How does Integrated Risk Management help reduce costs and increase efficiency to achieve GRC goals

PRESENTED BY:

Lih Chin Ong CA (Singapore), CISA, CCSP

Client Partner

Housekeeping

- Today's session will be 45 minutes with 15 minutes for Q&A at the end.
- Please submit your questions through the Q&A panel on your Zoom console.
- A copy of the slides will be shared with attendees.

Agenda

- Integrated Risk Management today and its challenges to the 3 line-of-defense
- Balance between managing risks and identifying opportunities
- Key areas to consider to achieve “reasonable assurance”
- Unified or integrated reporting for the executive leadership

Integrated Risk Management and its challenges to the 3LoD

Attributes of Integrated Risk Management*

Strategy: Implementation and enablement of a consistent strategy and framework

Assessment: Identification, evaluation and prioritization of risks

Response: Identification and implementation of mechanisms to mitigate risk

Communication and reporting: Provision of the best or most appropriate means to track and inform stakeholders of an enterprise's risk response

Monitoring: Identification and implementation of processes that methodically track governance objectives, risks to those objectives, compliance with policies and decisions that are set through the governance process, risk ownership/accountability, and the effectiveness of risk mitigation and controls.

Technology: Design and implementation of an IRM solution (IRMS) architecture.

Challenges to 3 LoD

Differences in measures of progress to support the strategy resulting in convoluted reporting

Risk taxonomy differs across the lines-of-defense

Different testing methods and approach to mitigate risk

Complex and fragmented reporting – what, how and timeliness of reporting leading to "assurance fatigue"

Duplicated efforts across External and Internal Assurance providers leading to audit fatigue

Various technologies used by different teams within and across the line-of-defense

*From Gartner: https://www.gartner.com/en/information-technology/glossary/integrated-risk-management-irm

© 2021 Diligent Corporation

Diligent

Poll #1:
What are the challenges you are facing with Integrated Assurance reporting?

Please submit your selection to the poll question. You can select multiple responses.

1. Method of data collection from each assurance function / LoD (e.g. Email, Shared Drive, etc.)
2. Timeliness of data collection from each assurance function / LoD (e.g. ad-hoc, periodically, scheduled, etc.)
3. Disjointed scoring & measurement methodologies (e.g. High/Medium/Low, Good/Excellent)
4. Repeated assessments on similar processes/controls (e.g. Cybersecurity Assessment, Data Privacy Review, etc.)

© 2021 Diligent Corporation

Benefits of IRM and Combined Assurance

- Adopt Combined assurance to prevent “assurance fatigue” and the following benefits*
  - One voice and taxonomy across all governance bodies and functions in the organization
  - Efficiency in collecting and reporting information
  - Common view of risks and issues across the organization
  - More effective governance, risk, and control oversight

