أنظمة الرقابة المؤسسية المتكاملة

Governance, Risk management and Compliance Integrated Systems

Prof Akram Hassan SME@PMI

Prof. Akram Hassan Shared in 12 Standards
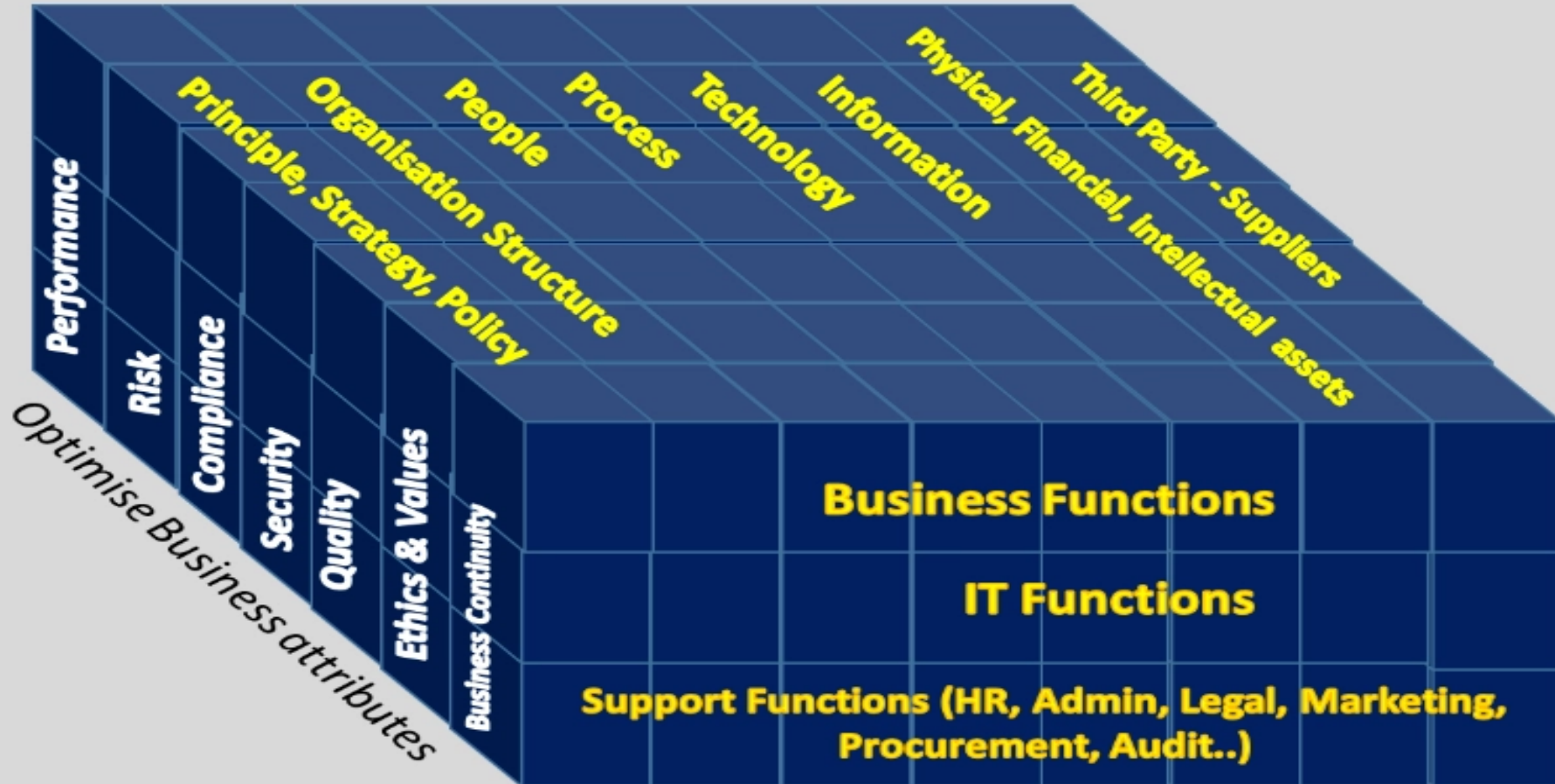
METAVERSE

Business Security

Data privacy risk

IT risk

101010 010101

Regulatory risk

Compliance

CRO CFO

CIO CCO

Model risk

Fraud risk

Operational risk

Disjointed GRC

1- Governance

- Governance is the oversight role and the process by which companies manage and mitigate business risks. The governance process within an organization includes elements such as:
  - o **Definition** and communication of corporate control and key policies, enterprise risk management, Regulatory and compliance management
  - o **Oversight** (e.g., compliance with ethics and options compliance as well as overall oversight of regulatory issues)
  - o **Evaluate** business performance through balanced scorecards, risk scorecards and operational dashboards.

