Crowe

Smart decisions. Lasting value.™

Privacy’s Role in Integrated Risk Management

Crowe LLP and OneTrust CPE Webinar Series

May 14, 2020

Learning Objectives

As a result of attending this Webinar, you should be able to:

- Outline the benefits organizations are receiving through integrated risk management, embedded in enabling technologies, and its impact.
- Describe common challenges and solutions when building an integrated risk management framework.
- Articulate the interconnected nature of privacy and data protection and its cross-functional impact on risk management.
- Benchmark your effort to align privacy and data protection with integrated risk management efforts against leading practices.

Polling Question #1

What role do you play within your organization?

- Product/ Line of Business
- Risk Management
- Privacy
- Compliance
- Information Security
- Internal Audit
- Other

Why Integrated Risk Management?

What is Integrated Risk Management?

Integrated risk management (IRM) is a set of practices and processes supported by a **risk-aware culture** and enabling technologies, that **improves decision making** and performance through an **integrated view** of how well an organization manages its unique set of risks. – Definition from Gartner

Key phrases that we will highlight as we discuss Privacy's Role in IRM today…

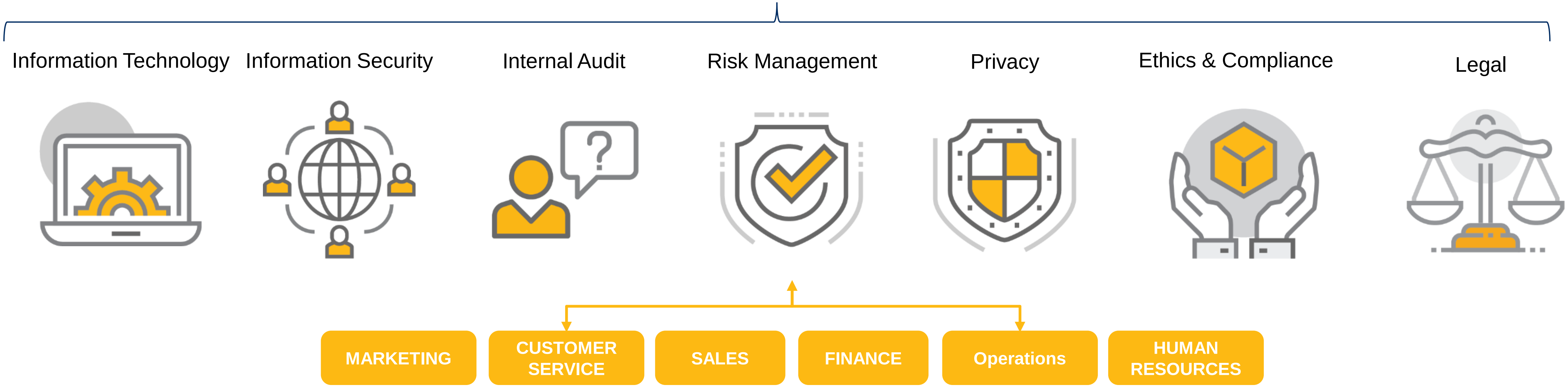
1) Integrated View
2) Risk Aware Culture
3) Improves Decision Making & Performance

End in Mind: Integrated Risk Management

Organizations with effective integrated risk management processes across all or many silos have:

- ✓ Reduced Cost and Complexity
- ✓ Strong Leadership Support
- ✓ Strategic Direction / Focus
- ✓ Informed Decision Making

- ✓ Authoritative Risk Database
- ✓ Clear Prioritization
- ✓ Positively Impacted Operations
- ✓ Improved Information Quality

