Going beyond the Sample:

End-to-end integrated data-driven GRC methodology

The Institute of
Internal Auditors

Jacob Wanjohi

10th May 2022

19th Annual Seminar

FACT!

"If you don't have relationships, the tool by itself doesn't solve the problem."

The Institute of
Internal Auditors

Foundation

Brick

Wall

Castle

Internal Audit function is more than checking boxes, verifying signatures, and recalculating figures.

IA- verify that processes are **BUILT RIGHT** and **RUN RIGHT!**

This includes goal setting, staff preparedness, reporting lines, risk mitigation, control activities, performance monitoring mechanisms, escalation procedures, assurance and support governance.

Journey to 100%?

SAMPLE
From- To
100%
POPULATION

The Institute of
Internal Auditors

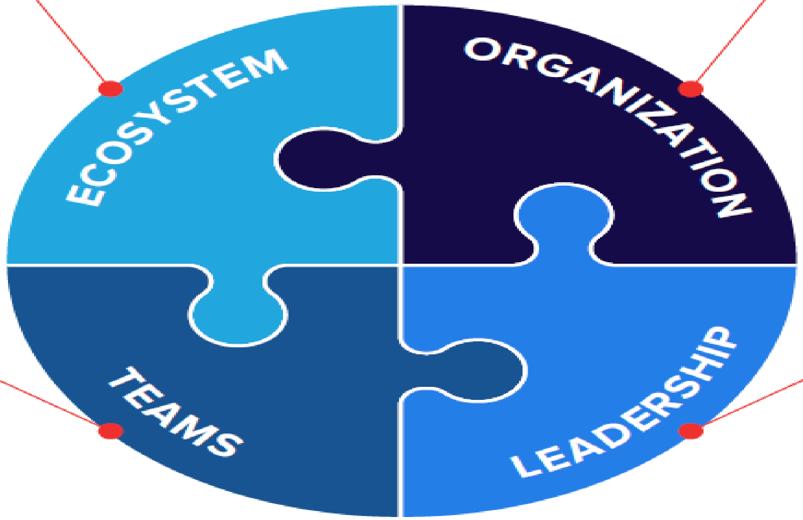
Stakes

ECOSYSTEM

Ecosystem is the environment in which the organization operates, driven by purpose, culture and **tone at the top**. Build an infrastructure that helps the organization meet its IA goals and puts purpose/Strategy at core

TEAMS

Teams thrive when automation and workflows maximize time and efficiencies. Enable real-time collaboration and innovation in one secure ecosystem.



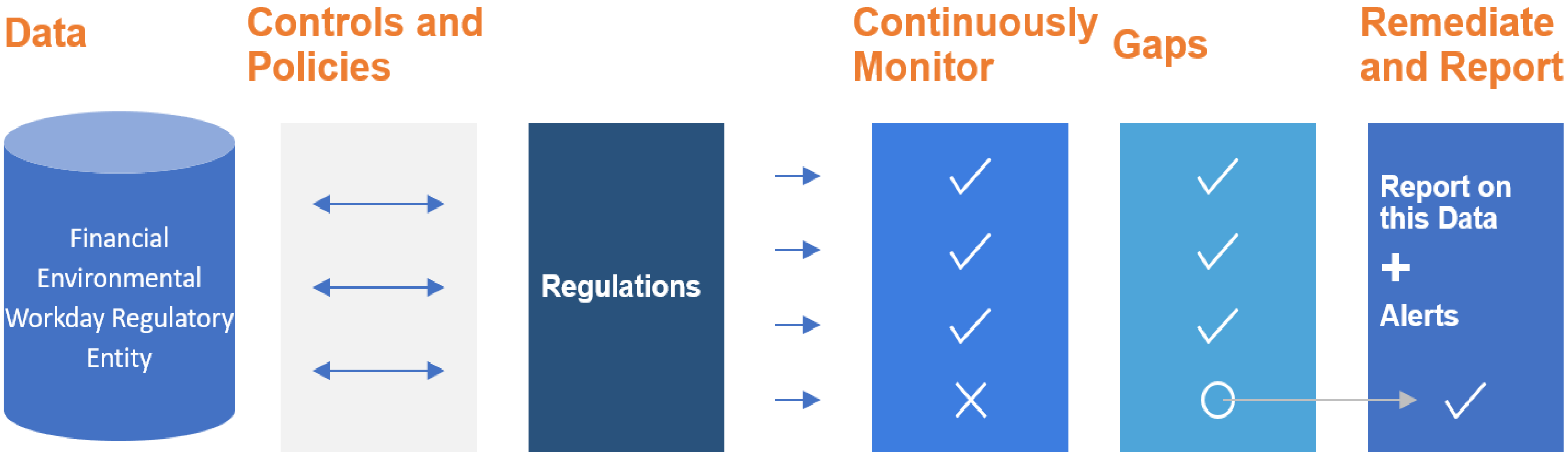
ORGANIZATION

Organization represents the network of tools and capabilities that connect departments with one another. Drive collaboration with transparency, data and intelligence across the organizational structure.

LEADERSHIP

Leadership operates on secure platforms that keep information protected. Safeguard sensitive communication between management, the board and trusted third parties – and ensure a dedicated channel for times of crisis.