Good Governance Principles

Deloitte Governance Framework

2- Risk Management

- Risk management enables an organization to evaluate all relevant business and regulatory risks and controls and monitor mitigation actions in a structured manner.
- With the recent increase in regulatory mandates and increasingly activist shareholders, many organizations have become sensitized to identifying and managing areas of risk in their business: whether it is financial, operational, IT, brand or reputation related risk.
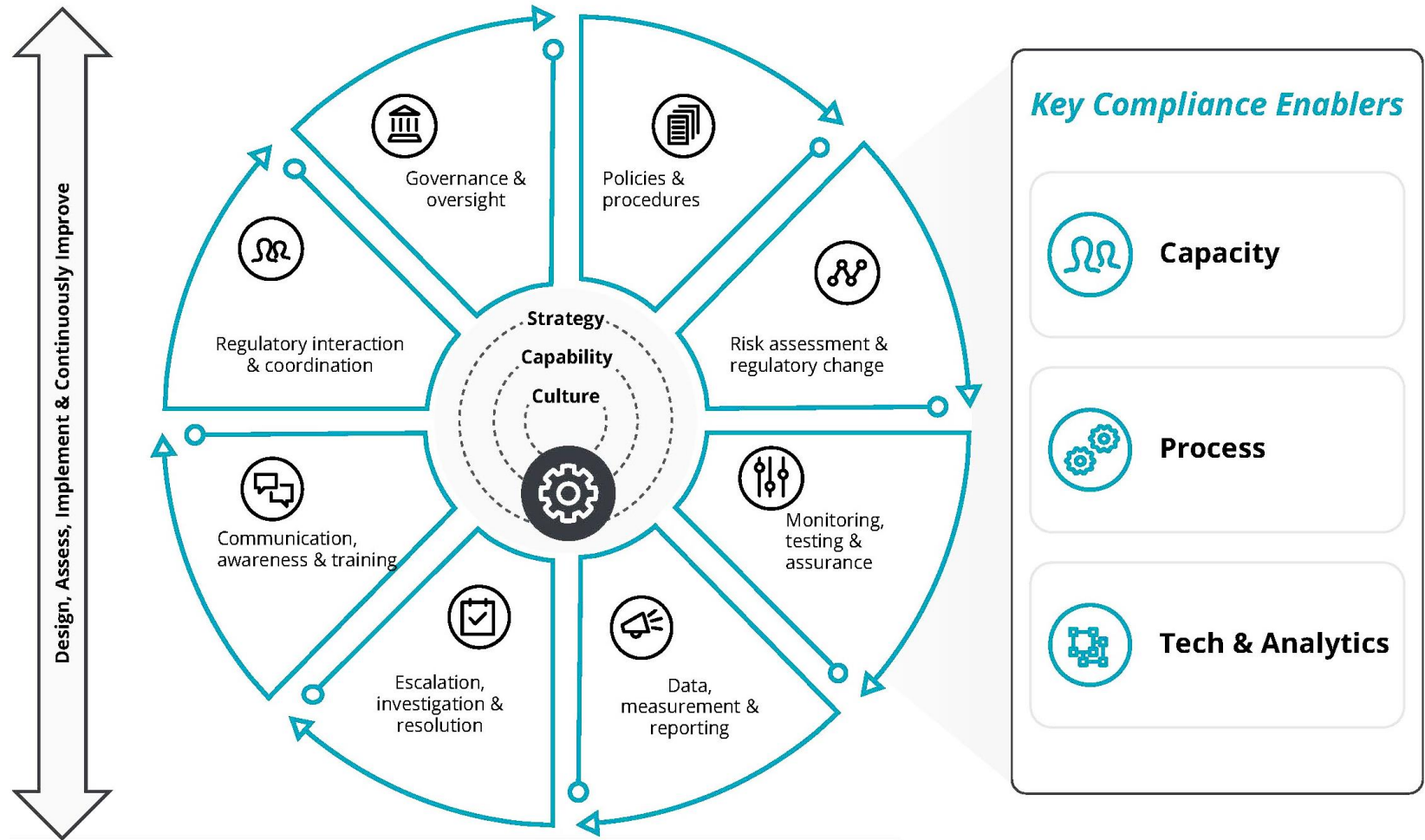
Risk Management Framework

3- Compliance

- Compliance ensures that an organization has the processes and internal controls to meet the requirements imposed by governmental bodies, regulators, or internal policies.
- Compliance is not a one-time event - organizations realize that they need to make it into a repeatable process, so that they can continue to sustain compliance with that regulation at a lower cost.
- When an organization is dealing with multiple regulations at the same time, a streamlined process of managing compliance with each of these initiatives is critical, or else, costs can spiral out of control and the risk of non-compliance increases.

