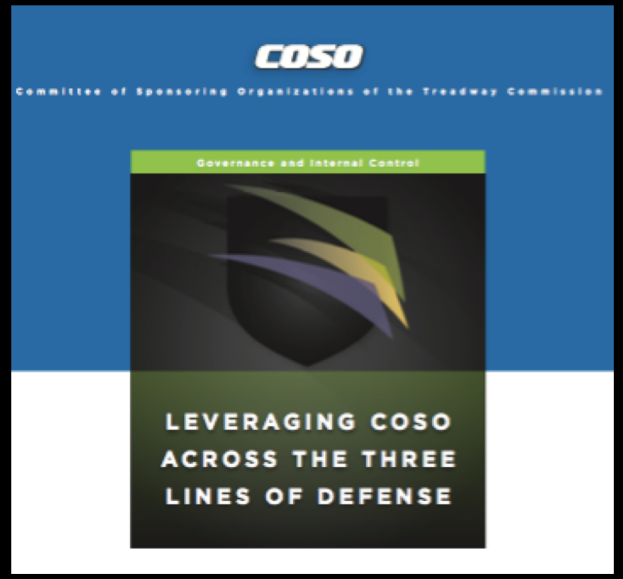
Review 3LoD - 2019

1992
COSO ICIF

2004
COSO ERM

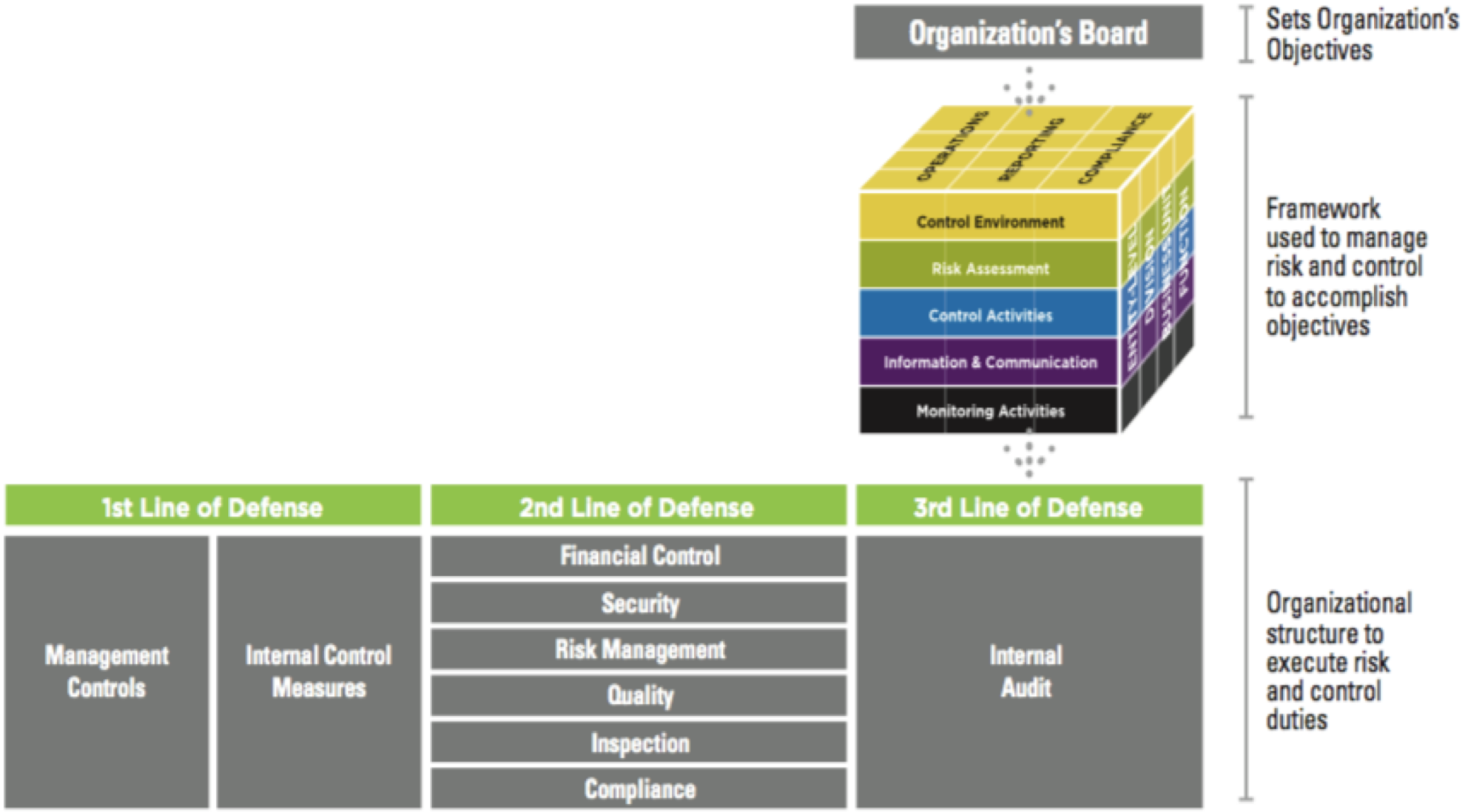
2013
COSO 2013

2017
COSO ERM 2017

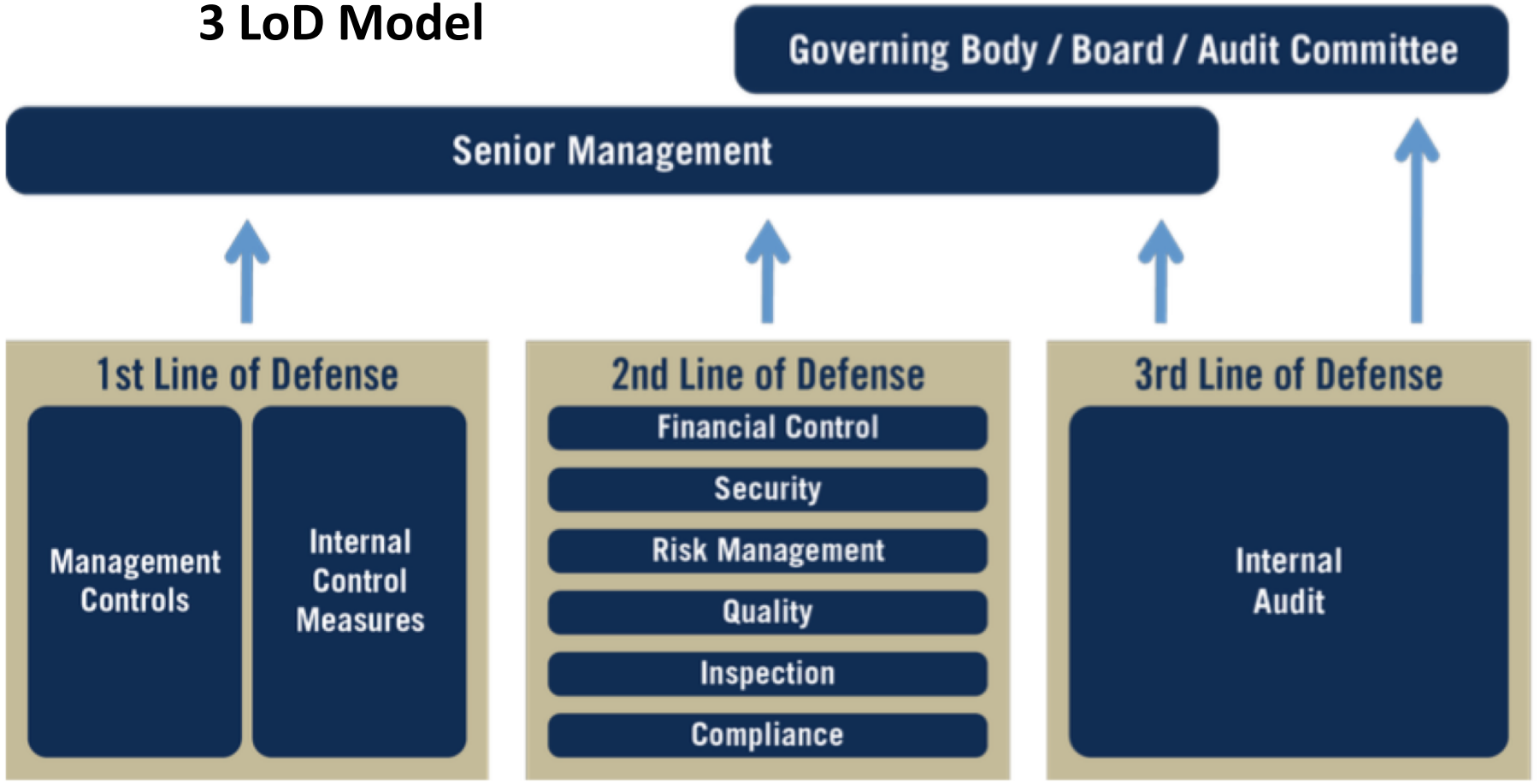


Oversight, Komisaris, Direksi, Tujuan, Kerangka, dan 3LoD Model

Signatory of: PRI Principles for Responsible Investment



3 LoD Model

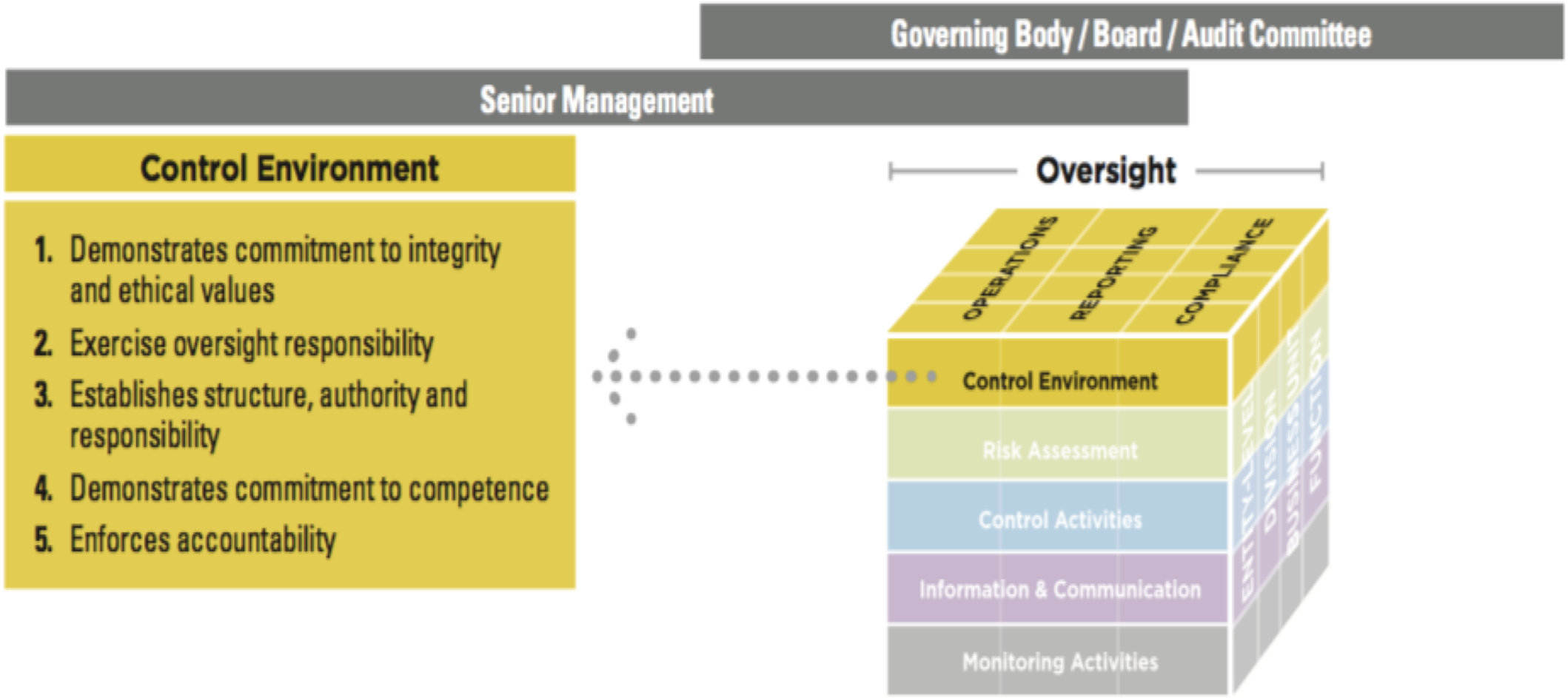


Own & Manage Risks | Monitor Risk & Controls | Independent Assurance

Principles for Responsible Investment

Signatory of:
PRI Principles for Responsible Investment

Tanggungjawab Komisaris dan Direksi terhadap Lingkungan Pengendalian



Signatory of:

PRI Principles for Responsible Investment

COSO & The First Line of Defense

Risk Assessment

6. Specifies suitable objectives
7. Identifies and analyzes risk
8. Assesses fraud risk
9. Identifies and analyzes significant change

Control Activities

10. Selects and develops control activities
11. Selects and develops general controls over IT
12. Deploys through policies and procedures