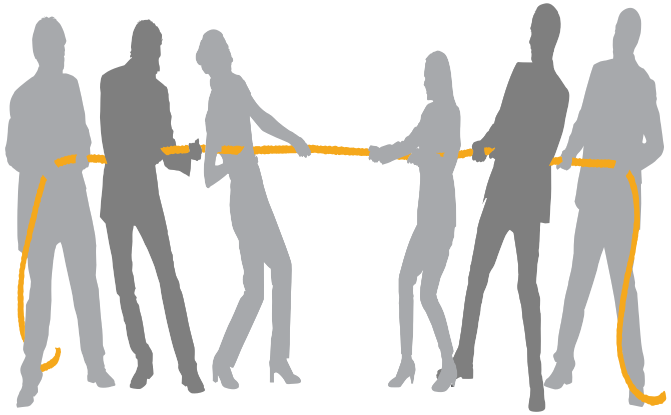


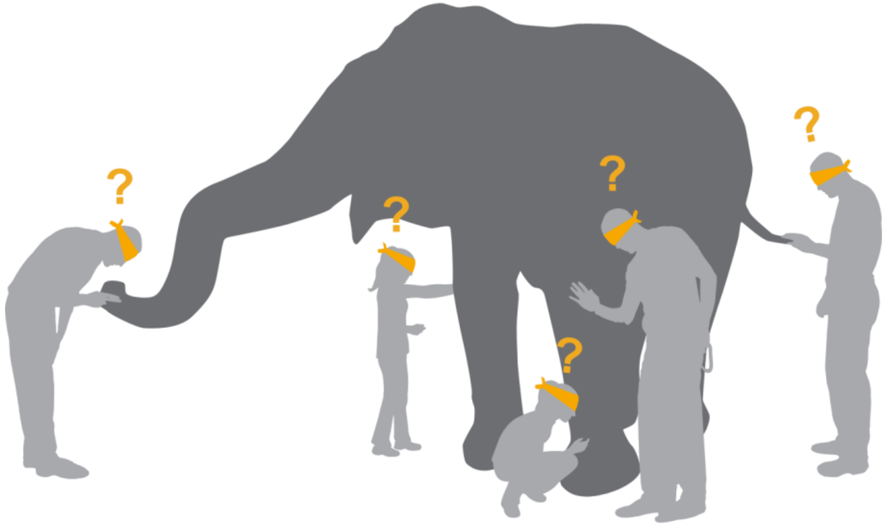
Challenges without Integrated Risk Management

- Lack of Strategic Vision
  - ✓ Disconnected Leadership Support and/or Direction
  - ✓ Lack of clarity in Executive Ownership for Key Decision Making
  - ✓ Reduced Resources/funding support because of the lack of visibility of the value
  - ✓ Unclear Plan and Prioritization

- Increased Complexity
  - ✓ Lack of Shared Risk Taxonomy
  - ✓ Lack of Holistic Risk Mitigation
  - ✓ Inconsistent Understanding of Business Value and Risk
  - ✓ Organizational Silos
  - ✓ Disjointed and Inefficient Decision Making

- Decision Making Impairment