Deloitte Compliance Framework

Design, Assess, Implement & Continuously Improve

Governance & oversight

Policies & procedures

Regulatory interaction & coordination

Risk assessment & regulatory change

Strategy
Capability
Culture

Communication, awareness & training

Monitoring, testing & assurance

Escalation, investigation & resolution

Data, measurement & reporting

Key Compliance Enablers

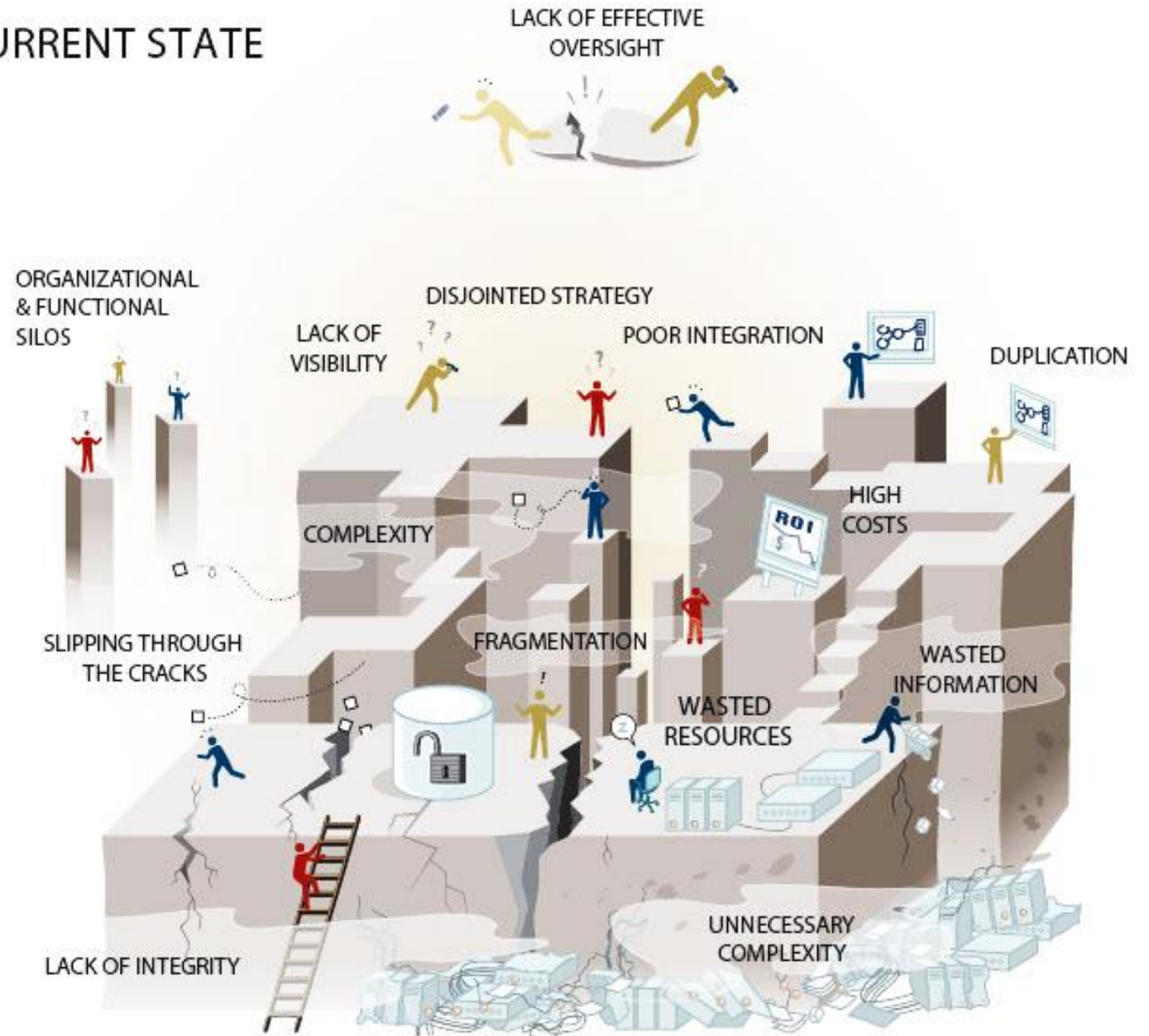Capacity

Process

Tech & Analytics

13

Disjointed GRC Done Wrong

- Unfortunately, Governance, risk and compliance departments and programs are often siloed, ineffective and yield troubling drawbacks:
  - High costs
  - Lack of visibility into risks
  - Inability to address third party risks
  - Difficulty measuring risk-adjusted performance
  - Too many negative surprises

Disjointed GRC Done Wrong

CURRENT STATE

LACK OF EFFECTIVE OVERSIGHT

ORGANIZATIONAL & FUNCTIONAL SILOS

DISJOINTED STRATEGY

LACK OF VISIBILITY

POOR INTEGRATION

DUPLICATION

HIGH COSTS

COMPLEXITY

SLIPPING THROUGH THE CRACKS

FRAGMENTATION

WASTED INFORMATION

WASTED RESOURCES

LACK OF INTEGRITY

UNNECESSARY COMPLEXITY

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

Integrated GRC Done Right

- When GRC is done right, the benefits accrue. Organizations that integrate GRC processes and technology across all silos have:
    - Reduced costs
    - Reduced duplication of activities
    - Reduced impact on operations
    - Achieved greater information quality
    - Achieved ability to gather information quickly and efficiently
    - Achieved ability to repeat processes in a consistent manner

