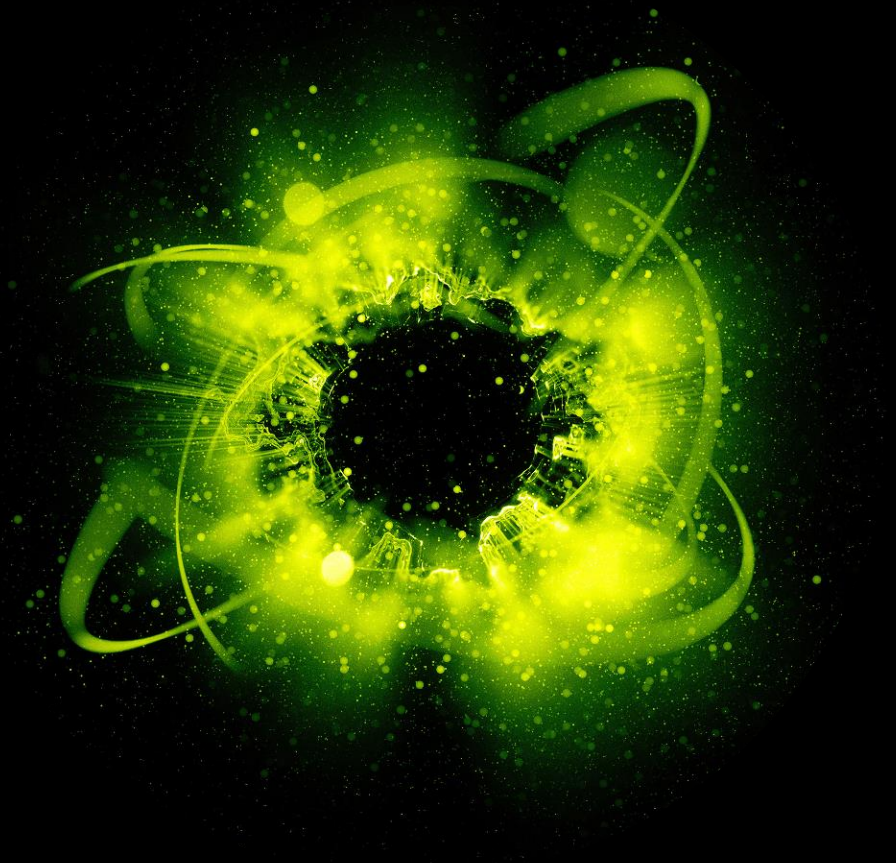
Deloitte.