  - ✓ Incomplete Risk Data Set
  - ✓ Inconsistent Top-Down Visibility
  - ✓ Misalignment of Measurements
  - ✓ Not Measuring What Matters
  - ✓ Lack of Trending and Tolerances





- Inefficient Efforts
  - ✓ Recreating Risk Data Across Organization
  - ✓ Accumulating Data Without Alignment to Plan
  - ✓ Overuse of Point to Point Integration

Polling Question #2

How does your organization currently manage risk?

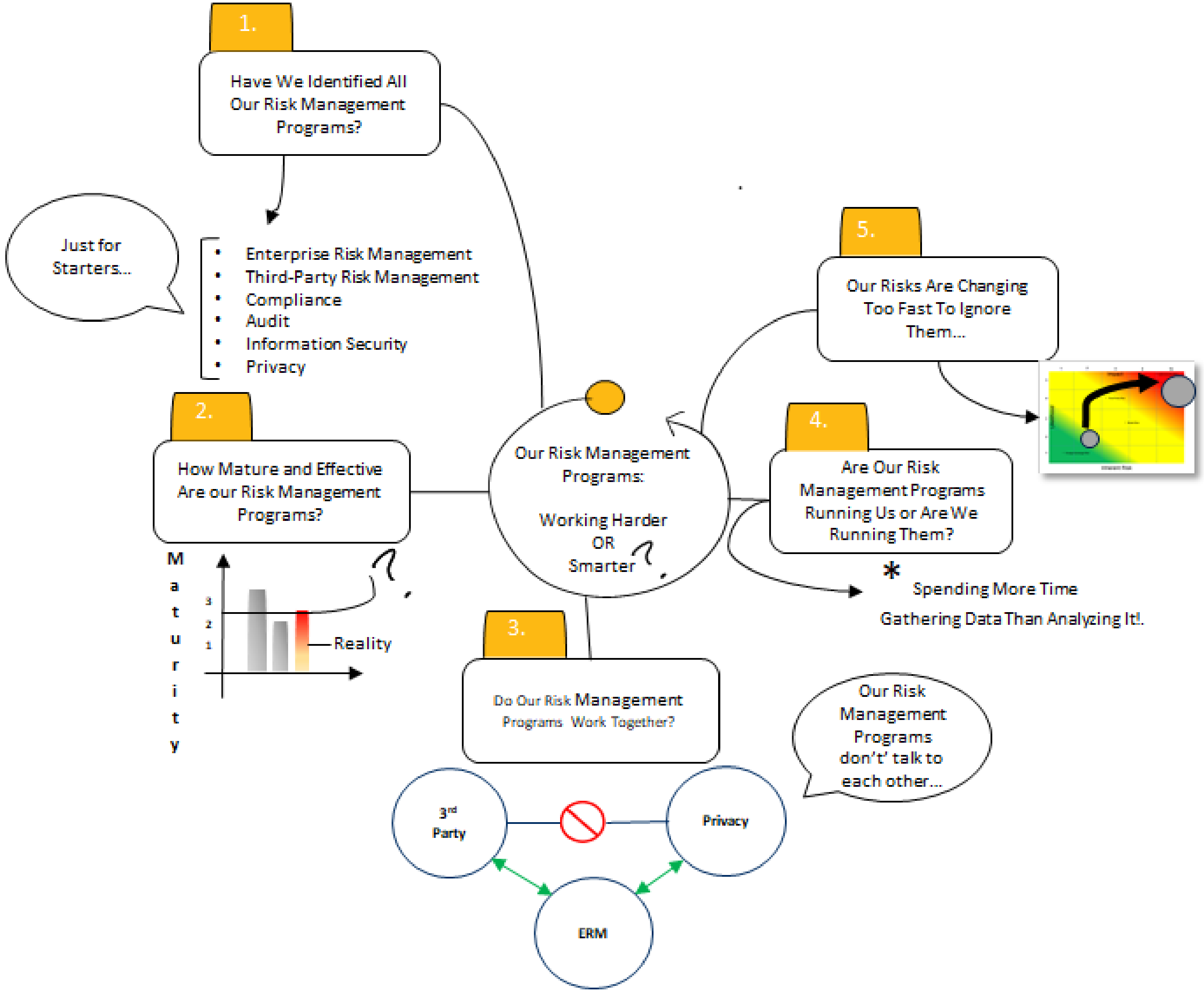
- Owned or embedded in the product teams and advised and challenged by Risk and Audit functions
- Siloed – everyone must look out for themselves
- Risk Management’s Responsibility
- Internal Audit will tell me if I’m out of line