Information & Communication

13. Uses relevant information
14. Communicates internally
15. Communicates externally

Monitoring Activities

16. Conducts ongoing and/or separate evaluations
17. Evaluates and communicates deficiencies

1st Line of Defense

Management Controls	Internal Control Measures

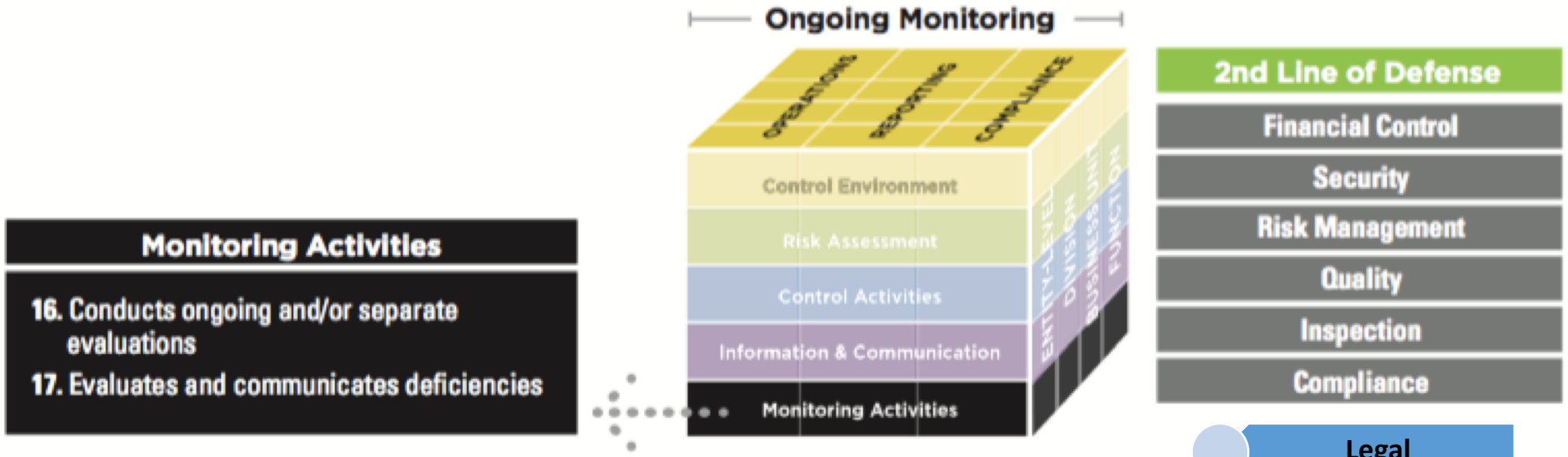
Manajemen Operational

Memiliki dan Mengelola Risiko dan Pengendalian (Risks & Control Owners)

Signatory of:

PRI Principles for Responsible Investment

Figure 5. COSO and the 2nd Line of Defense



- Legal
- Safety
- Health
- Performance (HR)

Memonitor Risiko dan Pengendalian untuk mendukung manajemen

Signatory of:

PRI Principles for Responsible Investment

COSO dan Third Line of Defense

Figure 6. COSO and the 3rd Line of Defense

Assessment of Design and Implementation

Control Environment

1. Demonstrates commitment to integrity and ethical values
2. Exercise oversight responsibility
3. Establishes structure, authority and responsibility
4. Demonstrates commitment to competence
5. Enforces accountability

Risk Assessment

6. Specifies suitable objectives
7. Identifies and analyzes risk
8. Assesses fraud risk
9. Identifies and analyzes significant change

Control Activities

10. Selects and develops control activities
11. Selects and develops general controls over IT
12. Deploys through policies and procedures

Information & Communication

13. Uses relevant information
14. Communicates internally
15. Communicates externally

Monitoring Activities

16. Conducts ongoing and/or separate evaluations
17. Evaluates and communicates deficiencies

Assurance on Effectiveness

3rd Line of Defense

Internal Audit

Memberikan *independent assurance* atas efektivitas Governance, Manajemen Risiko, dan Pengendalian

Signatory of: PRI Principles for Responsible Investment

Review 2019 - 3LoD model

Statis, tidak mencerminkan realitas saat ini

Tidak dinamis, sebagaimana kompleksitas organisasi modern

Fokus pada *defense*, mengabaikan value creation, preservation

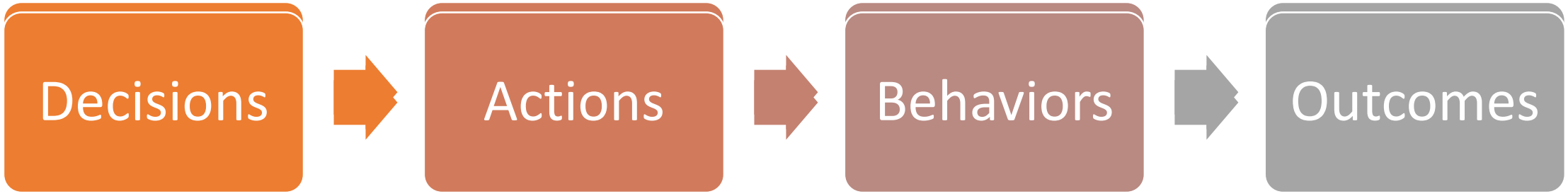
Silo – blurring of the lines

Limit the roles of internal auditor (trusted advisor, strategic partners)

Signatory of:

PRI Principles for Responsible Investment

Value creation dalam organisasi



Enabler of organizational success and value creation

Signatory of:
PRI Principles for Responsible Investment

Governing Body

Internal Audit

Executive Management

Risk, quality, control, and compliance functions

Signatory of:

PRI Principles for Responsible Investment

Enabler of organizational success and value creation

- Regular communication
- Strategy aligned
- Common understanding
- Common vocabulary
- Common rating/measures
- Leverage data/technology
- Blurring the lines (w/ safeguard)

Signatory of:

PRI Principles for Responsible Investment

GRC - Disruption challenges

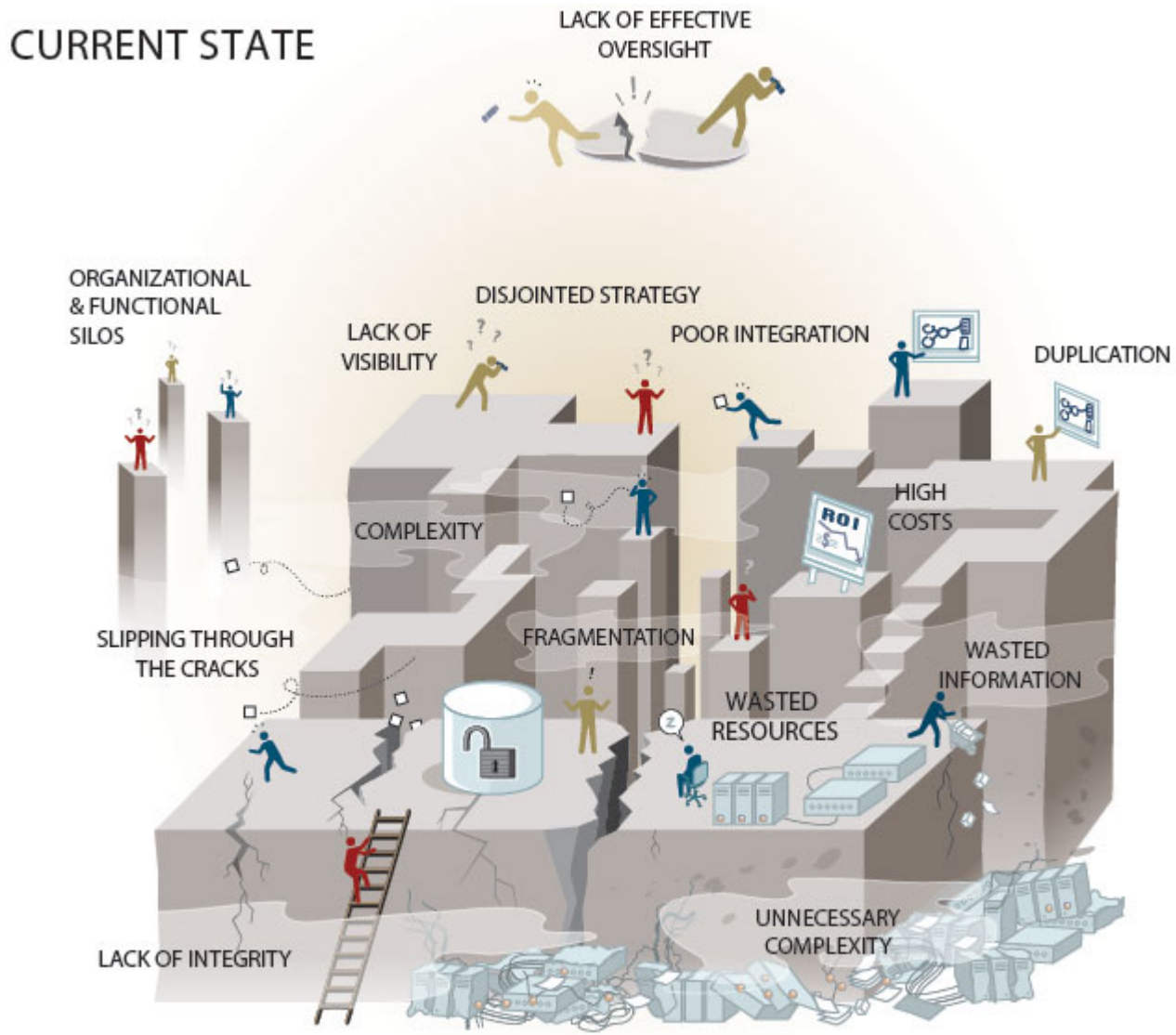
Demand for increased performance	Demand for increased visibility	Growing, conflicting, overlapping regulations
Change in value creation & valuation	Increasing the pace of changes	Finding the 'true north' - turbulence forces
Strategic risk - game changers	Connected - disintermediation	Digitalization, AI, big data, robotics, IoT

Signatory of:

PRI Principles for Responsible Investment

Respons kita terhadap tantangan ini ➔ membuat berbagai program dan fungsi, tetapi ***fragmented dan silo***:

- **Objectives yang counter productive**
- **Strategi yang suboptimal**
- **Kinerja tidak optimal**
- **Lack of information quality**
- **Flows informasi yang tidak memadai**
- **Wrong decisions: ineffective actions and controls**
- **Tend to add more actions and controls**
- **Fail to grasp opportunities**
- **Lack of foundation of a well-run business**



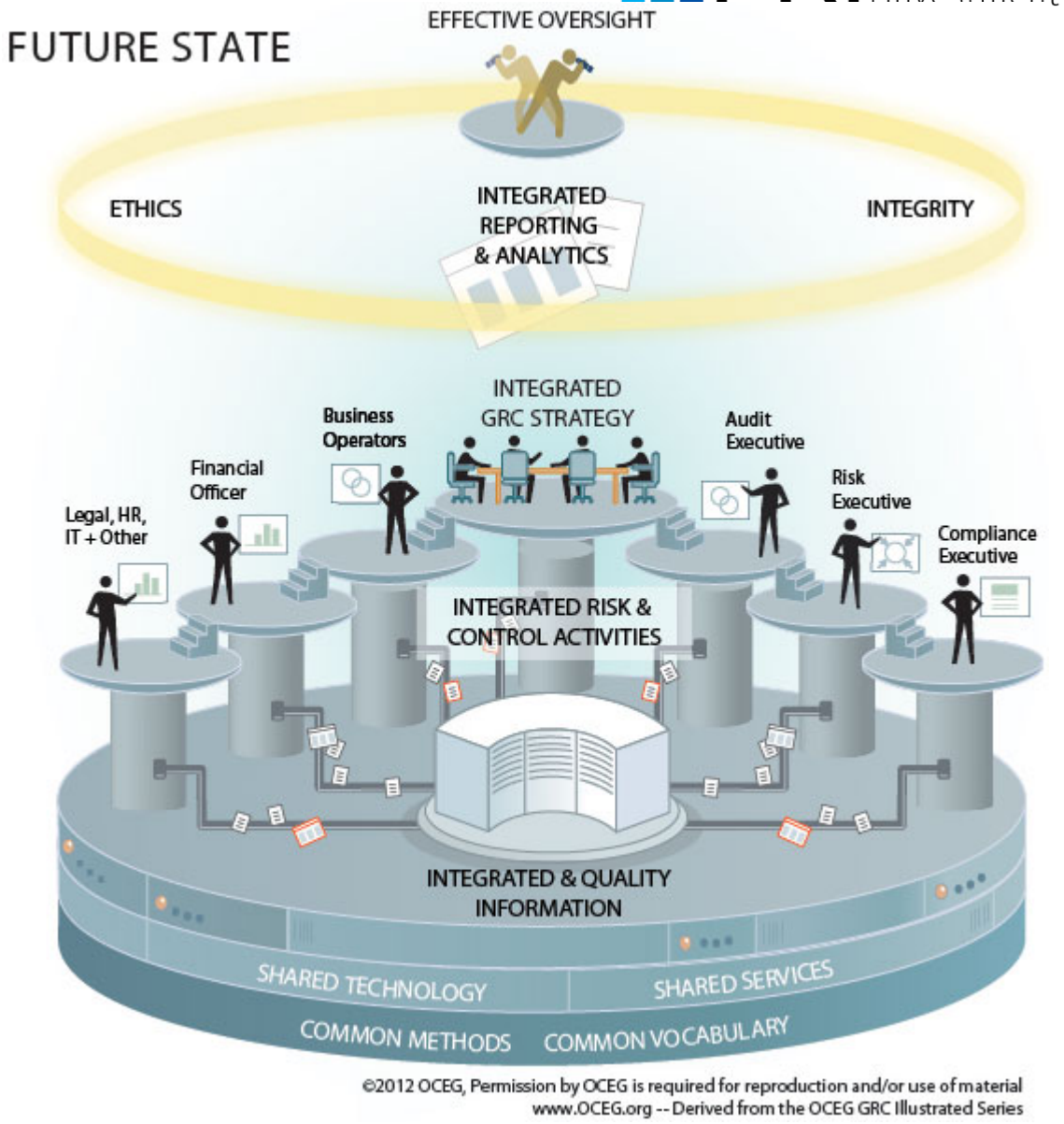
©2012 OCEG, Permission by OCEG is required for reproduction and/or use of material
www.OCEG.org -- Derived from the OCEG GRC Illustrated Series