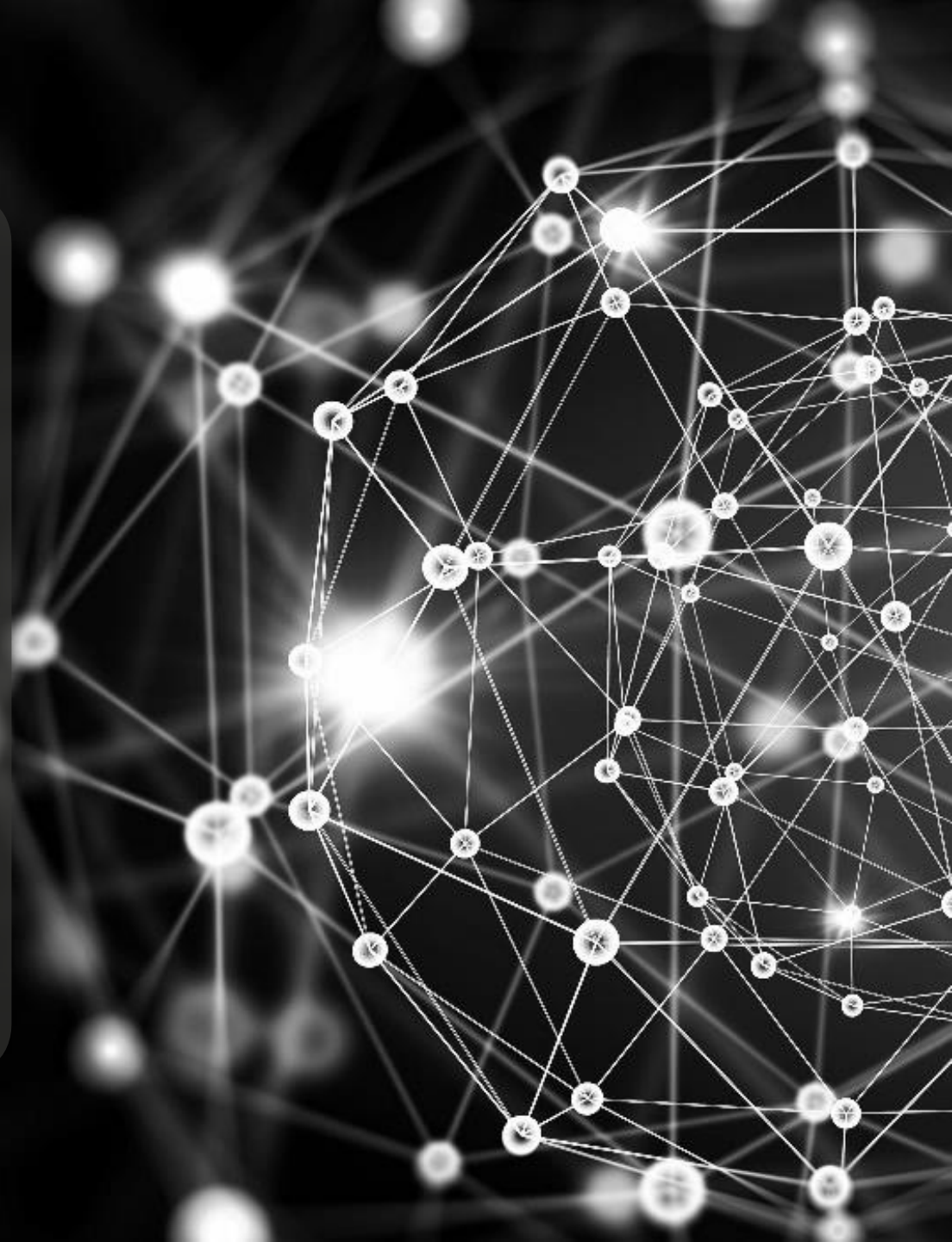


Deloitte Forum 2023: Navigating GRC Trends in the Tech Age

22 November 2023

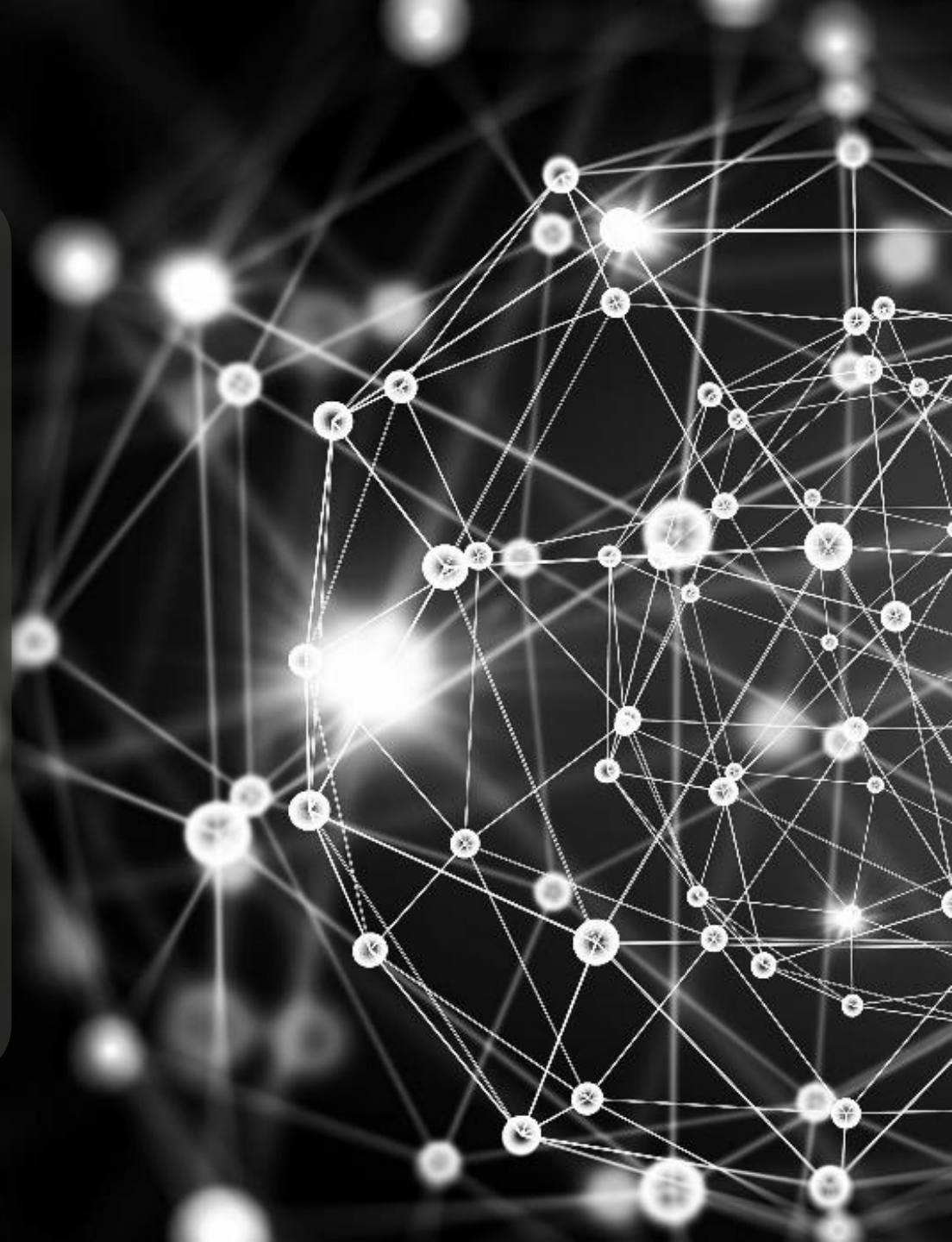
Agenda

- Making a Start with Overview GRC
- Taking a glance Through each Stage of GRC
- Moving Forward with GRC in Digital Era
- Accomplishing GRC Integration



Agenda

- Making a Start with Overview GRC
- Taking a Glance Through each Stage of GRC
- Moving Forward with GRC in Digital Era
- Accomplishing GRC Integration

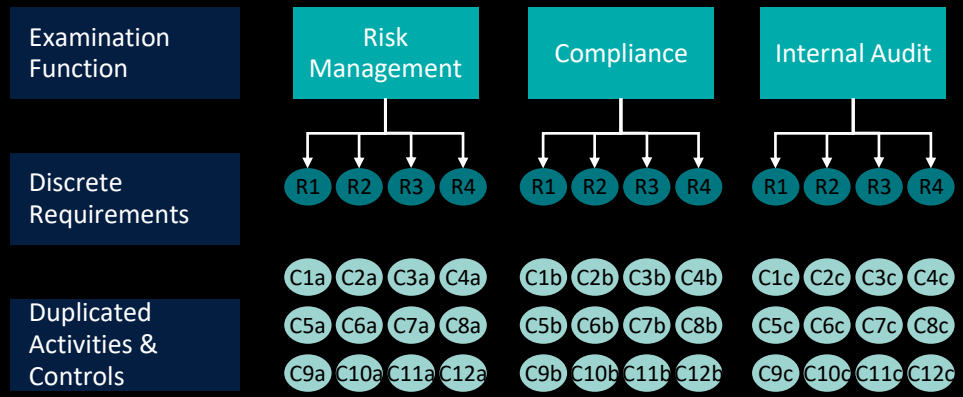


What is Your Current GRC Practices ….

Q1

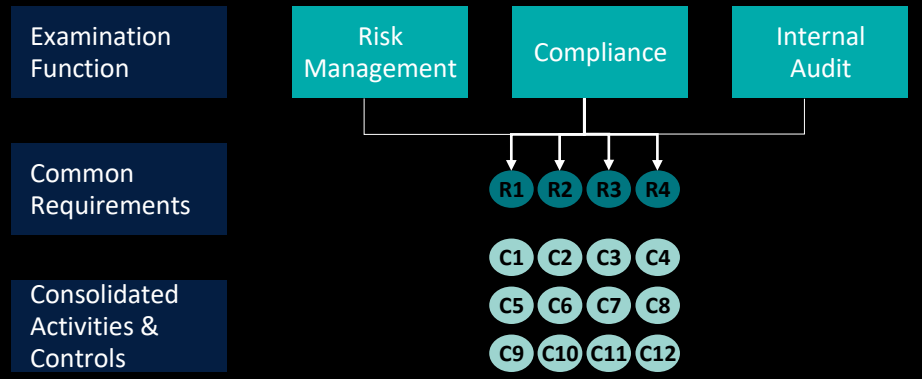
Silo-Based Program

Current “One-off” approach creates multiple discrete compliance programs which leads to inconsistency and inefficiency in managing requirements from multiple regulations



Integrated Program

Integration that reduces the cost, complexity, and workload to support compliance efforts is needed; considerable cost efficiencies can be realized when the overlap is removed and a common definition of requirements is applied



Common Symptoms:

- Are you struggling with multiple views of requirements?
- Is risk and compliance management taking too much time and getting too complicated?
- Does your organization have different processes and tools that produce inconsistent interpretations?
- Is the business frustrated they are always being audited and assessed by different functions – for essentially the same thing?
- Is the aggregation and transparency of risk unclear?