Exhibit 1 **Parties Involved in the Combined Assurance Framework**

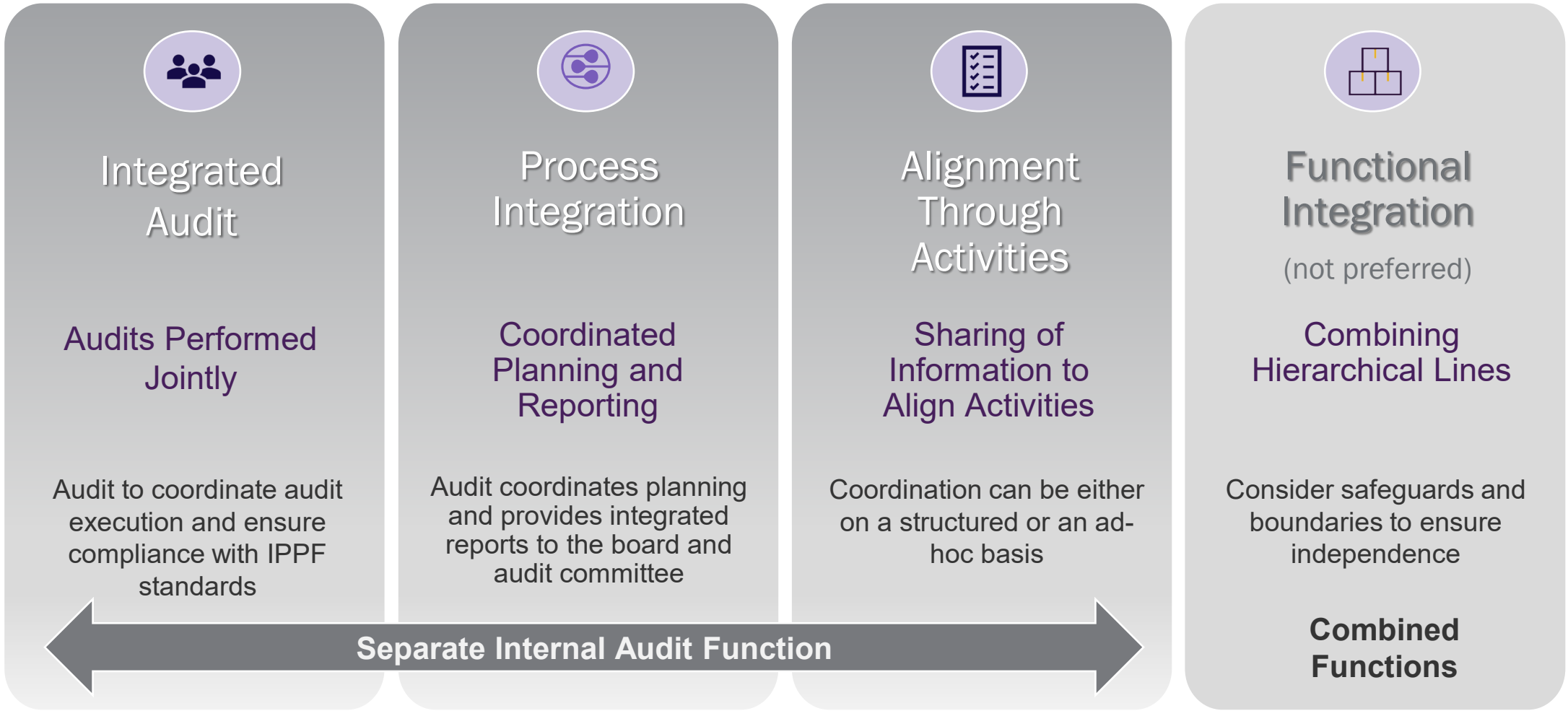
Source: Adapted from *King Code of Governance for South Africa 2009* (Institute of Directors in Southern Africa) and *Combined Assurance: Case Studies on a Holistic Approach to Organizational Governance* by G. Sarens, Decaux, L., & Lenz, R. (Altamonte Springs, FL: The Institute of Internal Auditors Research Foundation, 2012).

Benefits of Combined Assurance	Tangible Deliverables of Combined Assurance
Consolidated, single source of truth	Accessible and harmonized data
More informed Board and Executive Leadership	Integrated, holistic assurance reporting
Streamlined workflows/time savings	Automated, standardized process

*Source: Combined Assurance: One Language, One Voice, One View by Sam C. J. Huibers from IIA CBOK (Common Body of knowledge

© 2021 Diligent Corporation
Diligent

Key areas to consider to achieve "reasonable assurance"



*Source: Combined Assurance: One Language, One Voice, One View by Sam C. J. Huibers from IIA CBOK (Common Body of knowledge

© 2021 Diligent Corporation

Critical Components to implement IRM

Adopted from How to implement Combined Assurance: Critical Components

1. ERM Maturity
   - Success of combined assurance implementation depend on ERM's maturity
2. Combined Assurance Awareness
   - Tone at the top: board-level and executive leadership
3. Combined Assurance Champion
   - CAE/IAF could become the custodian of daily combined assurance
4. Combined Assurance Strategy
   - Identify areas that need assurance based on board, executive, and stakeholder priorities
5. Assurance Mapping
   - Coverage areas aligned to Assurance providers
6. Combined Assurance Report
   - A global picture of assurance coverage to the board and the audit committee to allow both to exercise their oversight role appropriately

*Source: "Implementing combined assurance: insights from multiple case studies" by Loïc Decaux and Gerrit Sarens Louvain School of Management, Université Catholique de Louvain, Louvain-la-Neuve, Belgium