Signatory of:
PRI Principles for Responsible Investment

Solusinya adalah membuat pendekatan yang memastikan bahwa:

- the right people get the right information at the right times;
- the right objectives are established;
- and that the right actions and controls are put in place to address uncertainty and act with integrity.

- Mengurangi biaya
- Mengurangi duplikasi kegiatan
- Mengurangi dampak terhadap operasi
- Mendapatkan *information quality* yang lebih baik
- Mampu mengumpulkan informasi secara cepat dan efisien
- Memiliki kemampuan untuk mengulangi proses secara konsisten dengan lebih cepat

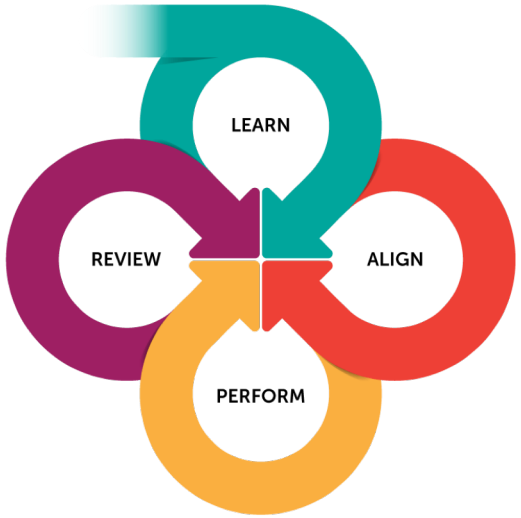


Signatory of:

PRI Principles for Responsible Investment

GRC

PRINCIPLED PERFORMANCE



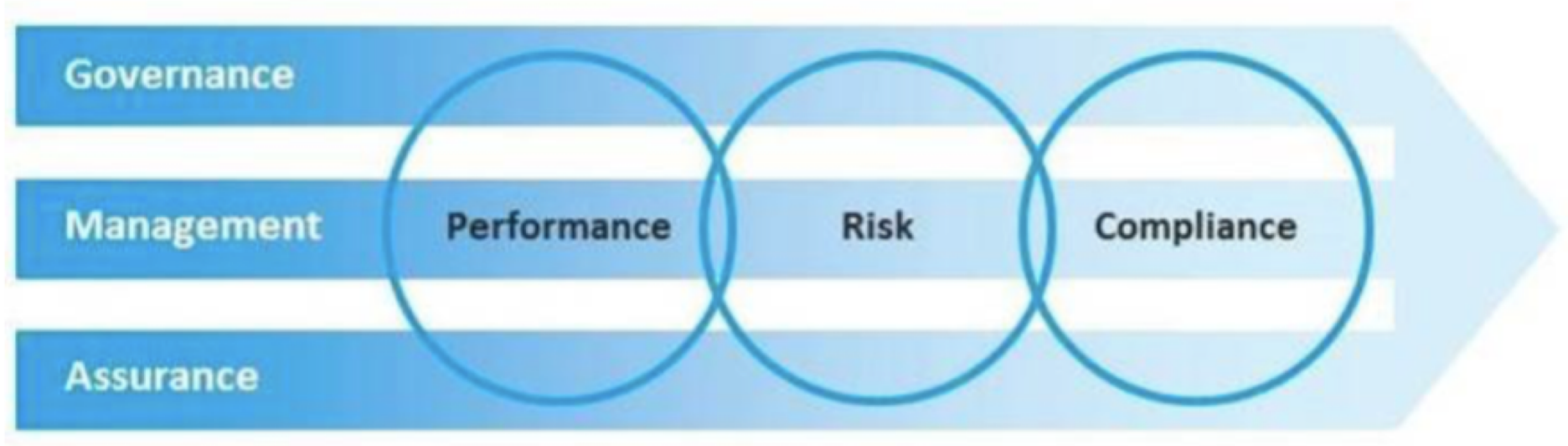
Principled Performance

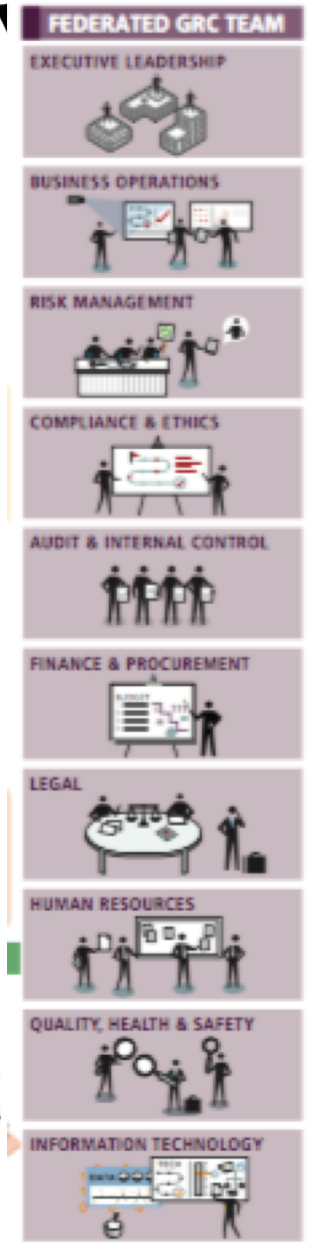
4 reliable 1 achievement of objectives
2 while addressing uncertainty
3 and acting with integrity