GRC & Data


Data

Controls and Policies

Continuously Monitor

Gaps

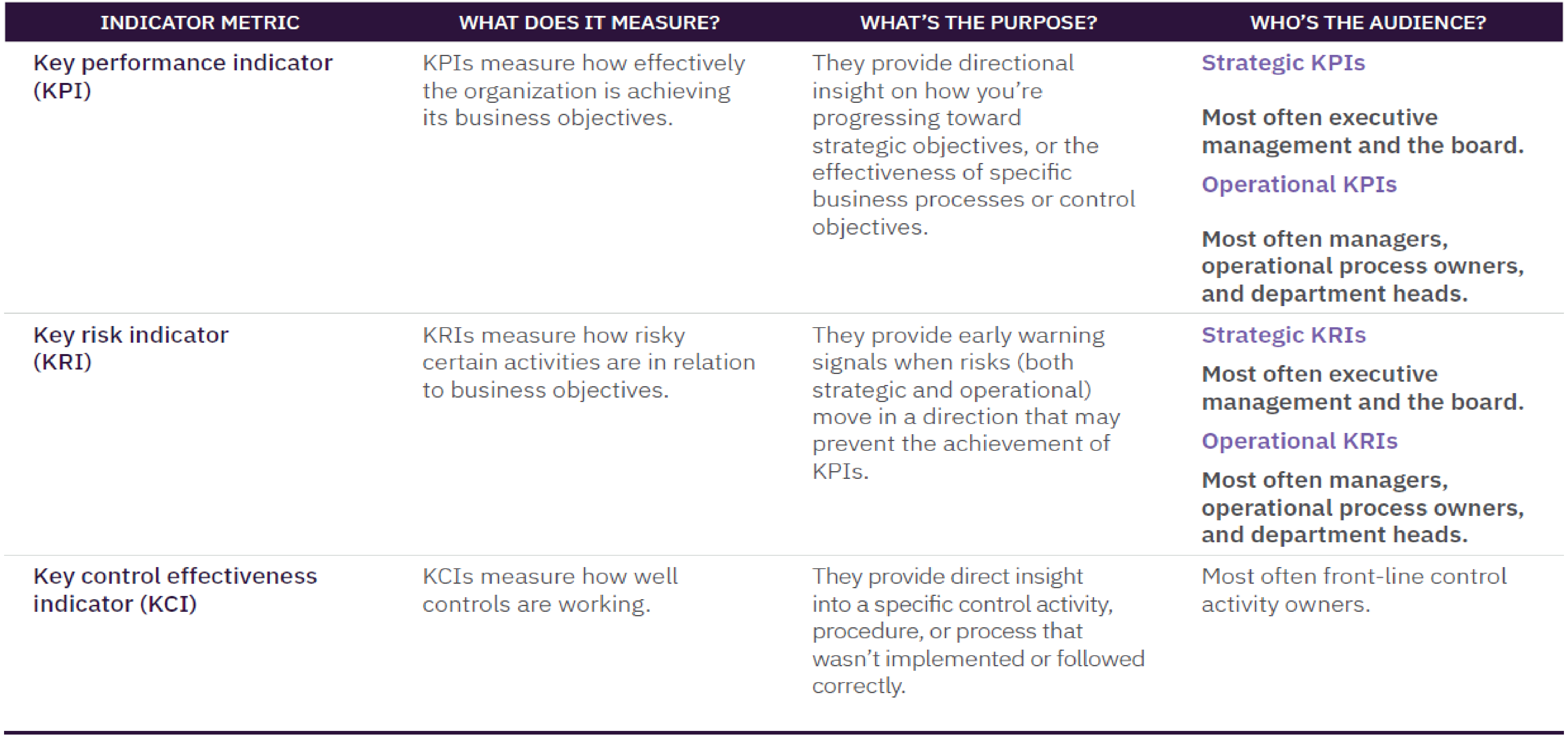
Remediate and Report

Financial
Environmental
Workday Regulatory
Entity

Regulations

Report on this Data
+
Alerts

KPI, KRI, KCI



INDICATOR METRIC	WHAT DOES IT MEASURE?	WHAT'S THE PURPOSE?	WHO'S THE AUDIENCE?
Key performance indicator (KPI)	KPIs measure how effectively the organization is achieving its business objectives.	They provide directional insight on how you're progressing toward strategic objectives, or the effectiveness of specific business processes or control objectives.	**Strategic KPIs** **Most often executive management and the board.** **Operational KPIs** **Most often managers, operational process owners, and department heads.**
Key risk indicator (KRI)	KRIs measure how risky certain activities are in relation to business objectives.	They provide early warning signals when risks (both strategic and operational) move in a direction that may prevent the achievement of KPIs.	**Strategic KRIs** **Most often executive management and the board.** **Operational KRIs** **Most often managers, operational process owners, and department heads.**
Key control effectiveness indicator (KCI)	KCIs measure how well controls are working.	They provide direct insight into a specific control activity, procedure, or process that wasn't implemented or followed correctly.	Most often front-line control activity owners.