© 2021 Diligent Corporation

Unified or Integrated Risk reporting for Executive Leadership

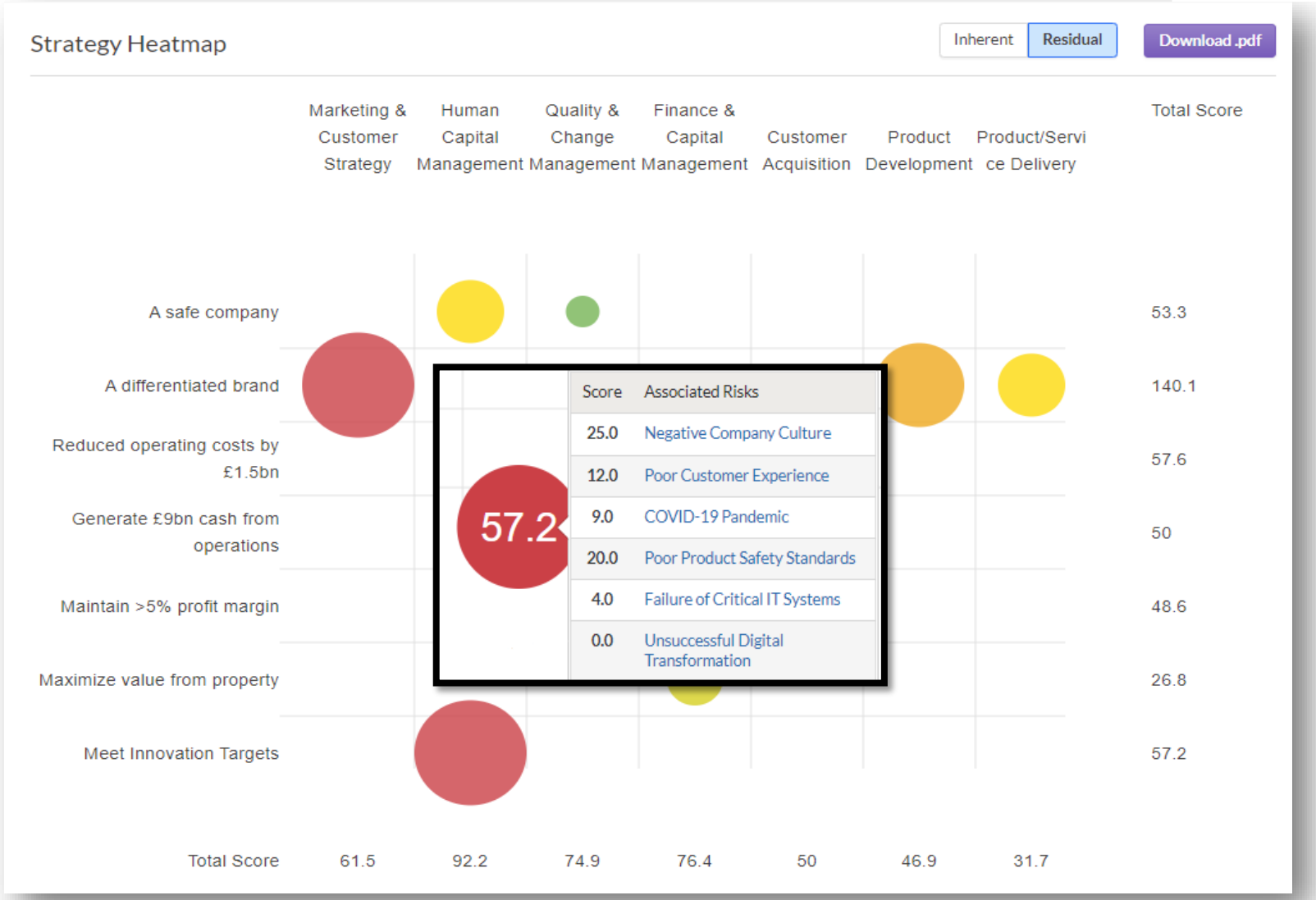
Types of Assurance Reporting

- Mapping to Strategic Priorities
- Mapping to Processes
- Mapping to Key Risks
- Mapping to ESG Objectives