Signatory of:

PRI Principles for

GRC Integration





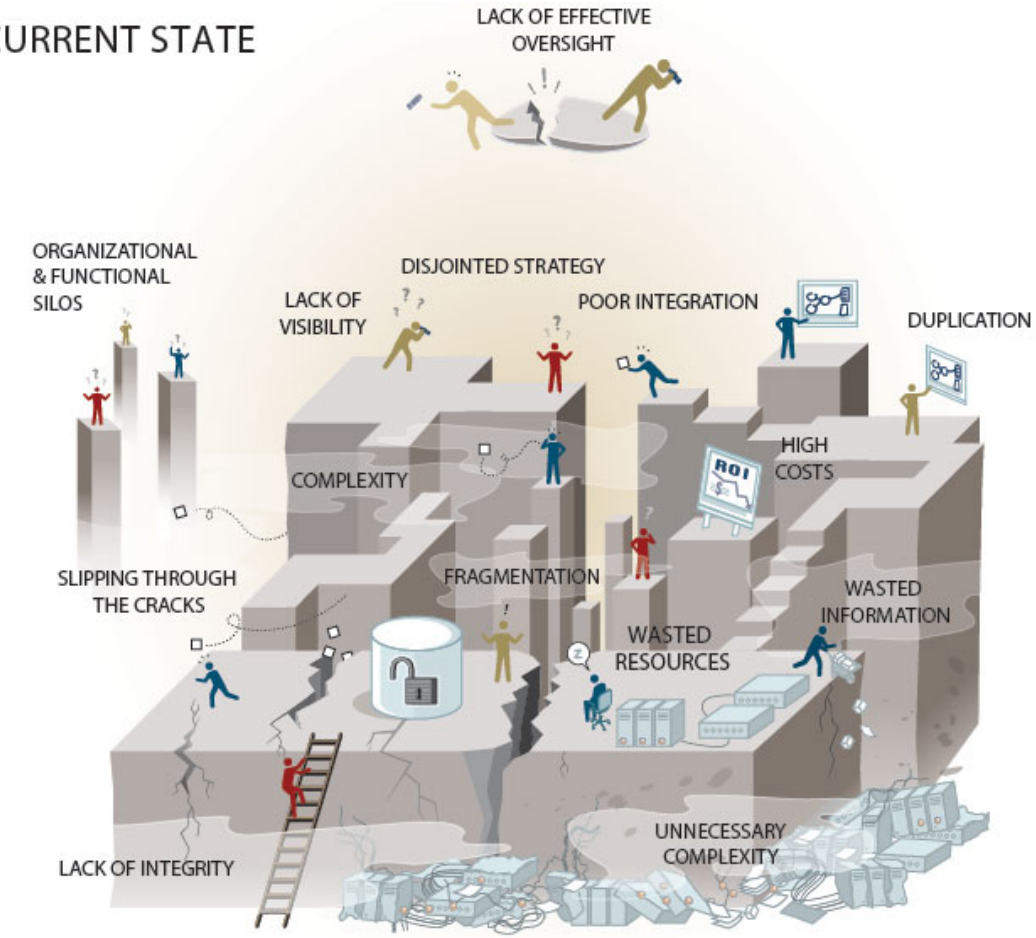
International Organization for Standardization ISO 9001

International Organization for Standardization ISO 14001

Signatory of:

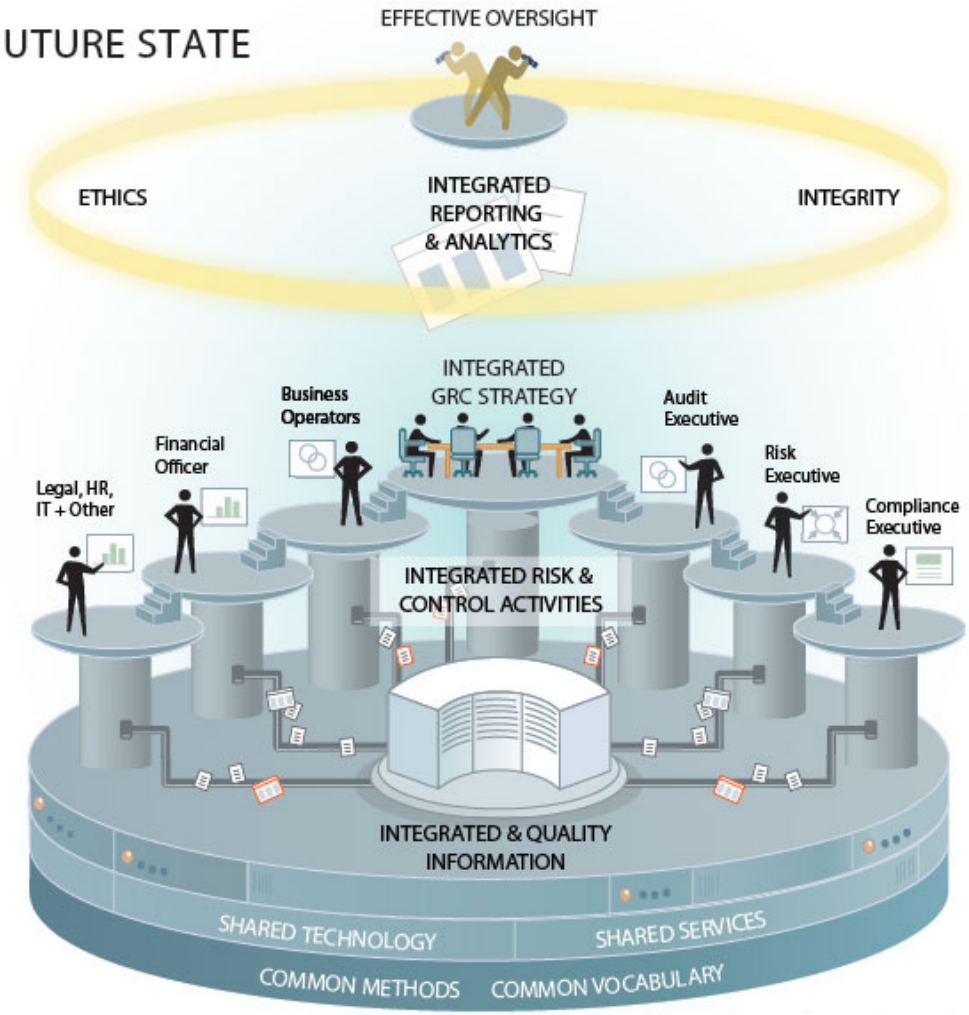
PRI Principles for Responsible Investment