The Institute of
Internal Auditors
Elevating Impact

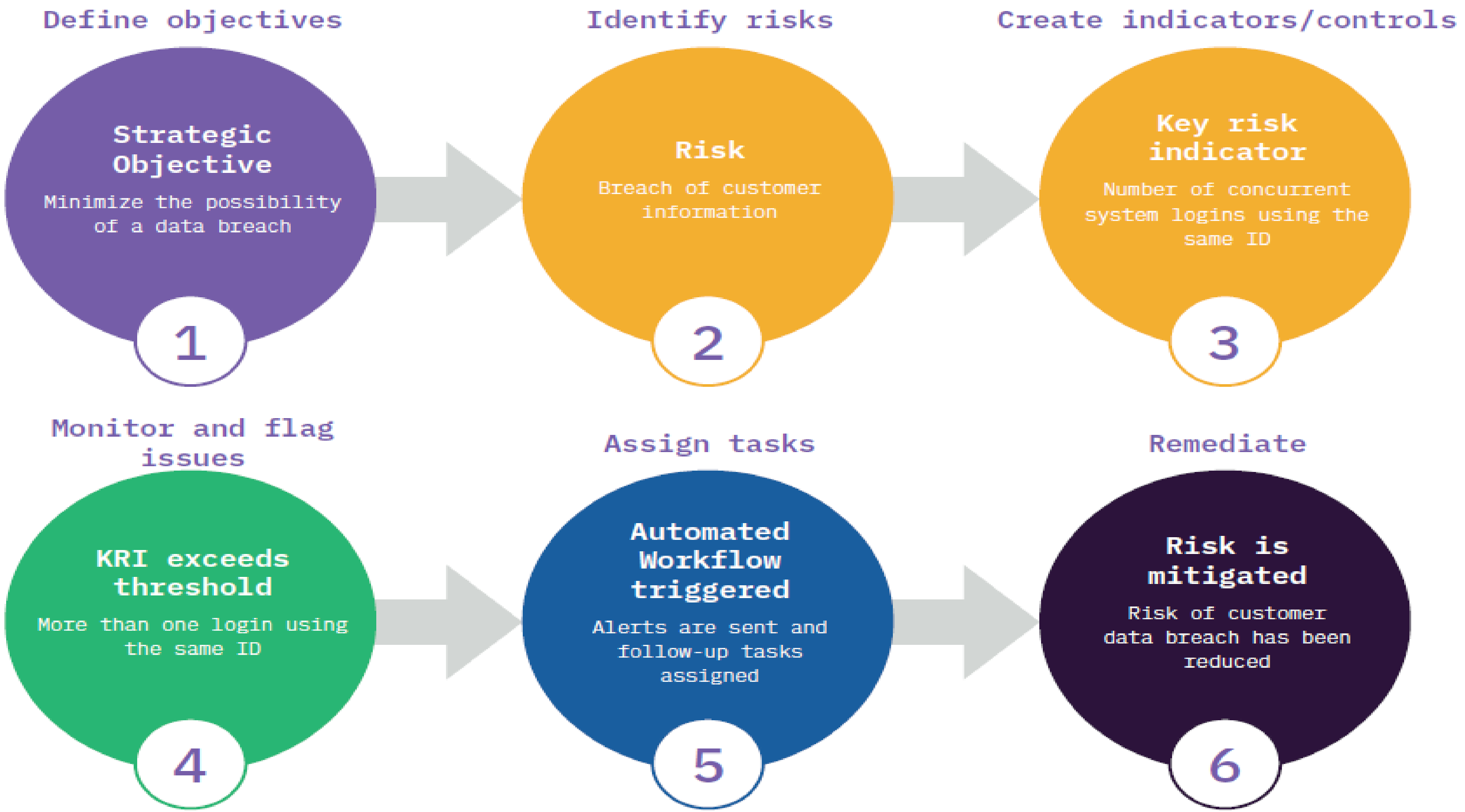
TYPES OF KRI

Leading indicators. Emerging risk trends for events that might happen in the future and need to be addressed. For example, the number of employees who click on fake phishing emails.

Current indicators. Where you currently sit with your risk exposure. For example, the number of staff who haven’t completed mandatory security training.

Lagging indicators. Events which took place in the past and could occur again. For example, the time between employee termination and deletion of accounts

USE OF KRI



Define objectives

Strategic Objective

Minimize the possibility of a data breach

1

Identify risks

Risk

Breach of customer information

2

Create indicators/controls

Key risk indicator

Number of concurrent system logins using the same ID

3

Monitor and flag issues

KRI exceeds threshold

More than one login using the same ID

4

Assign tasks

Automated Workflow triggered

Alerts are sent and follow-up tasks assigned

5

Remediate

Risk is mitigated

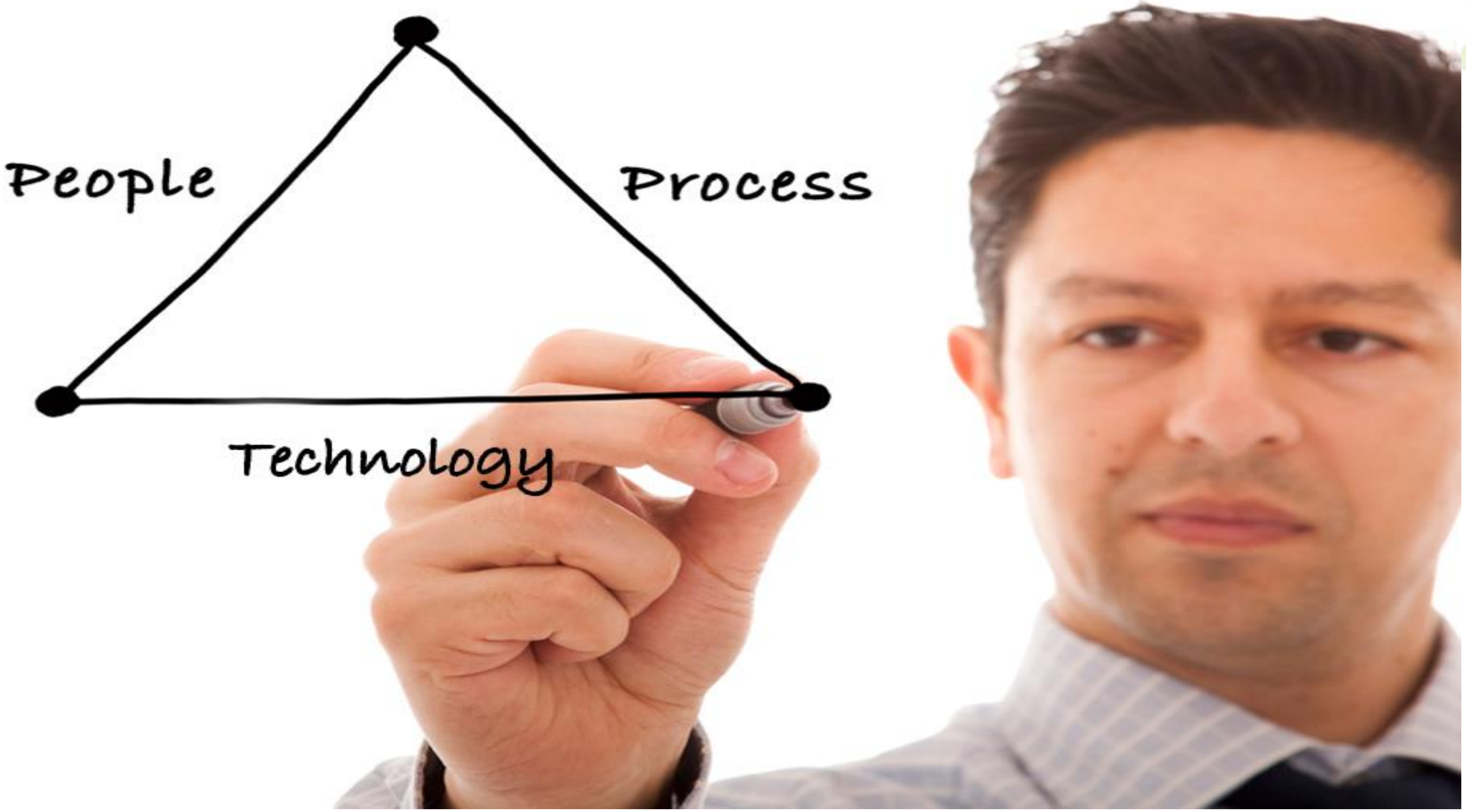
Risk of customer data breach has been reduced