Integrated GRC Done Right

FUTURE STATE

EFFECTIVE OVERSIGHT

ETHICS

INTEGRATED REPORTING & ANALYTICS

INTEGRITY

INTEGRATED GRC STRATEGY

Business Operators

Financial Officer

Legal, HR, IT + Other

Audit Executive

Risk Executive

Compliance Executive

INTEGRATED RISK & CONTROL ACTIVITIES

INTEGRATED & QUALITY INFORMATION

SHARED TECHNOLOGY

SHARED SERVICES

COMMON METHODS   COMMON VOCABULARY

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

GRC Definition

- GRC is the integrated collection of capabilities that enable an organization to reliably achieve objectives, address uncertainty and act with integrity
- GRC represents the capabilities that integrate the governance, management and assurance of performance, risk and compliance activities
- GRC is viewed as an integrated collection of all capabilities necessary to support Principled Performance and does not burden the business, it supports and improves it.
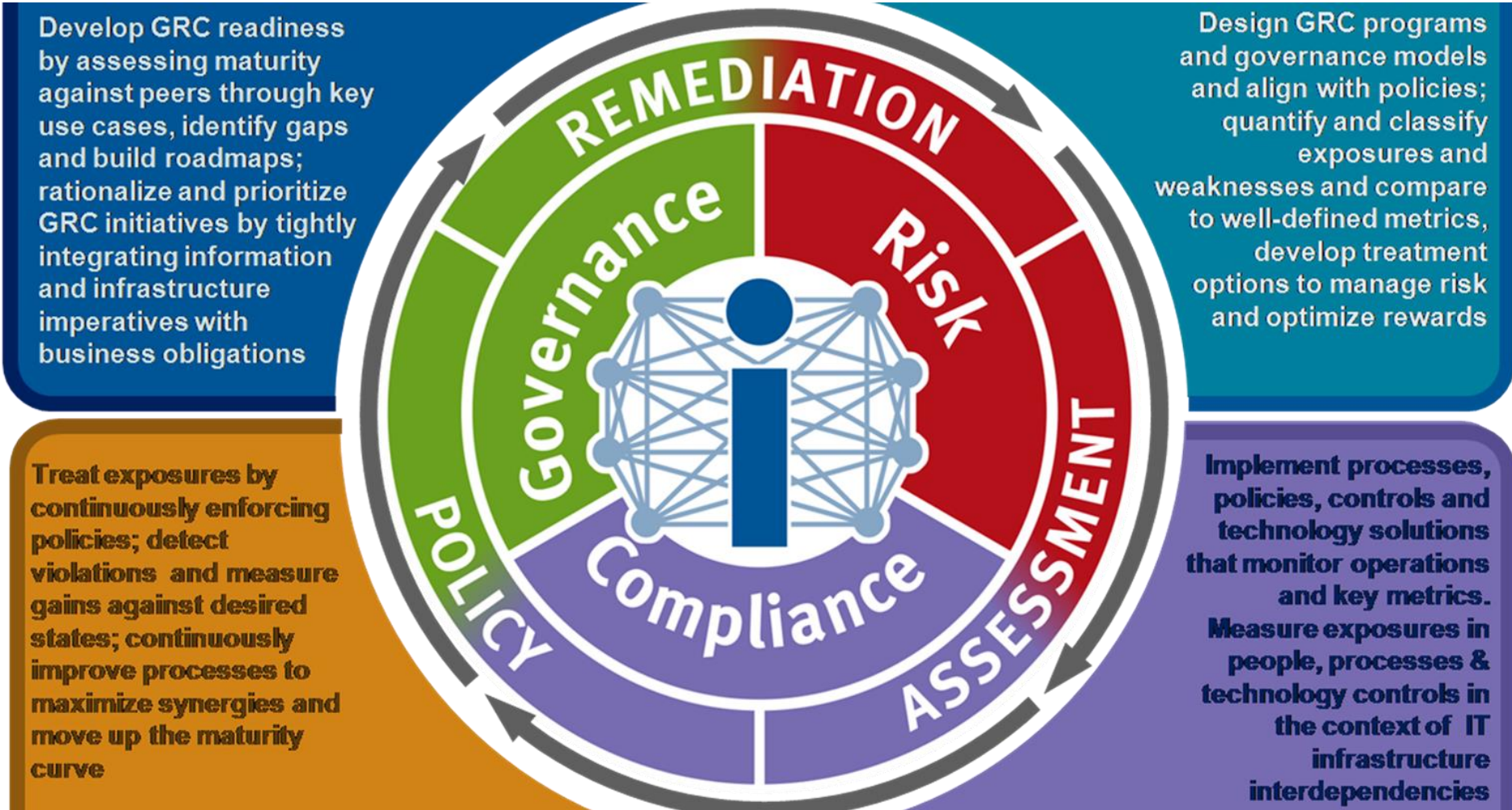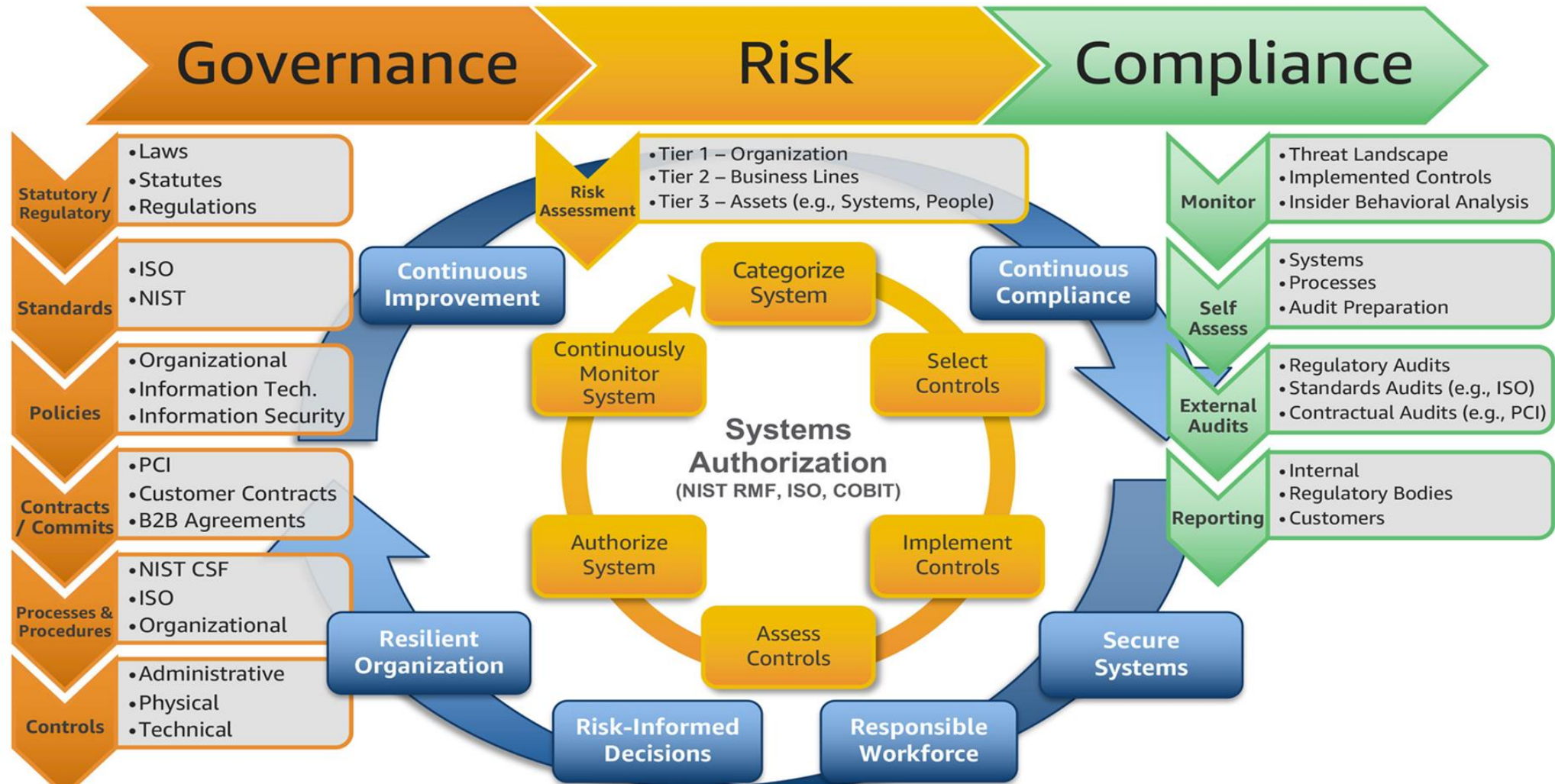
GRC Domains