GRC Overview

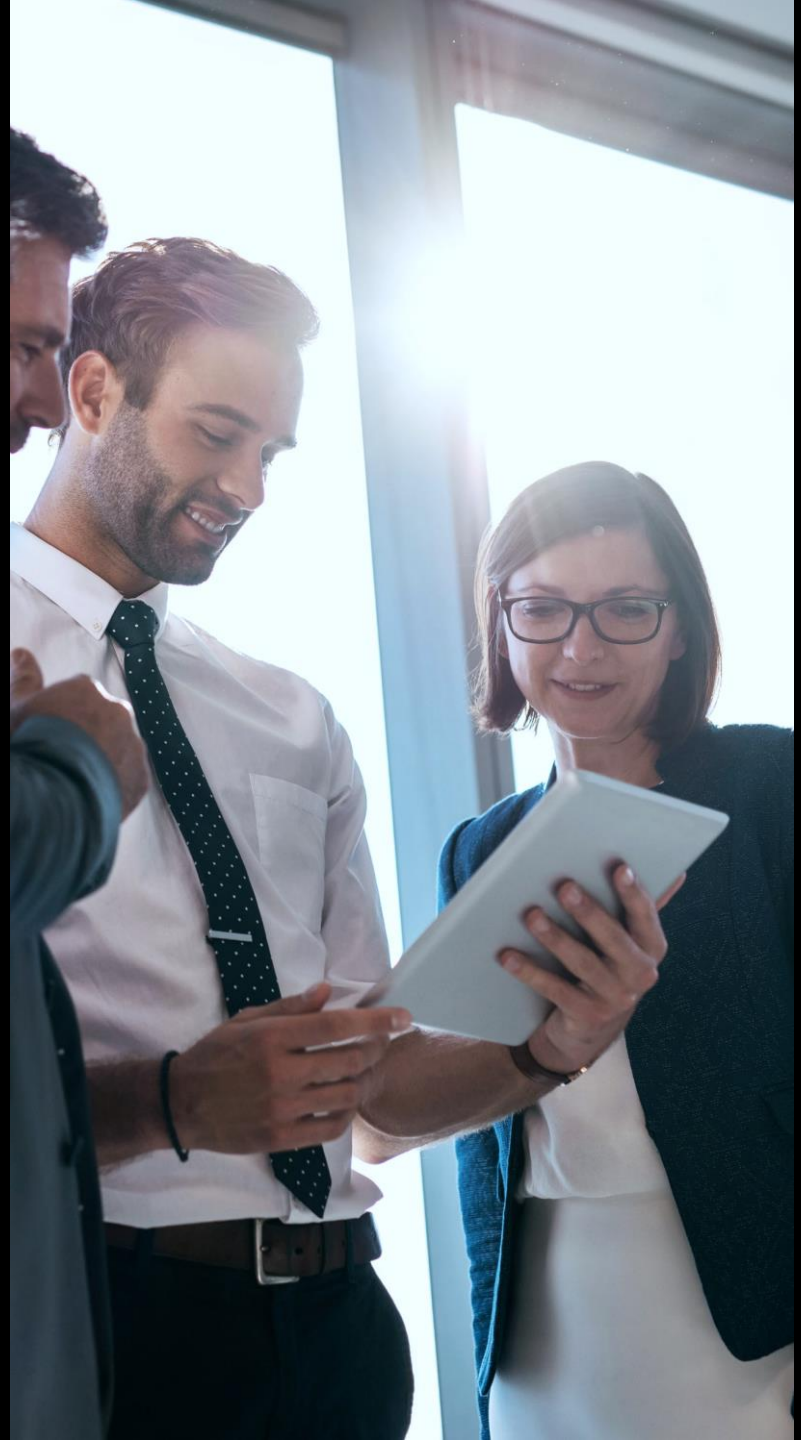
Governance, Risk, and Compliance (GRC) is the product of three integrated and inter-related pillars within an organization that enable its ability to effectively and holistically govern the organisation's risks while ensuring compliance to all internal policies and procedures as well as regulatory requirements

GRC Program is neither a project not a technology, but a corporate objective for improving governance through more-effective compliance and a better understanding of the impact of risk on business performance. GRC is the culmination of People, Processes, and Technology deployed in a systematic and integrated manner to assist in managing risk and compliance in an effective and efficient manner across the enterprise.

GRC Overview (Cont.)

A capability and a culture that enables an organization to achieve principled performance by:

- Prioritizing stakeholder expectations
- Setting and evaluating achievement of objectives
- Ensuring that objectives are achieve with integrity and excellence
- Managing the desirable and undesirable effect of uncertainty on objectives
- Operating within voluntary and mandatory boundaries of conduct
- Communicating with internal and external stakeholders about system performance
- Providing assurance that the system is effective, efficient and agile



Key Relevant GRC Modules…

- Governance
- Ethics & Culture Management
- Performance Management
- Audit Management
- Compliance Management
- Risk Management

Recent Drivers for Increasing GRC Capabilities

In recent years, there has been significant push for Governance, Risk and Compliance (GRC) services particularly around the support for such requirements including transparency, auditability, corporate governance and risk management that they bring accommodate for companies.

This is predominantly in response to a growing multitude of legislative, regulatory, standards and obligations companies are increasingly faced with affecting different areas of the organisation including as follows:

This increase in regulatory requirements results in a series of needs common to all organizations, including the need to implement **risk management and internal control models** to minimize the risks of regulatory non-compliance or real time risk response.

How the External Threat Accelerates Effective GRC Mechanism…

With recent major events such as the COVID-19 pandemic transforming the way we work, the risk landscape is seen to be continually evolving, posing greater challenges for management to monitor the organization’s key risks and stay up-to-date with aspects of GRC.

Highlighted the Need for Better Rapid Response Capability

According to OCEG Survey, there are essential results on GRC,

“Beginning with the changes in response to the COVID-19 pandemic in early 2020, including the accelerated pace of digital transformation and remote working environment, to the resulting impact on supply chains and shifts in the workforce, investor, and consumer demands, virtually all organizations have seen their GRC capabilities straining under the pressure.

69% Have more employee work remotely

60% Are having to respond to increased data privacy and cybersecurity regulations

52% Are experiencing more cyberthreats and ransomware attacks

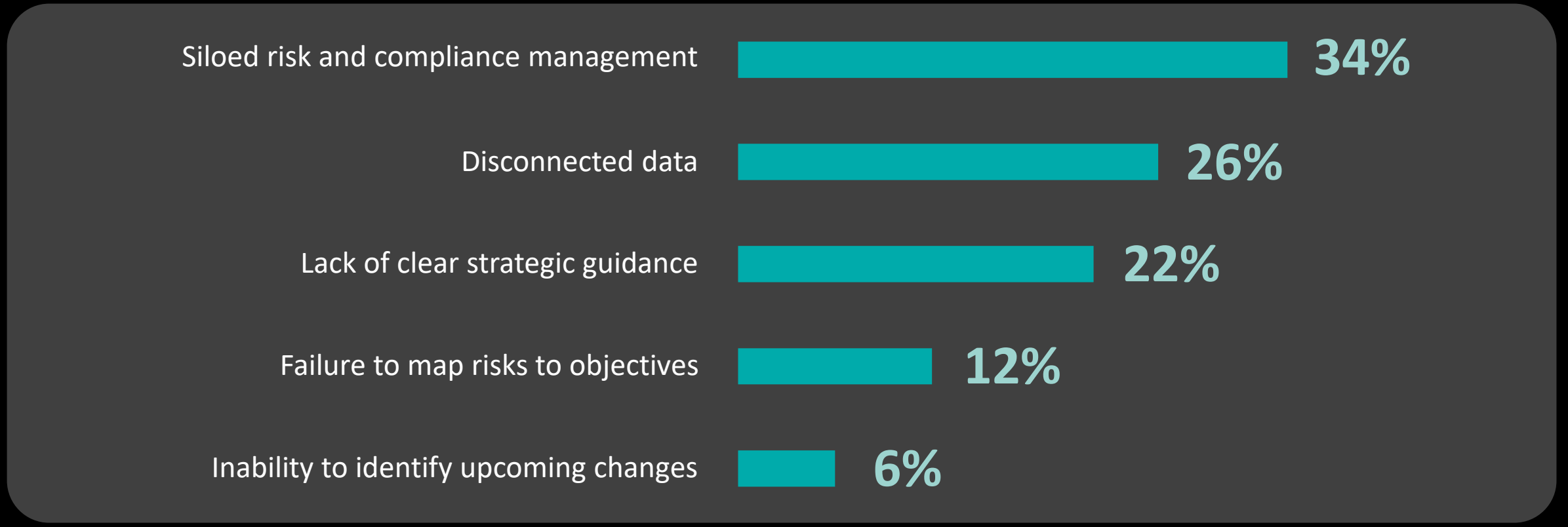
48% Feel economic pressures to improve performance