6

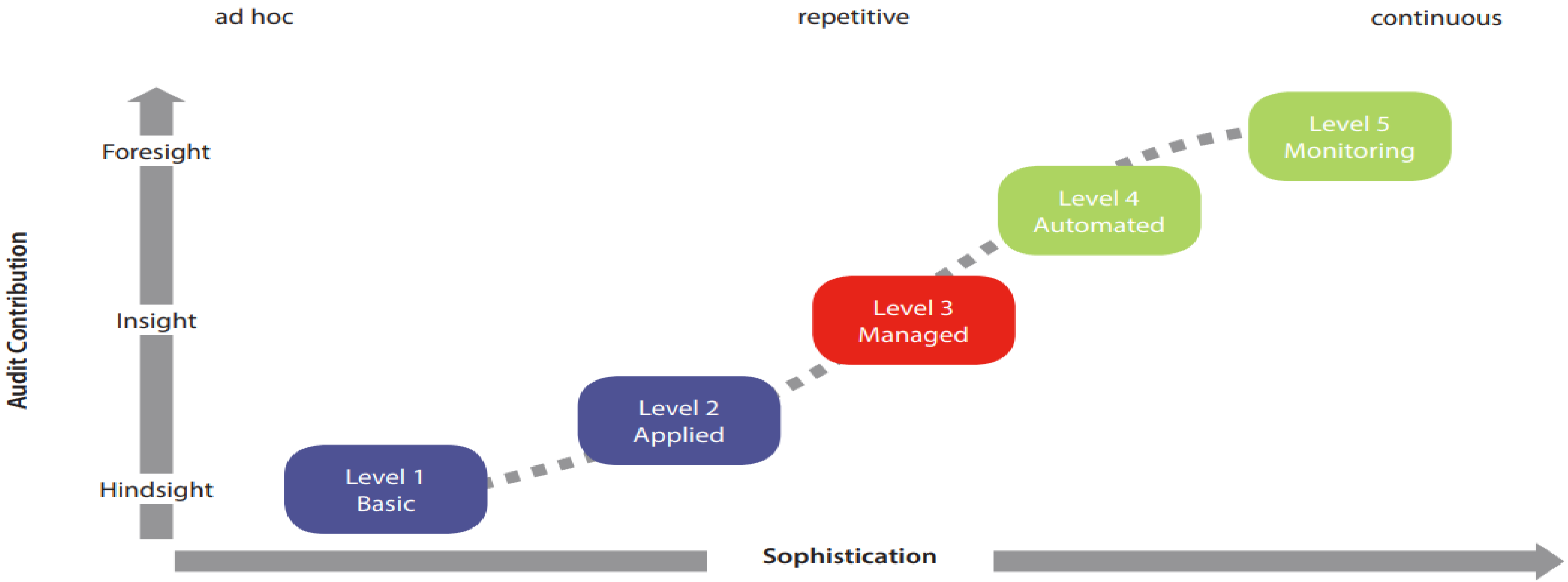
The Institute of Internal Auditors

Elevating Impact

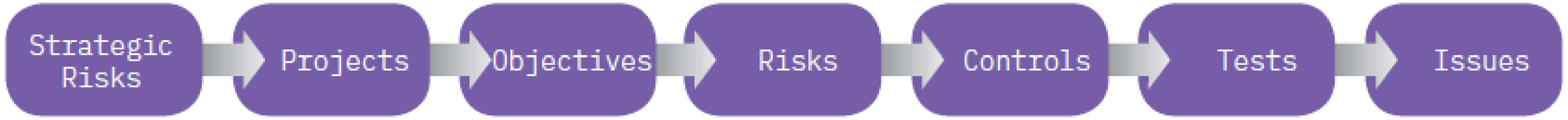
PPT- Model



IA- Contribution to Assurance



Step 1- Simple & Practical



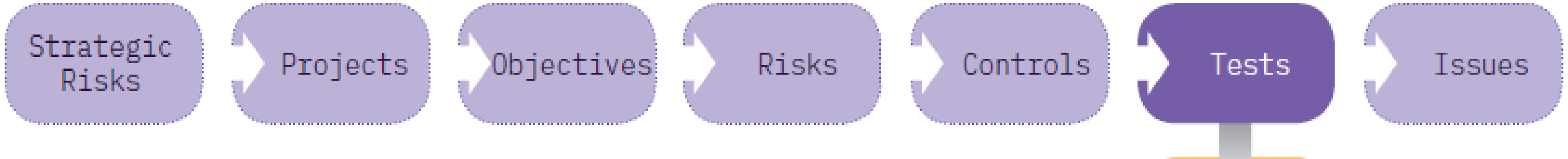
Benefit: Better view of risk and control issues within a given audit area- Time saving

Challenge: - Data access and data knowledge to support the test required

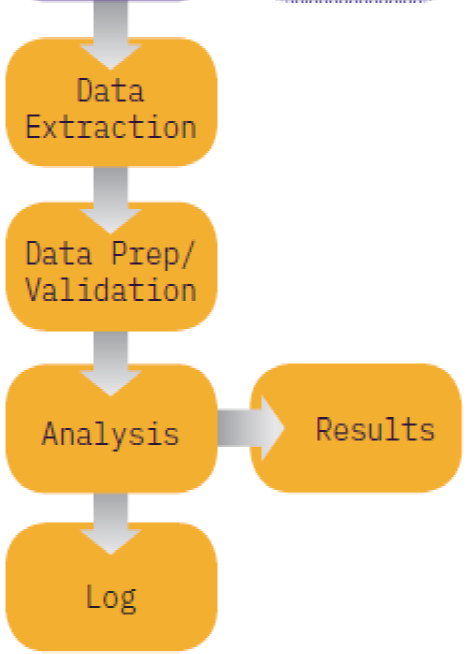
Optimization:

PEOPLE	PROCESS	TECHNOLOGY
• **Train Team** • **Link with IT** • **Have IA- resource - IS Auditor**	• Start with Simple Plan • Identify scope- data analysis • Liaise with IT • Data Accuracy • Determine Output	• Ensure- technology support • Environment- Support large data • Ensure Audit Logging

Step 2- Leverage Data Analysis



Strategic Risks
Projects
Objectives
Risks
Controls
Tests
Issues



Data Extraction
Data Prep/ Validation
Analysis
Results
Log

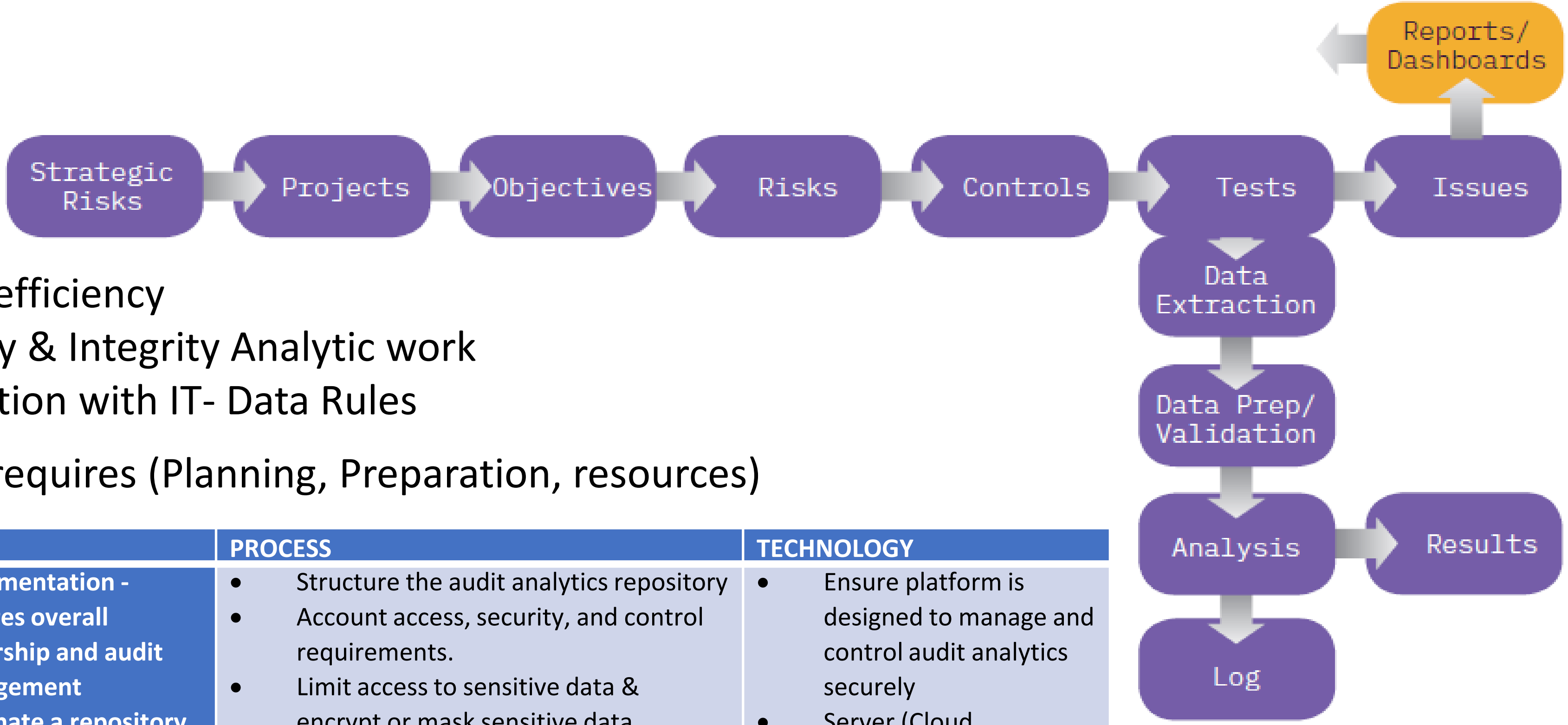
Benefits: - Analytics transform the audit process- higher assurance
- More coverage, less manual, no sampling

Challenge: - Occasional use & making Analytics Core part of audit
- Ownership & responsibility

Optimization:

PEOPLE	PROCESS	TECHNOLOGY
• **Assign overall responsibility- Analytics** • **Consider technical and audit expertise** • **Develop and train specialists in data access** • **Ensure management reviews test logic and results**	• Define and broadly communicate goals and objectives- Resources & Investments • Develop procedures for quality control of analytics development • Develop a comprehensive audit analytics program plan that can evolve to meet the needs of subsequent Audit needs	• If data access challenges exist, consider specialized data connectors (e.g., SAP or other core business systems)