© 2021 Diligent Corporation

Assurance – Mapping to Strategic Priorities

- Map areas that need assurance based on board, executive, and stakeholder priorities and link to organization's strategic risks
- Key risks and key controls being reported multiple times to multiple assurance functions (ie. Audit, Risk, Compliance, Regulators)



© 2021 Diligent Corporation

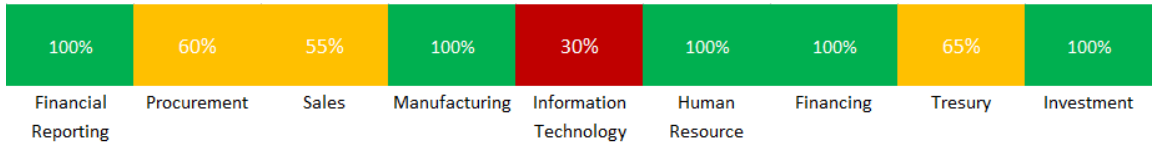
Assurance – Mapping to Processes

Assurance Map of processes and business areas being monitored and regularly assessed

COMBINED ASSURANCE - BY BUSINESS PROCESS

	Business Processes	Management Assurance (LoD 1)	Periodic Assurance (LoD 2)	Independent Assurance (LoD 3)		Combined Assurance
1	Financial Reporting					
2	Procurement					
3	Sales					
4	Manufactoring					
5	Information Technology					
6	Human Resource					
7	Financing					
8	Treasury					
9	Investment					

PROCESS ASSURANCE



- Each LoD performing independent assessments/reviews
- Provide Management with clear picture of risk & control posture

© 2021 Diligent Corporation

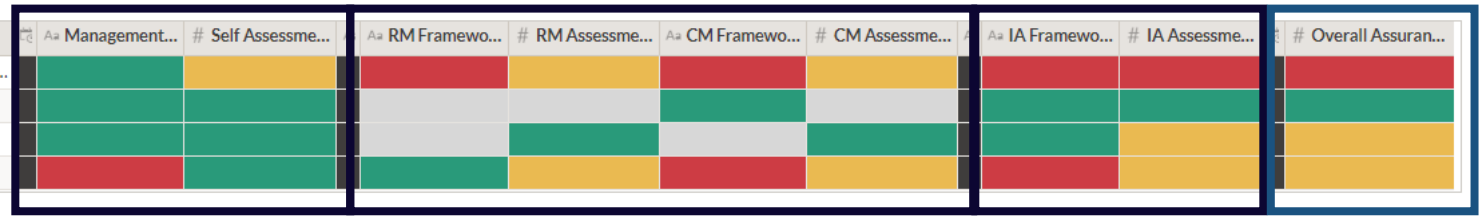
Diligent

Assurance – Mapping to Key Risks

Assessing activities aligned to key risks to determine the actual risk level

	Key Risks	Sub Process	Key Controls
1	Breach of Procurement Purchasing Proce...	Small Value Purchases	Multiple purchases of the same ite...
2	Breach of Procurement Purchasing Proce...	Purchasing Approving Authori...	Limits of Authority
3	Fraudulent Payments	Vendor Payment	Duplicate Vendor Payments
4	Inappropriate Ordering	Approval Process	System Entry

COMBINED ASSURANCE - BY KEY RISKS



1st LoD – Management Process & Self-Assessment

2nd LoD - Risk Management & Compliance Management

3rd LoD – Internal Audit

TOP OPERATIONAL RISKS

	URL Risk	Risk Description	Likelihood	Impact	Risk Ca
37	Update Risk	Information Security Breach	5 - Extreme	D - High	IT & Securi
39	Update Risk	Information Security Breach	5 - Extreme	D - High	IT & Securi
203	Update Risk	Vulnerability to cyber attack due to inadequate system security design to	5 - Extreme	E - Very Likely	Cyber Secu

FAILED CONTROLS

	URL Control	Controls Title	Controls Description	Effectiveness Ass
27	Update Control	Quarterly Review of DENR Requirement	Quarterly Review of DENR Requirement	Not Effective
235	Update Control	Quarterly Review of DENR Requirement	Quarterly Review of DENR Requirement	Not Effective
601	Update Control	Quarterly Review of DENR Requirement	Quarterly Review of DENR Requirement	Not Effective
39	Update Control	System Back Up	System Back Up	Not Effective