Source: OCEG, OCEG GRC Readiness for Rapid Change Survey 2022

The top challenges in a GRC program is its inability to rapidly respond to risks

Q2

According to OCEG Survey, there are essential results on GRC,



Source: OCEG, OCEG GRC Readiness for Rapid Change Survey 2022

Internal Challenges Related to Risk and Internal Control Process

New Emerging Risk & Compliance Obligations

Over 100 annual regulatory guidelines with more emerging over time

1000 – 8000

Risk & Compliance Register

Annual RCSA assessment results are often copied from the previous year and scored subjectively

100 – 600

KRI Metrics

Human data collection each month / quarter with no assurance on completeness or accuracy

Manual and Repetitive

data collection, sampling and testing involving multiple touch points

Minimum Expectation for Critical/ High Risk controls to be tested

Between 1000-2000 standard Key Control Tests performed annually by 1st, 1.5 and 2nd LOD

30K – 80K

samples selected for testing annually

30 - 40

Samples per controls

Driver and demand for GRC solutions – typical GRC “buyers”

Compliance

- Newly established departments, according to industry sectors
- High frequency of regulatory changes
- Difficulty pinpointing high risks

Internal Control

- Poorly developed control models
- Large and complex internal control models, according to industry
- Manual management processes
- No tools for consolidated view

Risk Management

- Used software does not allow for advanced risk management.
- High effort for sending and reviewing assessment questionnaires

Internal Audit

- Limited visibility on areas of risk and control
- Completed work not disseminated effectively with other areas
- Non-scalability of office packages or dedicated to internal audit

IT Compliance

- IT Regulatory Compliance
- Heterogeneous systems management
- Too much time / effort devoted to maintenance
- Duplicate Risk and Control requirements

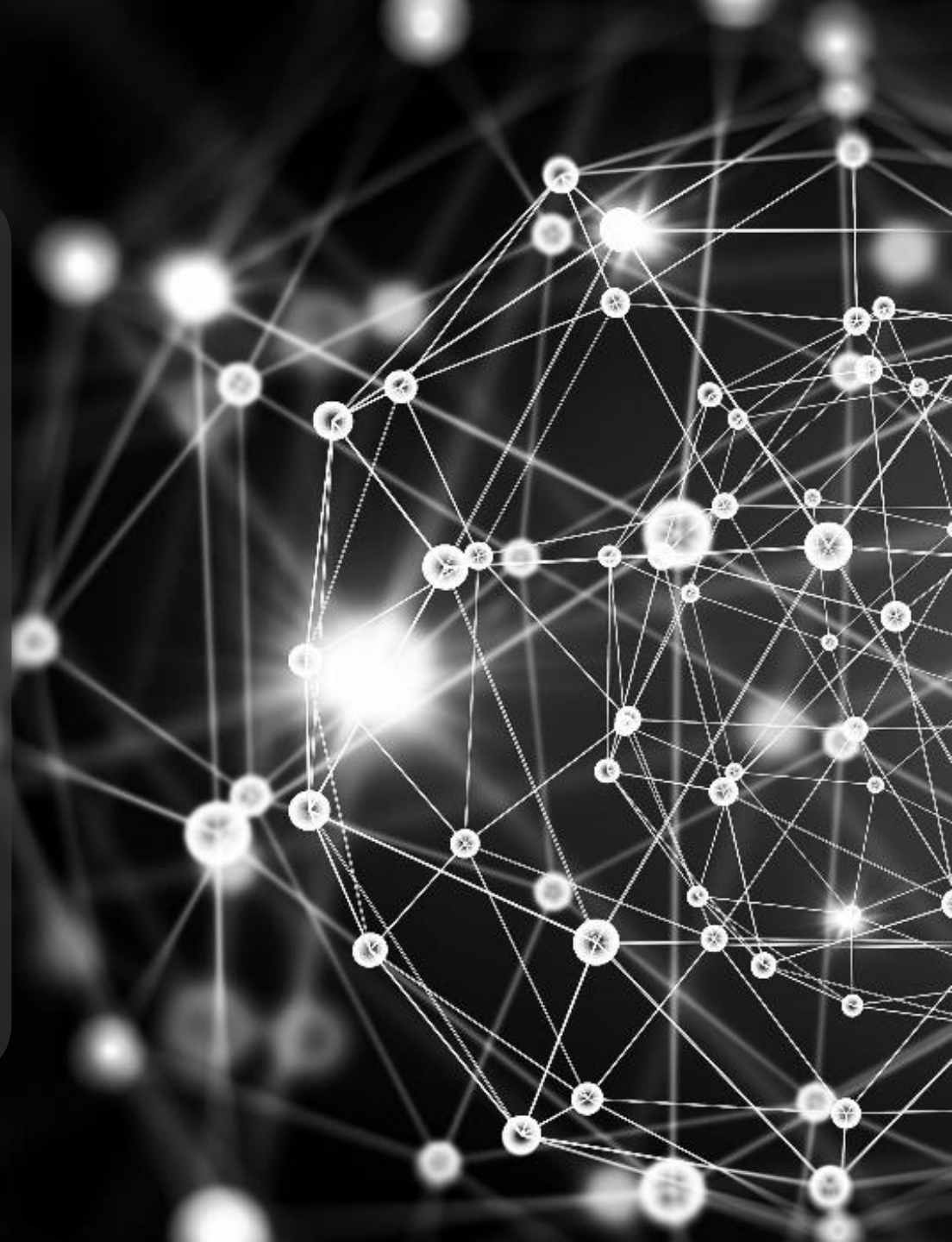
Business Area

- Duplication of efforts to evaluate controls
- Multiple feedback mechanisms to Risk & Control (email, conferencing, etc..)

Typically, highly regulated industries have the most complex / demanding GRC service requirements

Agenda

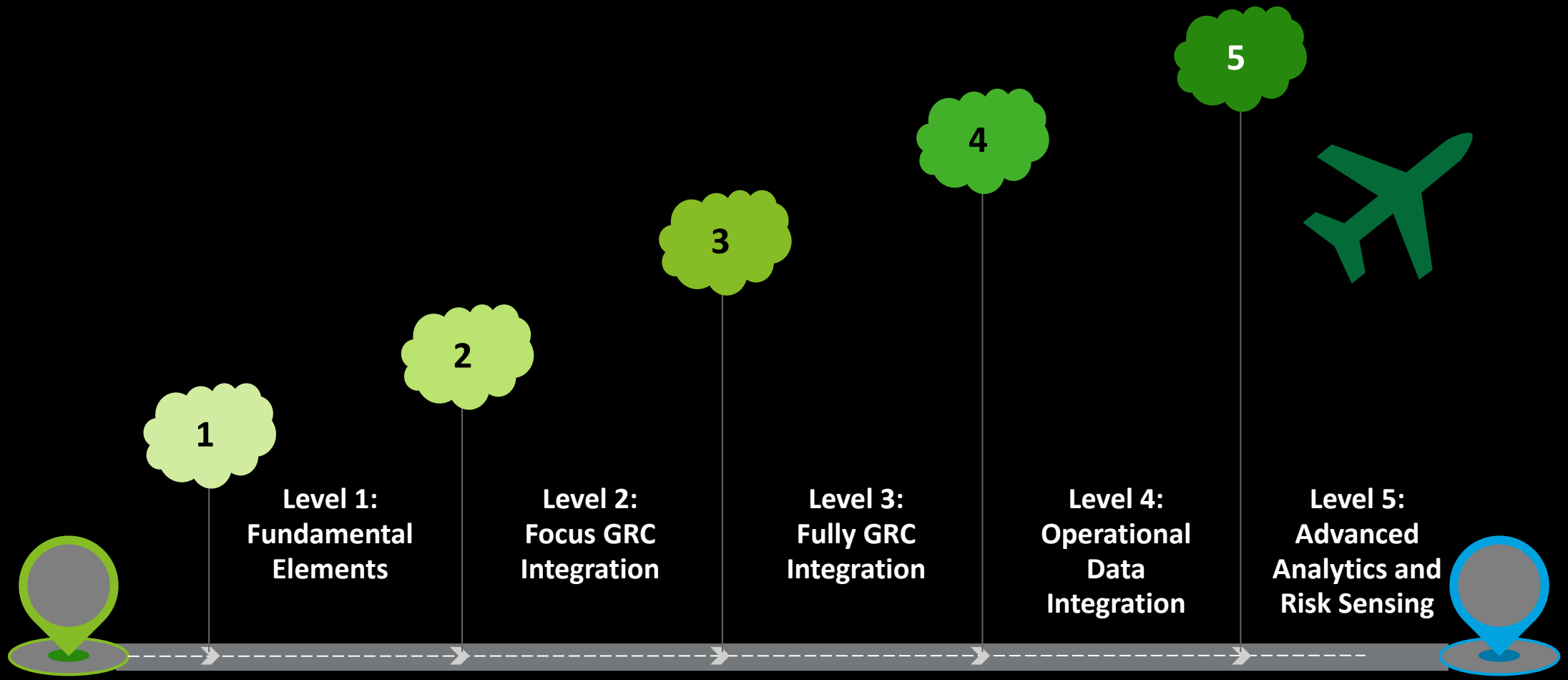
- Making a Start with Overview GRC
- Taking a glance Through each Stage of GRC
- Moving Forward with GRC in Digital Era
- Accomplishing GRC Integration