Step 3- Integrate GRC & data analysis



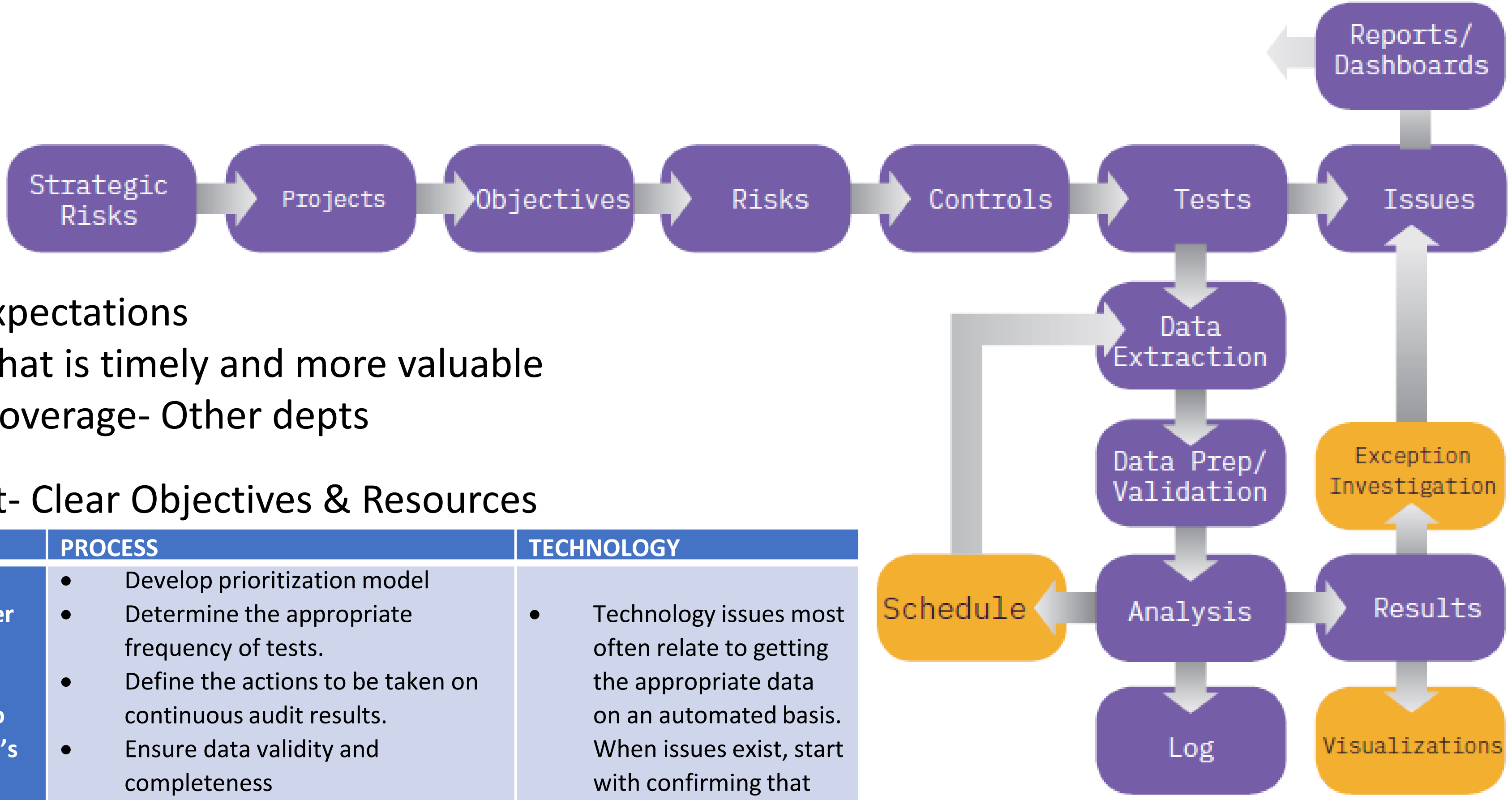
Benefits: - Improves team efficiency
- Improves quality & Integrity Analytic work
- More Collaboration with IT- Data Rules

Challenge: CAE & IA team requires (Planning, Preparation, resources)

Optimization:

PEOPLE	PROCESS	TECHNOLOGY
• Implementation - requires overall leadership and audit management • Designate a repository administrator who understands the audit organization and processes,	• Structure the audit analytics repository • Account access, security, and control requirements. • Limit access to sensitive data & encrypt or mask sensitive data • Completeness and validity of repository data • Standardize localization and structure.	• Ensure platform is designed to manage and control audit analytics securely • Server (Cloud preference) support the central server-managed analytics platform.

Step 4- Leverage CA for real-time insight



Strategic Risks

Projects

Objectives

Risks

Controls

Tests

Issues

Reports/ Dashboards

Data Extraction

Data Prep/ Validation

Analysis

Schedule

Results

Exception Investigation

Log

Visualizations

Benefits: - Meets the increasing expectations

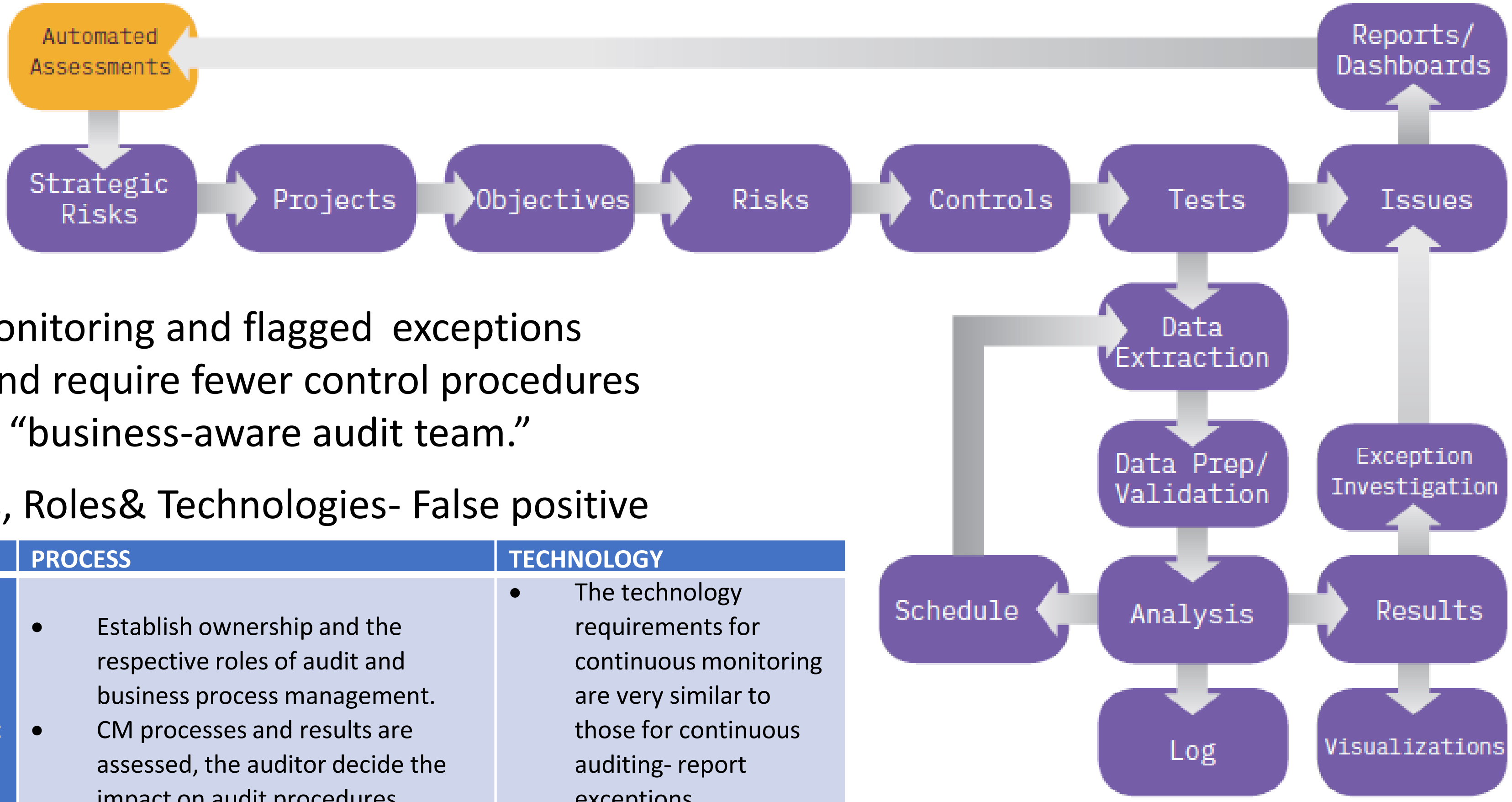
- Insight and assurance that is timely and more valuable
- Trends and Triggers – Coverage- Other depts