GRC Drivers

- Stakeholders demand high performance along with high levels of transparency
- Regulations and enforcement are ever-changing and unpredictable
- Exponential growth of third-party relationships and risk is a
- management challenge
- The costs of addressing risks and requirements are spinning out of control
- The harsh (and scary) impact when threats and opportunities are not identified.
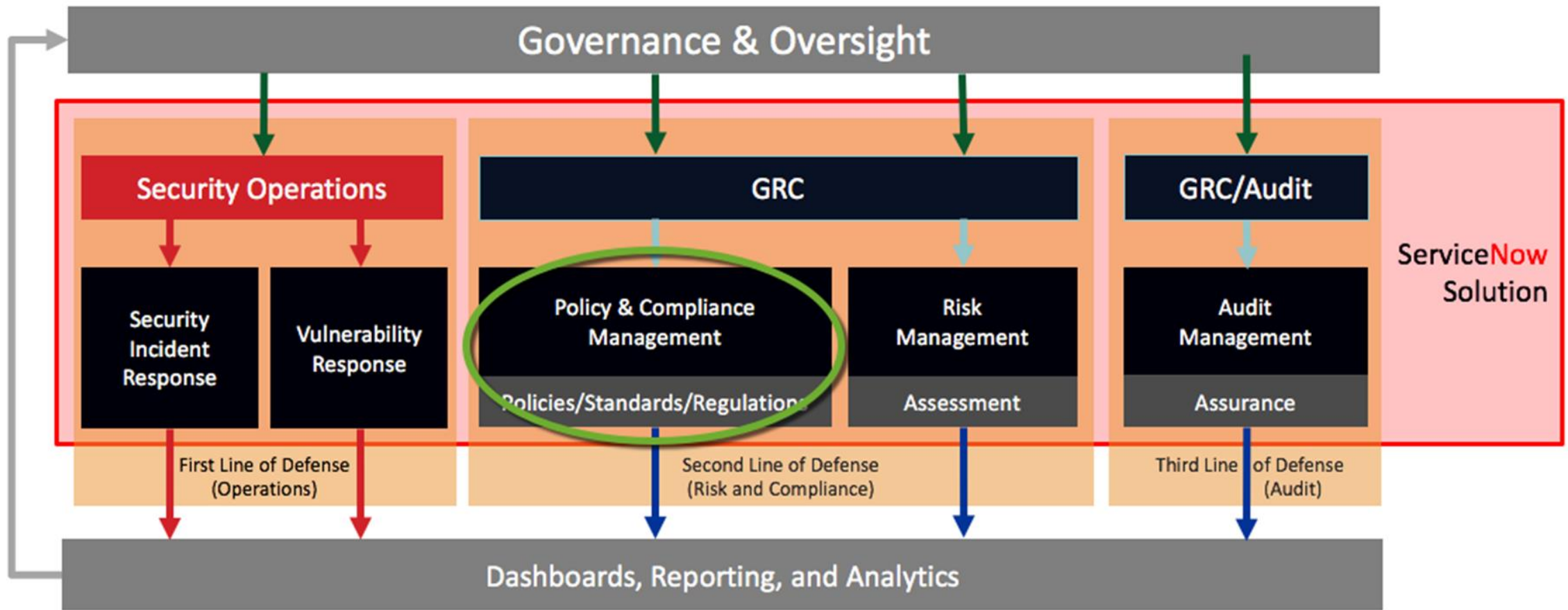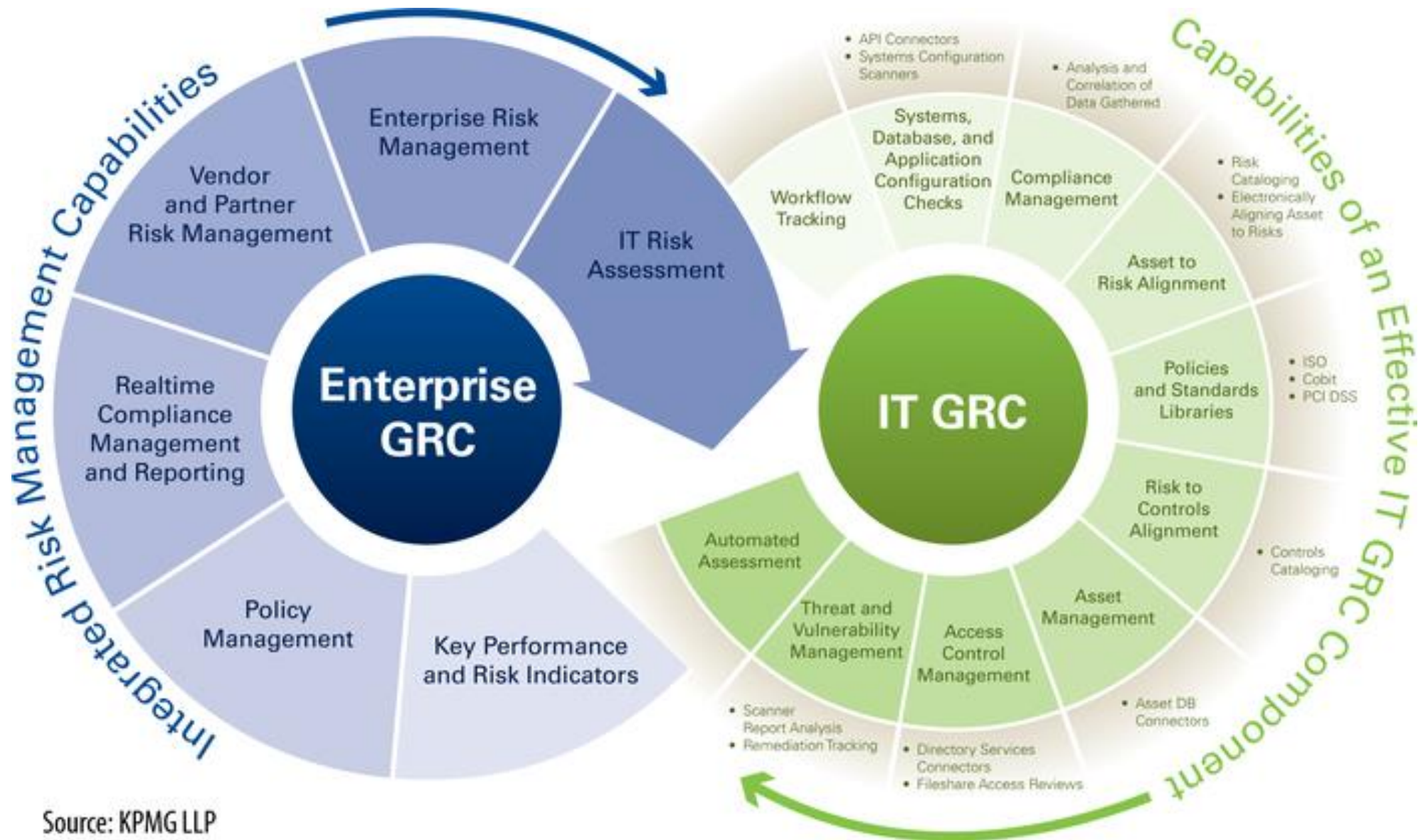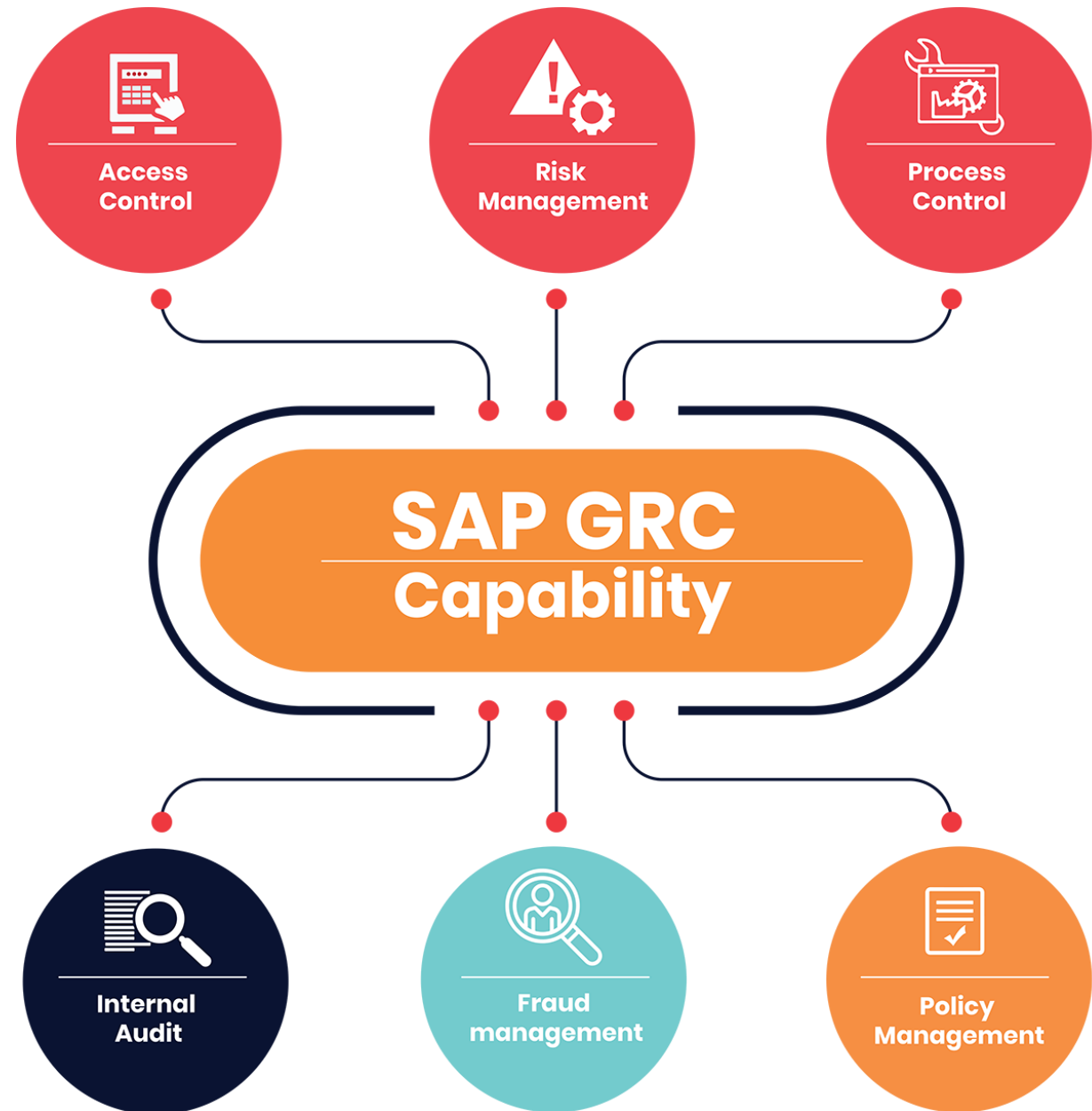
GRC Framework