Deloitte GRC Maturity Model

Q3

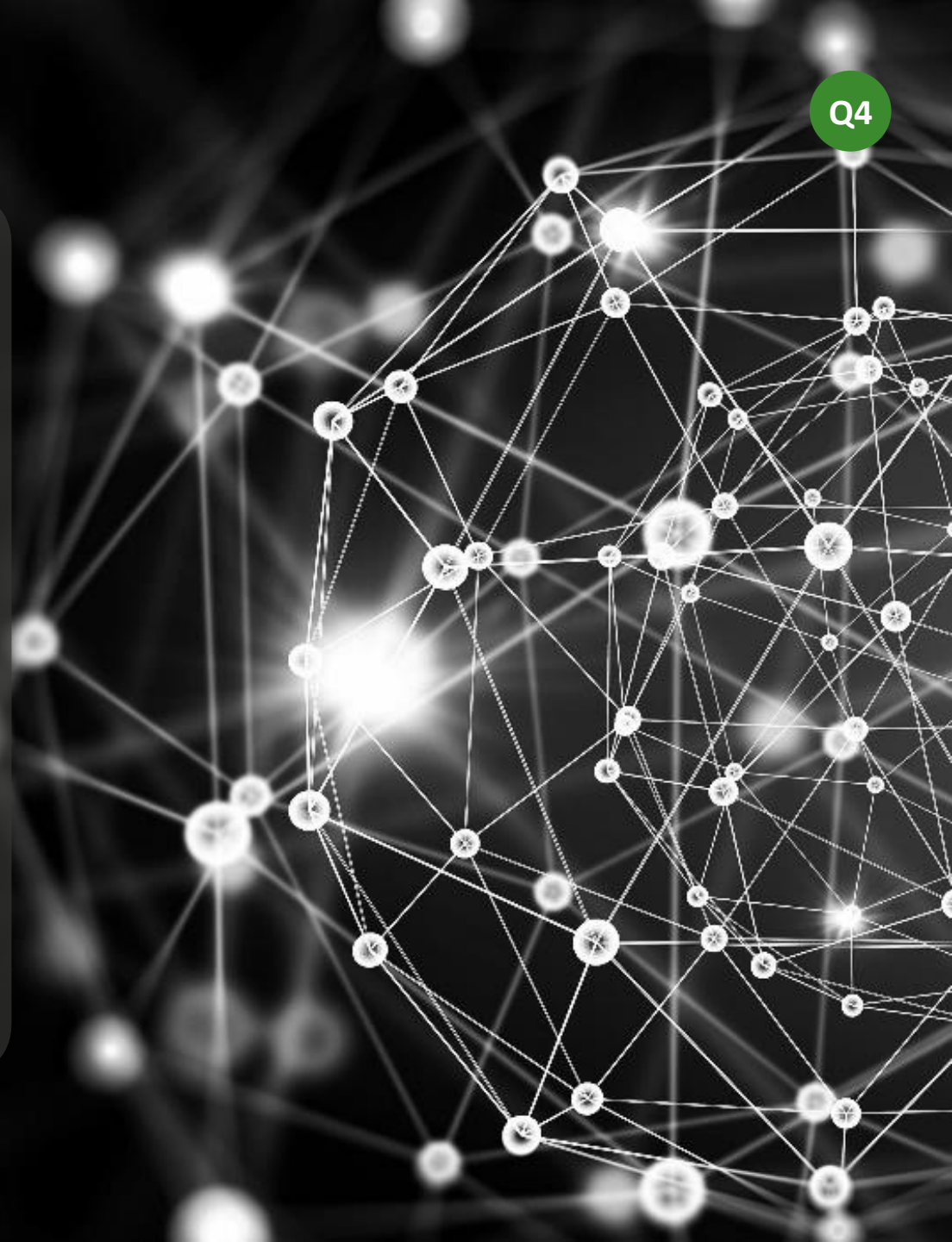
Deloitte has defined the GRC maturity level of GRC according to our experience which commence from initial to intelligence stage.