Challenge: To be led by Senior Mgt- Clear Objectives & Resources

Optimization:

PEOPLE	PROCESS	TECHNOLOGY
• Designate a continuous auditing program manager who is responsible for leading and coordinating. • Modify work processes so that an individual auditor's continuous auditing responsibilities fit in with other audit roles	• Develop prioritization model • Determine the appropriate frequency of tests. • Define the actions to be taken on continuous audit results. • Ensure data validity and completeness • Create procedures for modifying tests. & test for failed task run	• Technology issues most often relate to getting the appropriate data on an automated basis. When issues exist, start with confirming that the right data is available.

Step 5 - Integrate GRC & CM for data-driven GRC



Benefits: - Continuous transaction monitoring and flagged exceptions
- Effectiveness of controls and require fewer control procedures
- "audit-aware business." & "business-aware audit team."

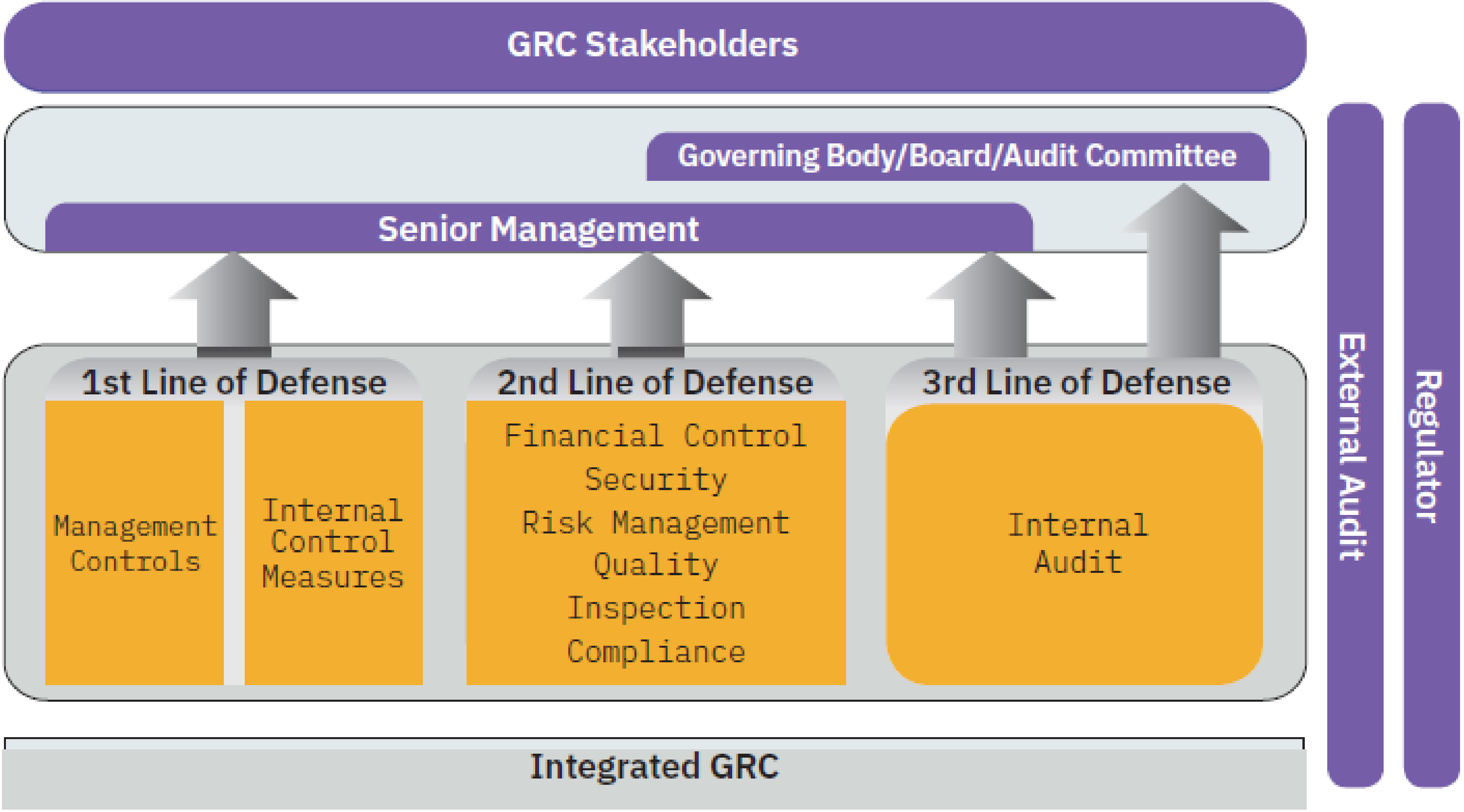
Challenge: Building Blocks- Processes, Roles& Technologies- False positive