© 2021 Diligent Corporation

Diligent

ESG Health Scorecard – Mapping to ESG Objectives

Assessing activities aligned to ESG Objectives to determine the organization's ESG Health

ESG HEALTH SCORECARD

	ESG Catego	ESG Objective	Assurance
1	Environment	Environmental Market Risk	70%
2	Environment	Environmental Reputational Risk	88%
4	Environment	Environmental Physical Risk	100%
5	Environment	Green Product & Services	95%
6	Environment	Resource Efficiency	88%
9	Social	Dignity and Equality	70%
10	Social	Health and Well-Being	88%
12	Social	Employment and Weath Generation	100%
13	Social	Innovation of Better Products and Services	100%
14	Social	Community and Social Vitality	80%
15	Governance	Governing Purpose	70%
16	Governance	Quality of Governing Body	88%
18	Governance	Ethical Behaviour	100%
19	Governance	Risk and Opportunity Oversight	90%

ENVIRONMENT: Climate-Related Risks, Opportunities, and Financial Impacts

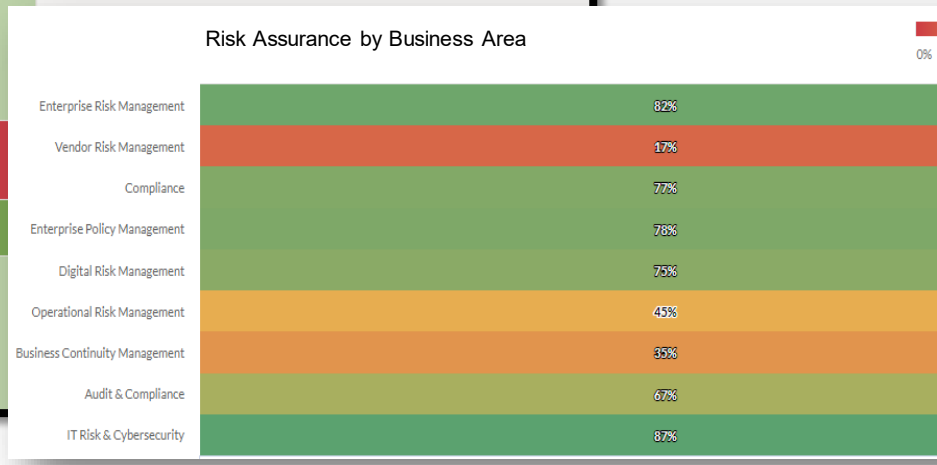
	Risk Category	Assurance	Description
1	Market	70%	Climate-related risks could impact the value company and reduce

SOCIAL: People Related Risks, Opportunities, and Financial Impacts

	Risk Category	Assurance	Description
1	Dignity and Equality	70%	Diversity and Inclusion; Pay equality; Wage level; Ethical employment

GOVERNANCE

	Risk Category	Assurance	Description
1	Governing Purpose	70%	The company's stated purpose, as the expression of the means by which a business proposes solutions to economic, environmental and social issues. Corporate purpose should create value for all stakeholders, including shareholders.
2	Quality of Governing Body	88%	Composition of the highest governance body and its committees by: competencies relating to economic, environmental and social topics; executive or non-
3	Stakeholder Engagement	60%	
4	Ethical Behaviour	100%	
5	Risk and Opportunity Oversight	90%	