Agenda

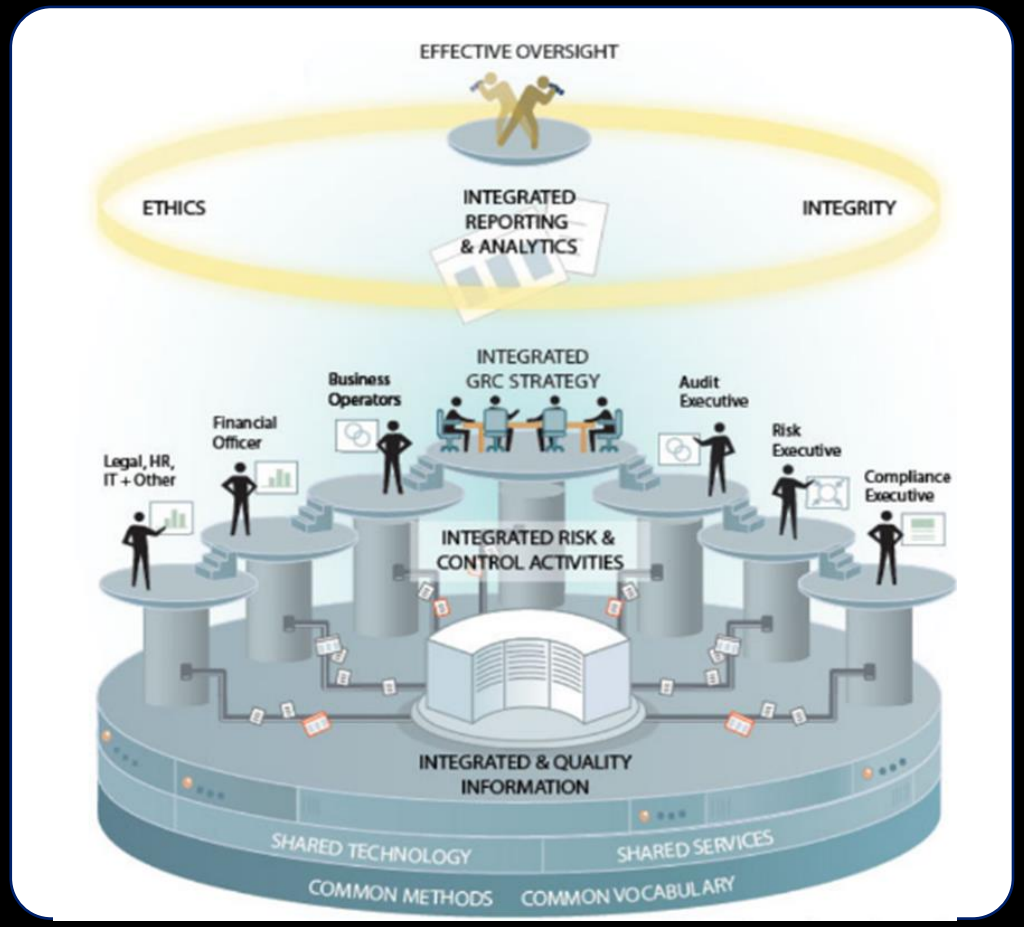
Q4

- Making a Start with Overview GRC
- Taking a glance Through each Stage of GRC
- **Moving Forward with GRC in Digital Era**
- Accomplishing GRC Integration



Deloitte Vision on the Future of GRC

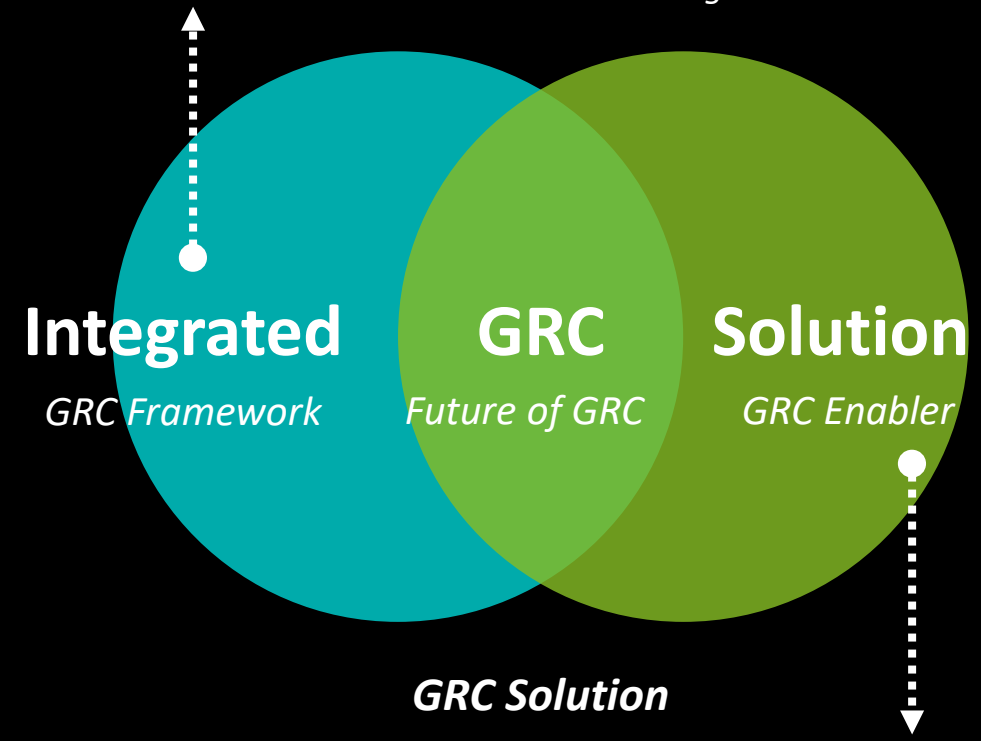
Future State



Source: OCEG

Integrated GRC

*"An **Integrated GRC** framework provides **harmonization between business functions** and encourages **data sharing** to reduce redundancy and serves to unlock business value through a consolidated GRC management*

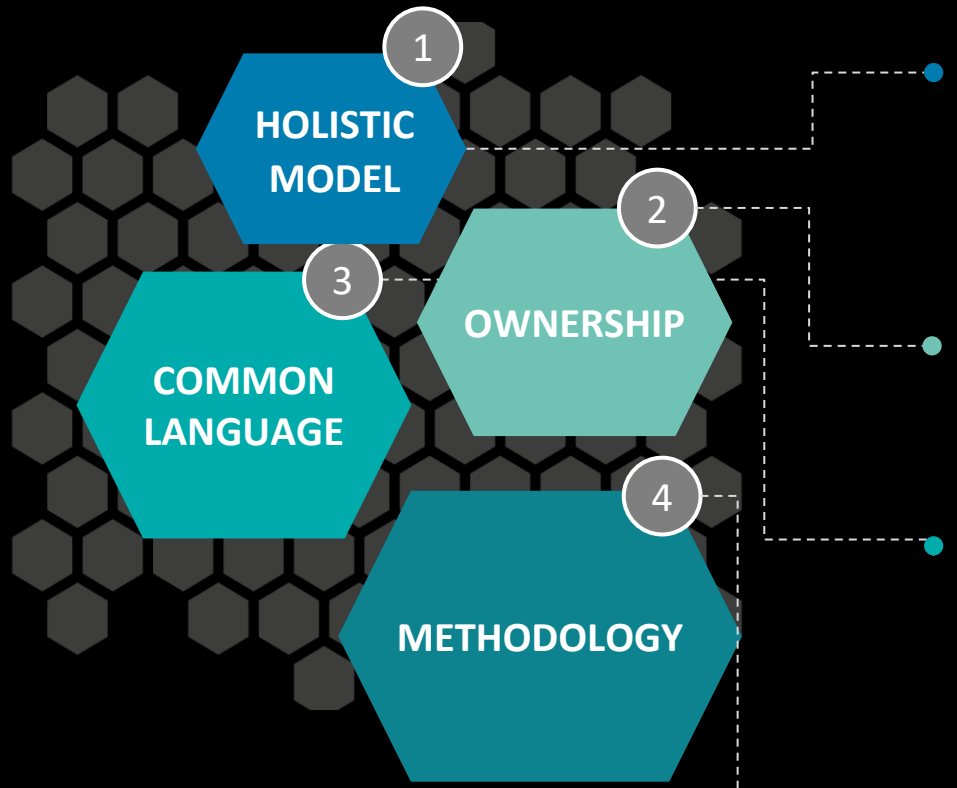


GRC Solution

*"Think of **GRC Solution** as the organization's personal assistant for a structured approach to operationalise the Integrated GRC process"*

Strategic Approach for GRC Solution Implementation

To successfully implement GRC solution, the foundation should be well prepared and ready for the implement and input into the system with comprehensive design.



Manage risk holistically across the organisation by converging taxonomies and methodologies.

End user information is not restricted to Corporate oversight functions alone but also Management.

Independently from any programme, the information is distributed to end users based on a set of rules, such as risk taxonomy and/or root causes.

Common methodologies supports risk aggregation and the decision on whether to accept or mitigate a risk.