- Clear levels of accountability for board, management and key staff responsible for risk management

- Risk assessment framework is understood and managed by the business

Governance structure

Risk assessment

Sustainable process

Compliance

- Updated at least annually as part of business planning process

- Optimise investments to update compliance programmes and activities

GRC Lifecycle

GRC Processes

GRC Integrated Systems

Source: KPMG LLP

GRC Software

Access Control

Risk Management

Process Control

SAP GRC Capability

Internal Audit

Fraud management

Policy Management
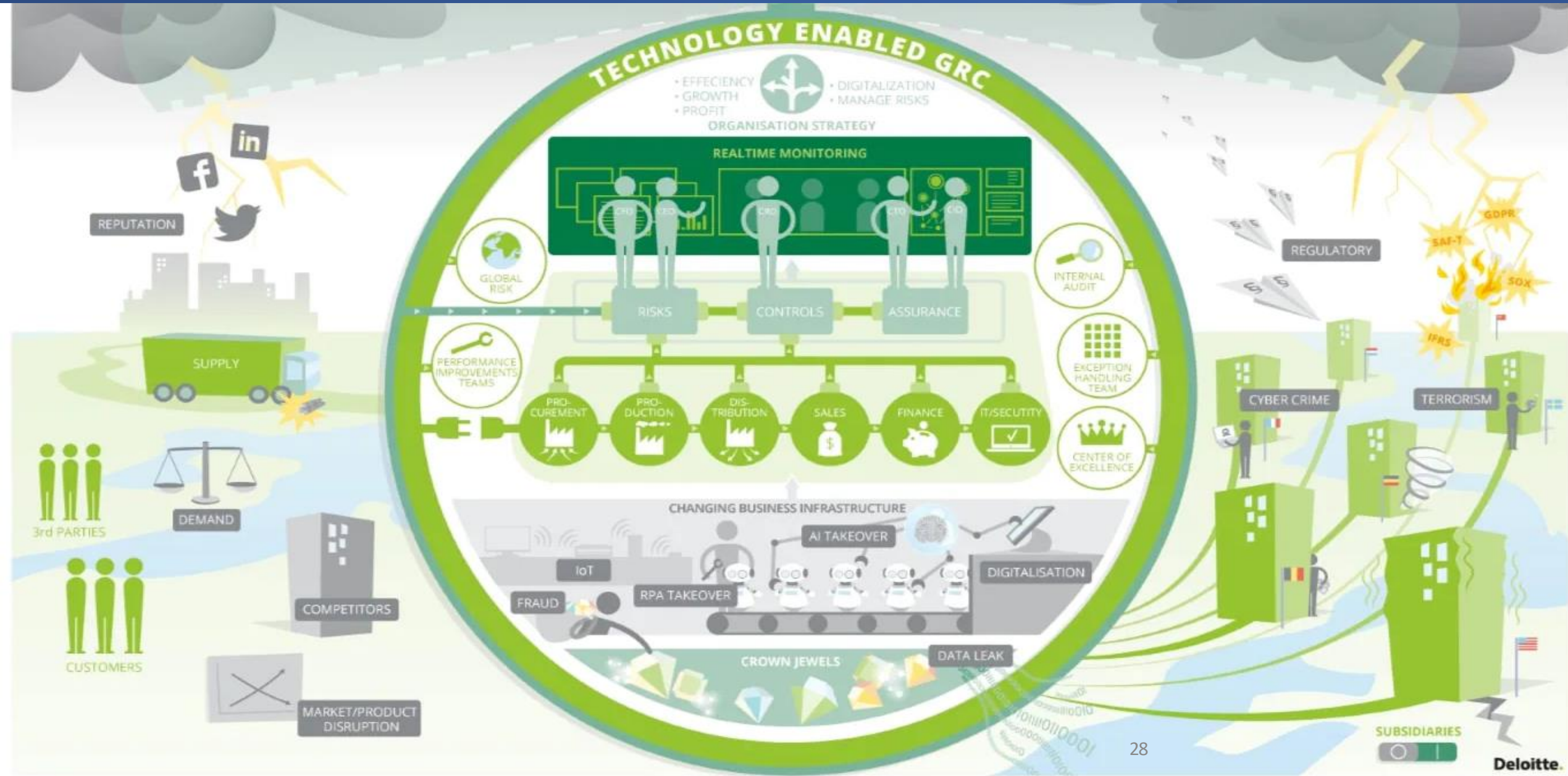
Governance, Risk management and Compliance Integrated Systems

Prof Akram Hassan
SME@PMI
akramkram@yahoo.com
+201014356420

Stay connected!