CURRENT STATE



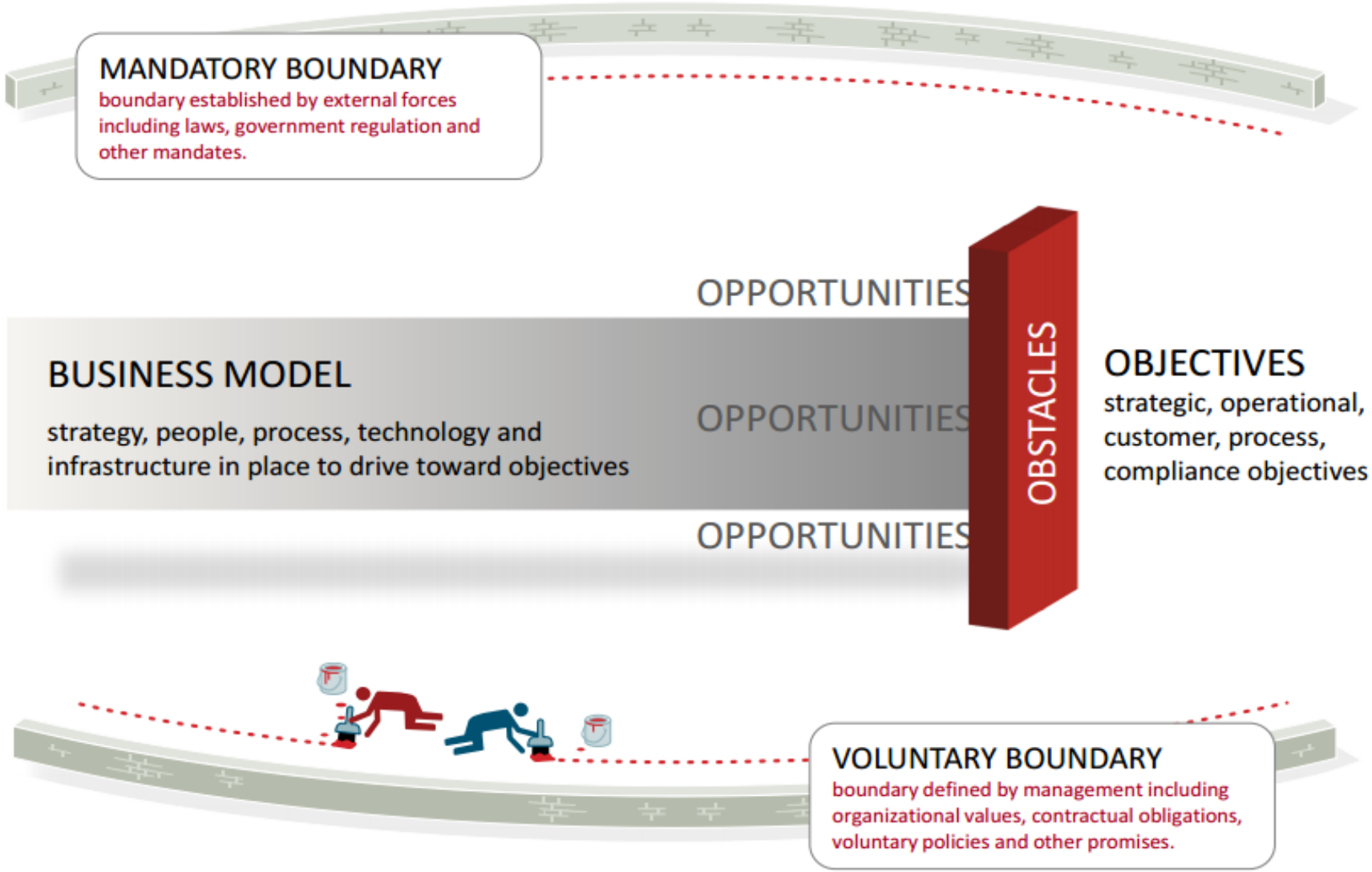
©2012 OCEG, Permission by OCEG is required for reproduction and/or use of material
www.OCEG.org -- Derived from the OCEG GRC Illustrated Series

FUTURE STATE



©2012 OCEG, Permission by OCEG is required for reproduction and/or use of material
www.OCEG.org -- Derived from the OCEG GRC Illustrated Series

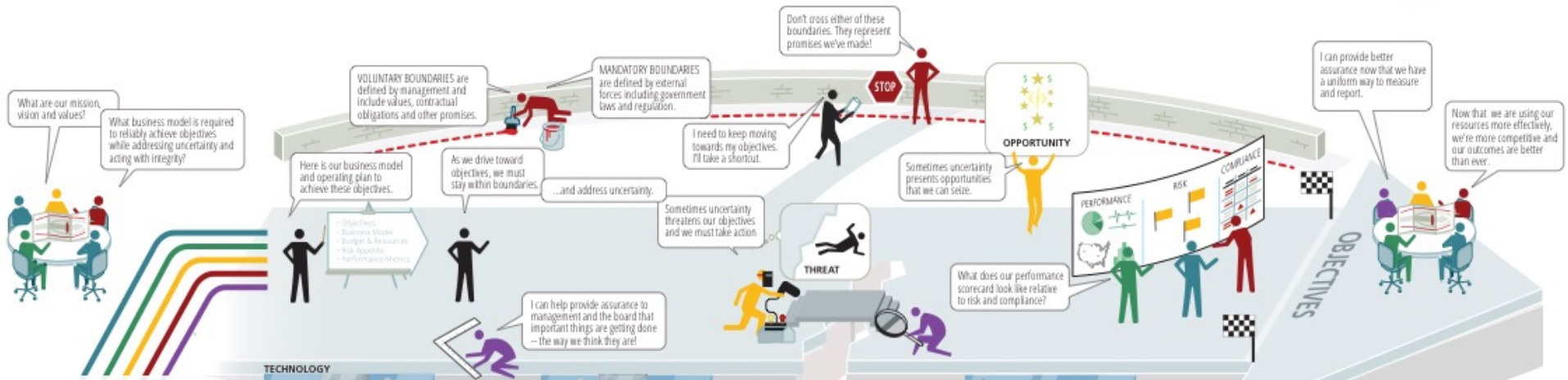
Big Picture


MANDATORY BOUNDARY
boundary established by external forces including laws, government regulation and other mandates.
OPPORTUNITIES
BUSINESS MODEL
strategy, people, process, technology and infrastructure in place to drive toward objectives
OPPORTUNITIES
OPPORTUNITIES
OBSTACLES
OBJECTIVES
strategic, operational, customer, process, compliance objectives
VOLUNTARY BOUNDARY
boundary defined by management including organizational values, contractual obligations, voluntary policies and other promises.