Sample of GRC Platform Function Architecture

Management Layer

(enables communication, coordination, and measurement of GRC processes)

- Create and view reports
- Dashboards
- Remediation simulations and plans
- Warnings
- Notifications
- Others

Application Layer

(applications layer for the different GRC modules)

- Application "1"
  - Methodology
  - Functionality
  - Workflow
- .....
- Application "n"
  - Methodology
  - Functionality
  - Workflow

Business Logic Layer

(tools that enable GRC modelling, facilitating the integrated multi-regulatory concept)

- Data entities
- Complex relations, interlinkages and overlaps
- Workflows

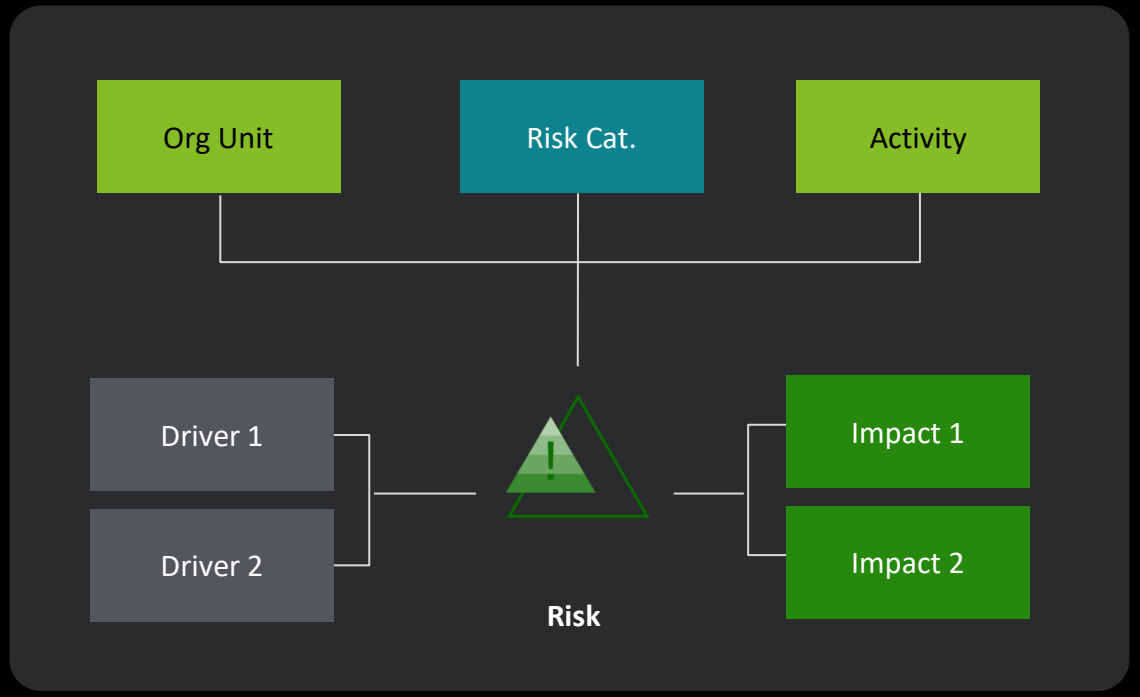
Repository Layer

(stores all entities that are part of GRC projects)

- Business units
- Processes
- Sub-processes
- Systems
- Risks
- Controls
- Policy
- Regulation

Use Cases of GRC Solution: 360-degree understanding of risk events

360-degree understanding of risk events



GRC Solution is able to support you manage risks and risk responses across the organization.

Leverage drag-and-drop functionality, drivers, impacts, and responses

Use in a workshop environment for consensus building

Model and visualize the relationships

Gain insight into cause-and-effect relationships

Directly input data via the bow-tie builder

Simplify the input process

Customize and report results

Customize colors for a printable report

Use Cases of GRC Solution: A single source of truth

A single source of truth

GRC Solution is able to support you manage the depository and require single source.

Shared frameworks

With no reconciling necessary

Consistent reporting and views

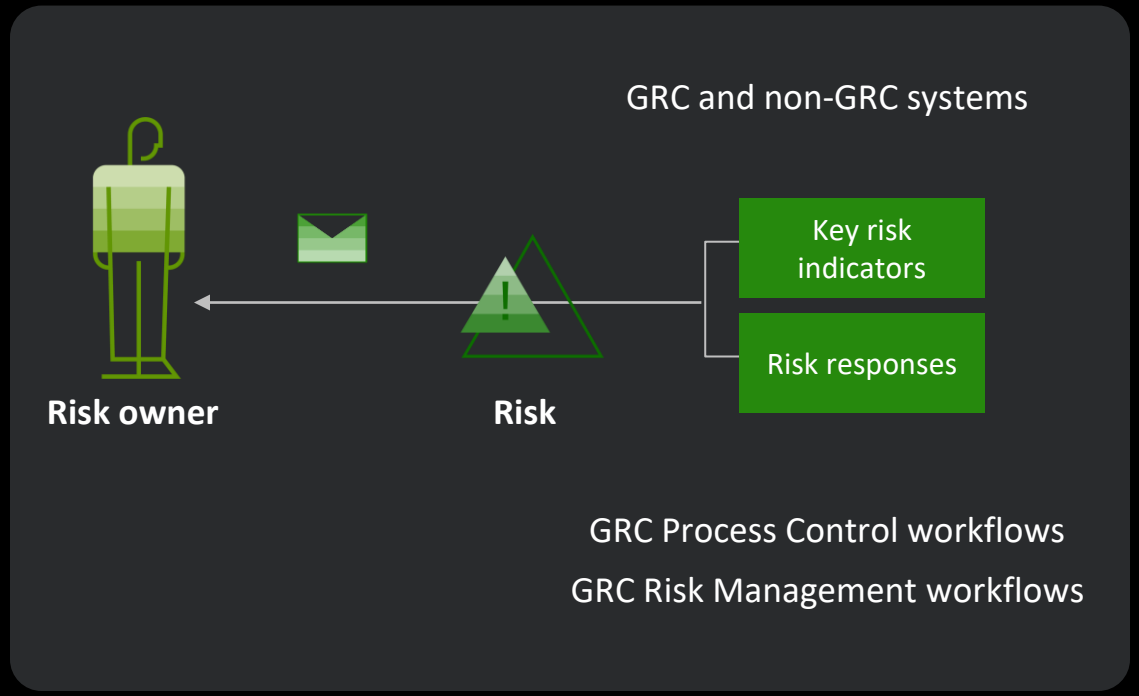
Across the common elements

Clear accountability

Based on ownership

Use Cases of GRC Solution: Continuous monitoring and alerting

Continuous monitoring and alerting



GRC Solution can streamline workflow-driven processes with online or offline tools.

With configurable key-risk indicators

With configurable key-risk indicators

Act

Using automatic e-mail-based reminders and escalations

Monitor performance

Through detailed tracking of risk assessments, evaluations, issues, and remediation plans

Use Cases of GRC Solution: Automation of manual activities

Automation of manual activities

Scheduled activities

Critical activities are driven by due dates

Triggered activities

Data and threshold violations drive action

Exceptional activities

Driven by management review.

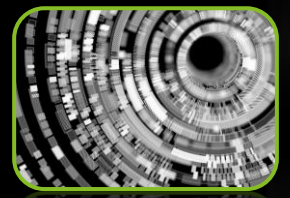
GRC Solution is designed to minimize manual tasks.