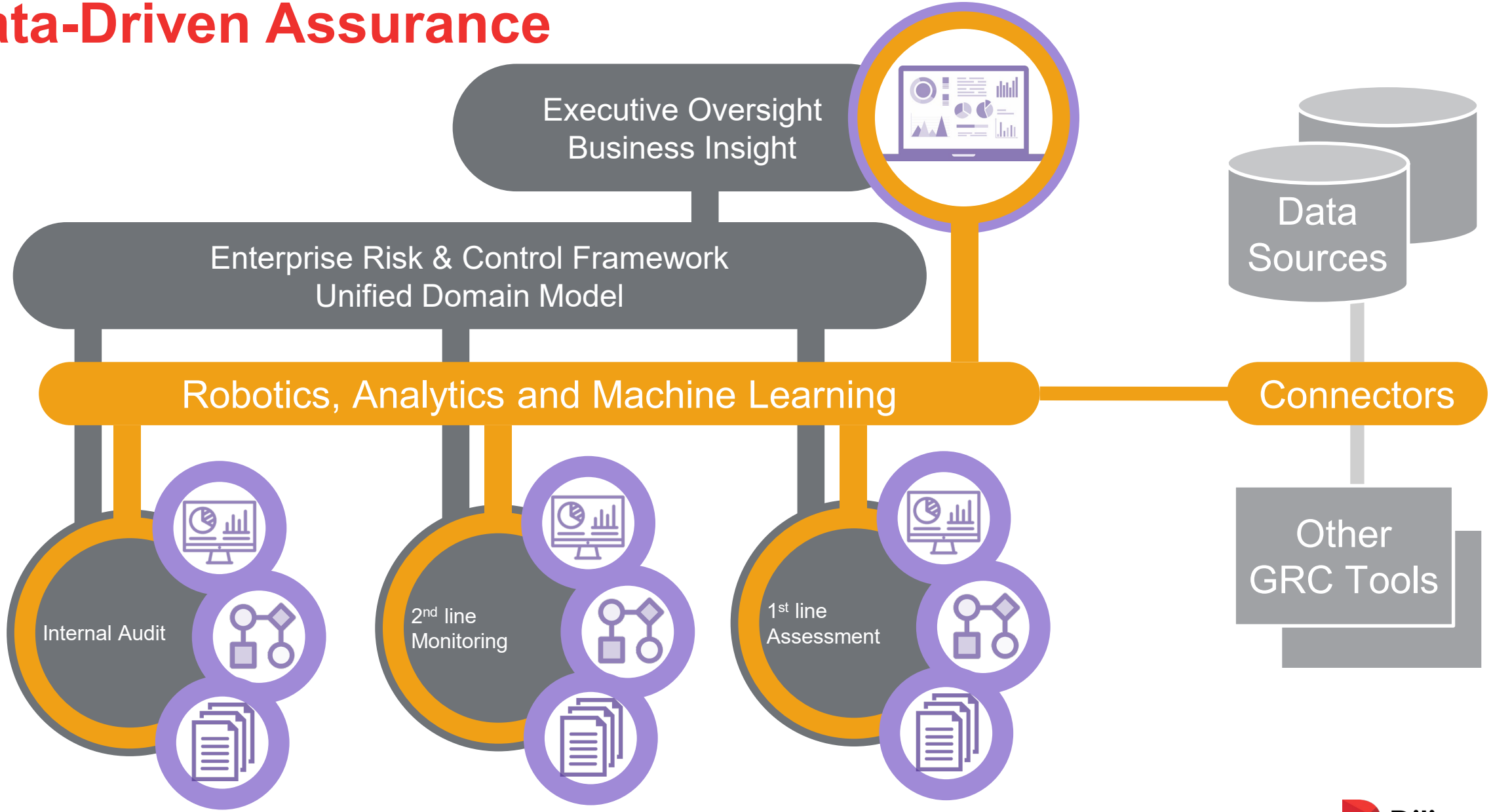


Impact of Risk Assurance work carried out by 3LoDs on ESG

© 2021 Diligent Corporation

Diligent

Data-Driven Assurance



© 2021 Diligent Corporation

Diligent

Poll #2:
How are you feeling about your progress to integrated risk reporting?

Please submit your option to the poll question.

1. Excellent - I'm confident I'm on the right path!
2. Good - but I could use some help from Diligent
3. Getting started – I would like more information
4. Not a priority right now

© 2021 Diligent Corporation

Key Takeaways

- Improve clarity of risk & compliance posture across functions
- Increase focus on stakeholder priorities
- Establish shared responsibility model across the organization
- Streamline reporting with flexible scoring methodologies

© 2021 Diligent Corporation

THANK YOU

PRESENTED BY:

Lih Chin Ong CA (Singapore), CISA, CCSP

Client Partner