Pathway to Principled Performance

DEVELOPED BY OCEG®

Principles for Responsible Investment



3 Pathway

By orchestrating integrated governance, audit and management systems, an organization can reliably achieve objectives, while addressing uncertainty and acting with integrity.

2 Systems

Core governance, audit and management systems are the backbone of an organization. They leverage common capabilities for multiple purposes.

1 Capabilities

Think of capabilities as "tools" to use for many different purposes. Develop capabilities that can be leveraged by all of your governance, management and audit systems. This way, when you improve the capability, all systems benefit.

LEVERAGE COMMON CAPABILITIES

LEARN

Learn about the organizational context, culture and key stakeholders to inform objectives, strategy and actions.

LEVERAGE COMMON CAPABILITIES

ALIGN

Align strategy with objectives, and actions with strategy, by using an effective decision-making approach that addresses values, opportunities, threats, and requirements.

PERFORM

Perform actions that promote and reward things that are desirable, prevent and remediate things that are undesirable, and detect when something happens as soon as possible.

LEVERAGE COMMON CAPABILITIES

REVIEW

Review the design and operating effectiveness of the strategy and actions, as well as the ongoing appropriateness of objectives to improve the organization.

Contact **info@oceg.org** for comments, reprints or licensing requests ©2014-2015 OCEG for additional GRC illustrations and resources visit **www.oceg.org/resources**

GRC CAPABILITY

MODEL ELEMENT VIEW

rinciples for
esponsible
nvestment

The Institute of Internal Auditors Indonesia

COSO ERM 2017

Signatory of: PRI Principles for Responsible Investment

What defines a modern business?

	KEY AREA OF FOCUS UNTIL NOW		NEW AREAS OF FOCUS
1	Steady growth, Structure & controls	→	Sustained impact Flexible & trusting
2	Big initiatives that take time	→	Rapid experimentation
3	Lots of multi-tasking	→	Passionate believers focus on single initiatives
4	Managers and "subordinates"	→	Leaders empower teams
5	Compete with barriers to entry	→	Compete with continuous innovation

Source: adapted from The Start-up Way website: http://thestartupway.com

The Institute of Internal Auditors Indonesia

COSO ERM 2017

Signatory of: PRI Principles for Responsible Investment

Figure 5.1: Risk Management Components

The Institute of Internal Auditors Indonesia

Signatory of: PRI Principles for Responsible Investment

Benang Merah

GRC

Revisi 3 LoD

Decisions → Actions → Behaviors → Outcomes

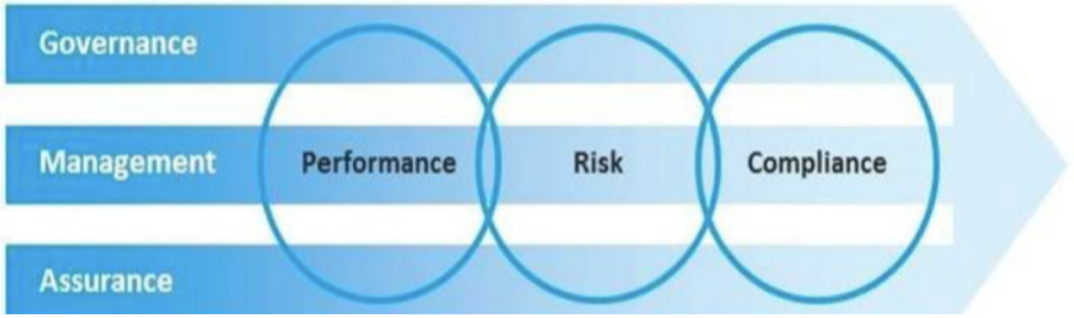
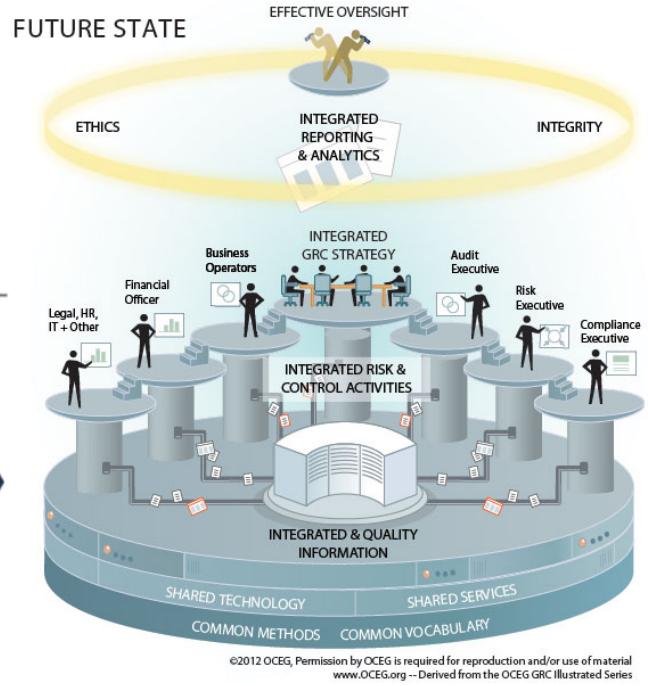


Figure 5.1: Risk Management Components



©2012 OCEG, Permission by OCEG is required for reproduction and/or use of material www.OCEG.org -- Derived from the OCEG GRC Illustrated Series

COSO ERM 2017

Signatory of:

PRI Principles for Responsible Investment

Benang Merah

Lingkungan bisnis, disrupsi, dan risiko baru berkembang sangat cepat, dari berbagai sumber

Respon kita terhadap perubahan lingkungan tidak memadai

- Reaktif, Silo, dan terfragmentasi
- Merespon dengan menambah pengendalian
- Strategy dan objective yang tidak tepat
- Kualitas dan flows informasi yang tidak baik
- Tidak memberi fondasi untuk mengelola business yang well run

Revisi 3LoD, GRC, dan COSO ERM memberikan kerangka untuk mengatasi kelemahan fundamental tersebut

- Integration, communication, culture, & technology,
- Establish process before technology
- Beware of building another silo
- Seek out overlaps and build efficiencies
- Create a common language and vocabularies: skeleton, calibration
- Integration means optimal allocation of resources and achieving objectives confidently

Signatory of:

PRI Principles for Responsible Investment

Implications for Internal Auditor

- Agile - audit at the speed of risks
- GRC (enterprise wide view of risks)
- Auditing Strategy
- Auditing Culture
- Cybersecurity
- Artificial Intelligent
- ESG (Climate and Sustainability)
- Data Analytics
- Talent management
- Managing Millennials

Signatory of:

PRI Principles for Responsible Investment

BUMN
Hadir untuk negeri

TERIMA KASIH