Futuristic GRC program aspirations fueled by…

Digital Transformation

Real Time Data and Analytics

Integrations



Modern Technologies e.g., AI, ML

Modern and Interactive Interface

Predictive Analytics

GRC Strategy and Implementation Program Goals

- A solid foundation of streamlined processes, data, people and technology incorporating leading practices
- Synergy across group, process and technology
- Access to real-time actionable data and insights using AI/ML/Advanced Analytics
- End-to-end digital and integrated processes with up-to-date visibility to the core
- A strategy and platform that addresses all GRC processes/ requirements (ERM, ORM, ITRM, TPRM, BCM, Policy Management, Regulatory Compliance and Change Management, TPRM, ESG etc.
- Enable an innovative architecture which is future-proof

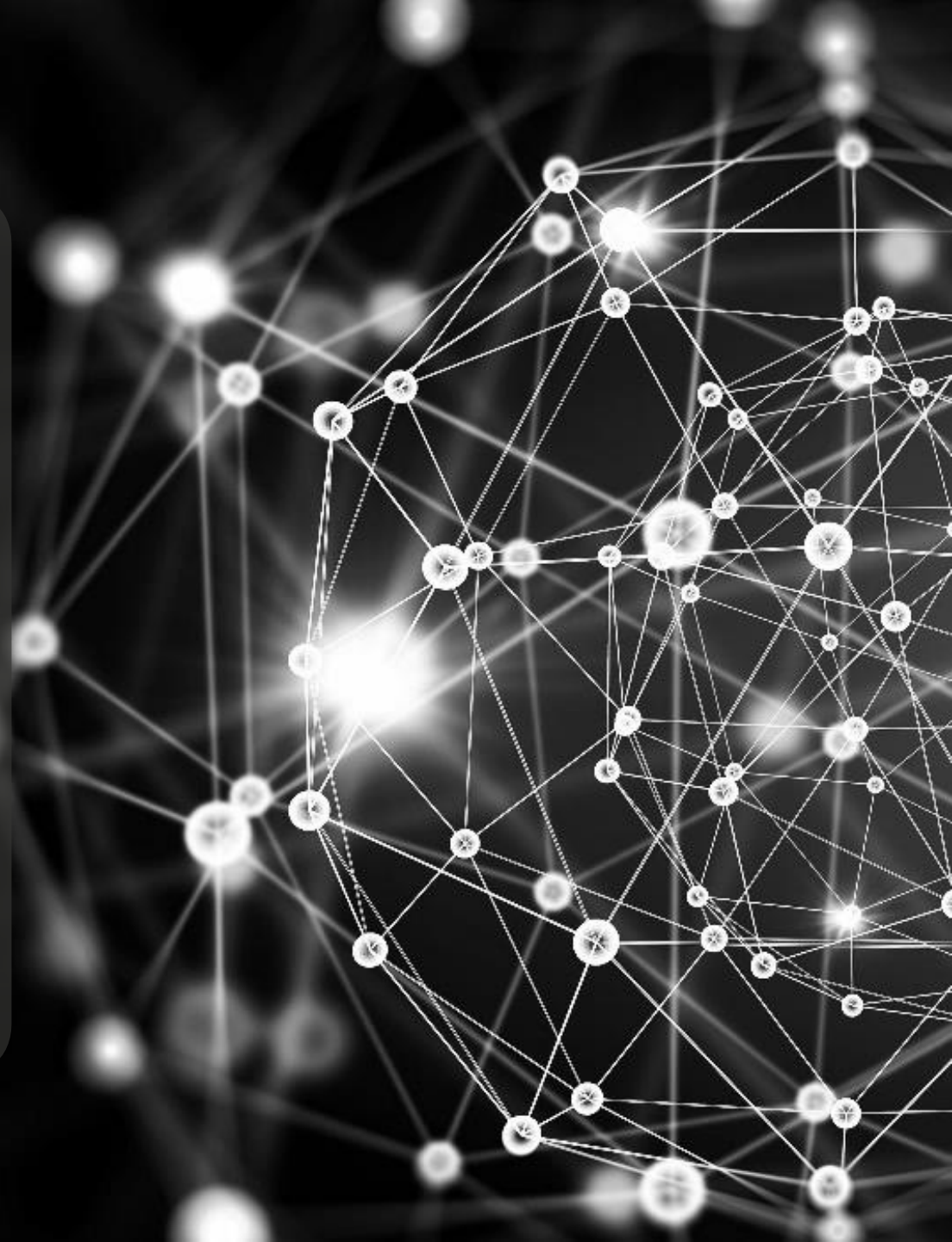
Benefits of GRC Technology Automation

In summary, some of the advantages associated by having an automated GRC tool in place are the following:

- Compliance with regulatory requirements
- Improvement of internal control structure
- Alignment of organisational functions according to best practices
- Risk and control design optimisation
- Risk monitoring and response in time
- Fraud risk mitigation (intentional or error)
- Reasonable level of confidence in internal control
- More efficient management and reduction in manual effort
- Accountability and traceability of the tasks performed
- Integrated and collaborative management of risk and control functions
- Improved reporting and decision-making
- Information consistency and integrity in the model

Agenda

- Making a Start with Overview GRC
- Taking a glance Through each Stage of GRC
- Moving Forward with GRC in Digital Era
- **Accomplishing GRC Integration**



GRC Key Challenges and Learning

	Key Challenges	Leading Practices
Strategy	▪ Establishing an enterprise-wide vision: absence of defined/agreed GRC objectives. ▪ Getting business stakeholders aligned with corporate objectives and working towards a common goal/objective. ▪ Sustaining GRC program in the longer run that is scalable.	• Working with stakeholder to define a common goal and strategy. • Establish ownership and a clear governance and operating model with defined roles and responsibilities. • Establish clear project plan with change and risk management activities.
People	▪ Receiving stakeholder buy-in: stakeholder are not clear on the ROI/payback of getting eGRC right. ▪ Enforcing Risk Culture. ▪ User adoption to new technology and processes.	• Communicate role and responsibilities, and work with stakeholders to own risk for their business unit. • Communicate the intrinsic and extrinsic value of the program. • Build tailored end user training, provide users opportunity to learn and own the system.
Process	▪ Absence of an underlying business architecture, inadequate to provide a holistic view of enterprise processes ▪ Programs and solutions working in siloes and no standardized operating model, risk and control taxonomy, or common reporting nomenclature	• Identify shared/common practices that should be standardized across all functions. • Document integrated process flows to identify areas that would improve visibility amongst the three lines of defense and/ or increase operational efficiency
Technology	▪ Access to the right solutions and/or unrealistic expectations of technology ▪ Insufficient infrastructure planning leading to sub-optimal performance ▪ Delay Failure to effectively deploy, or maintain technology solutions	• Establish processes for building and maintaining solutions in a centrally coordinated and standardized manner • Work with stakeholders to understand infrastructure requirements prior to installing the technology and establishing priorities for automation of processes
Data	▪ Lack of foundational data ▪ Failure to agree upon a common taxonomy ▪ Historical data cleansing and migration into an integrated eGRC solution	• Refine existing foundational data to align with a common taxonomy • Work with executive teams to identify and establish roles and responsibilities for ownership and maintenance of data • Develop a strategic plan for data migration

Deloitte's *Transformation Intelligence* framework will allow you to align on your *business ambition*, understand your *aptitude to change*, and generate *a customized change program*

- Right-sized approach
- Accelerated delivery
- AI and insights-driven
- Enterprise visibility
- Develop internal capability

Nassaya Sitthichokvarodom
Director, Risk Advisory
Tel: +66 (0) 2 034 0000 Ext. 14037
nsitthichokvarodom@deloitte.com

Deloitte.

Deloitte.

Deloitte Touche Tohmatsu Jaiyos Advisory Co.,Ltd.
AIA Sathorn Tower, 23rd – 27th Floor.
11/1 South Sathorn Road
Yannawa, Sathorn
Bangkok 10120, Thailand

Tel: +66 (0) 2 034 0000
www.deloitte.com

Deloitte.