Optimization:

PEOPLE	PROCESS	TECHNOLOGY
• Assign overall responsibility for the ongoing success of the continuous monitoring processes to an appropriate person. Process NOT Project • Allocate resources to the review and follow up of exceptions according to the nature and severity of the exceptions identified.	• Establish ownership and the respective roles of audit and business process management. • CM processes and results are assessed, the auditor decide the impact on audit procedures • Continuous monitoring tests should be validated – Minimise false positives	• The technology requirements for continuous monitoring are very similar to those for continuous auditing- report exceptions • Dashboards on the status of CM. Overall business trends- Risks

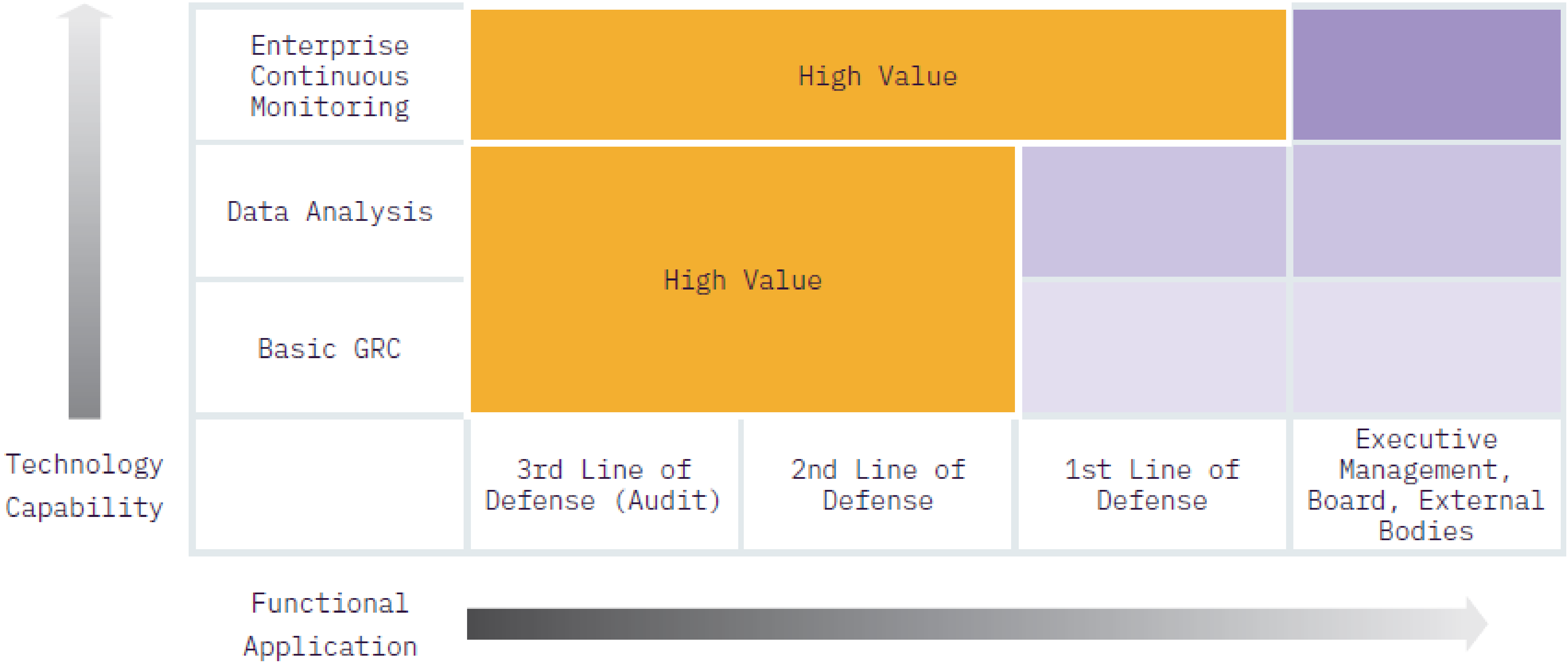
The Institute of
Internal Auditors
Elevating Impact

End to End GRC View- 3 LoD



The Institute of Internal Auditors
Elevating Impact

Technology Approach



	3rd Line of Defense (Audit)	2nd Line of Defense	1st Line of Defense	Executive Management, Board, External Bodies
Enterprise Continuous Monitoring	High Value			
Data Analysis	High Value			
Basic GRC				

The Diligent Platform

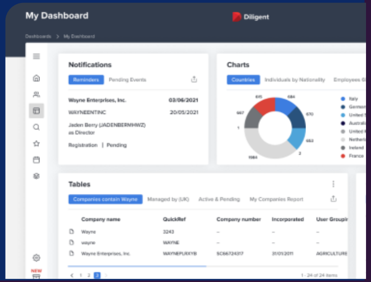
Board and C-Suite

Integrated Workflow

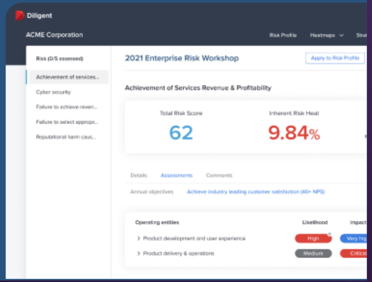
Secure Communication and Collaboration

Modern Governance

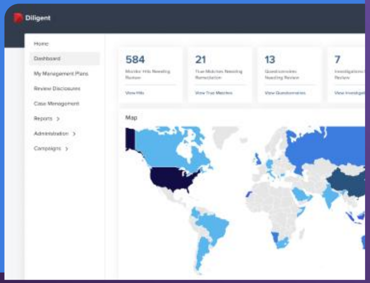
Modern ESG



Modern Risk


Diligent
ACME Corporation
2021 Enterprise Risk Workshop
Achievement of Services Revenue & Profitability
Total Risk Score
62
Inherent Risk Heat
9.84%

Modern Compliance



Modern Audit

Board and Leadership Collaboration

Modern Governance Analytics, Robotic Process Automation, 70+ Integrations

Diligent Story- Video

Thank you

?