Getting Started

Integrated Risk Management

Designing and building an Integrated Risk Management Program requires significant knowledge, effort and coordination.

Integrated Risk Management Programs must have a harmonization of many facets including processes, resources, and technology. Many organizations have established key elements of an integrated risk management program; yet, striking an acceptable balance of a fully integrated harmonized program can be complex and challenging.



1. Have We Identified All Our Risk Management Programs?

Just for Starters...

- Enterprise Risk Management
- Third-Party Risk Management
- Compliance
- Audit
- Information Security
- Privacy

2. How Mature and Effective Are our Risk Management Programs?

Our Risk Management Programs:

Working Harder OR Smarter

3. Do Our Risk Management Programs Work Together?

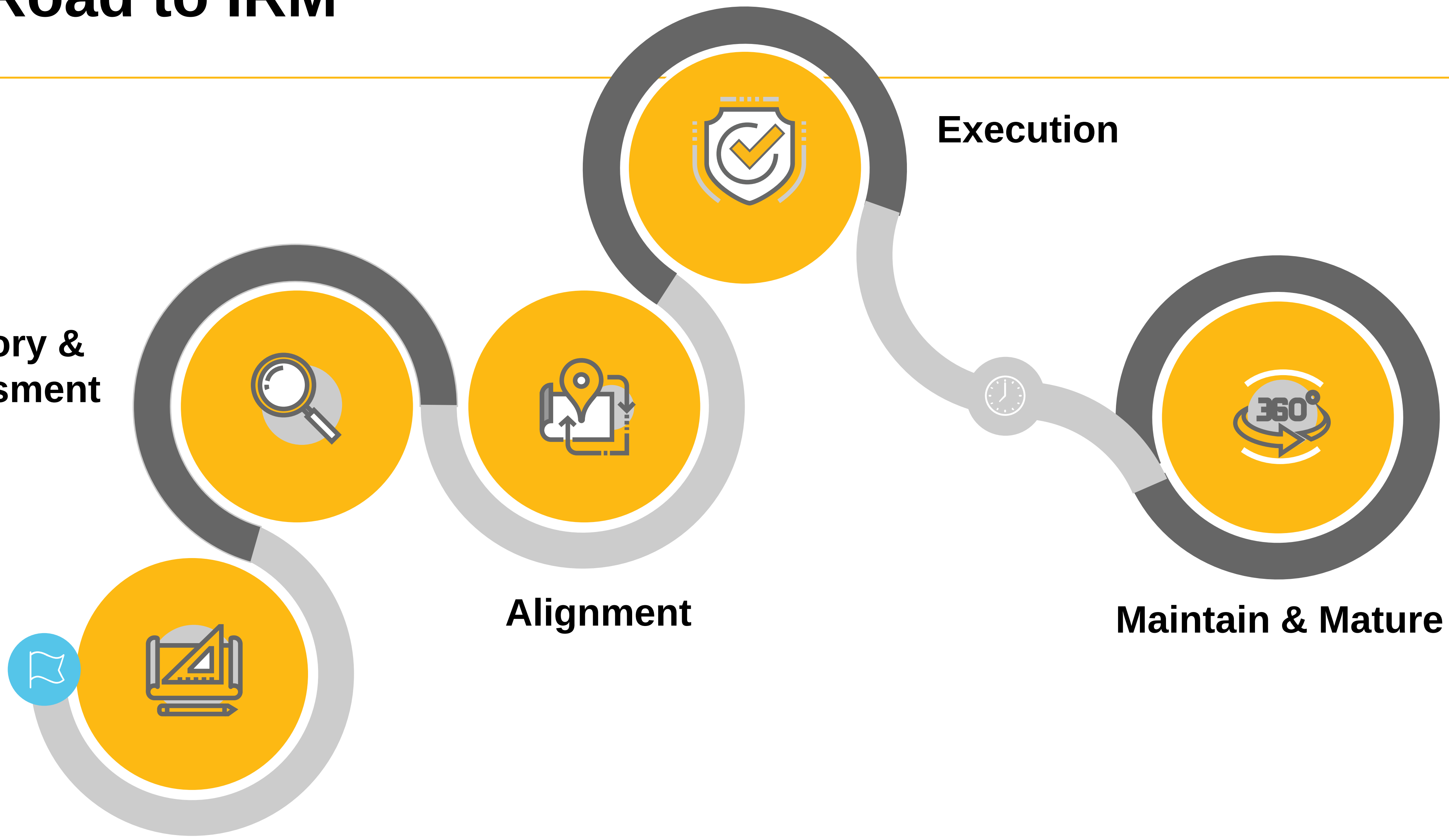
Our Risk Management Programs don't' talk to each other...

4. Are Our Risk Management Programs Running Us or Are We Running Them?

* Spending More Time Gathering Data Than Analyzing It!.

5. Our Risks Are Changing Too Fast To Ignore Them...

The Road to IRM



Execution

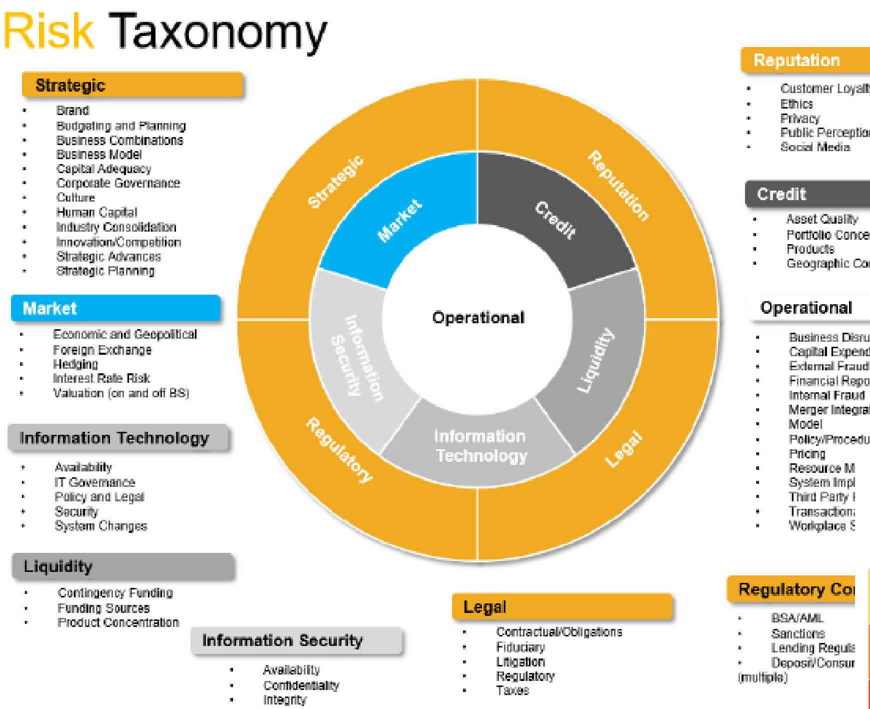
Inventory & Assessment

Alignment

Maintain & Mature

Planning & Strategy

Risk Taxonomy and Measurement



Risk Taxonomy

Strategic
- Brand
- Budgeting and Planning
- Business Combinations
- Business Model
- Capital Adequacy
- Corporate Governance
- Culture
- Human Capital
- Industry Consolidation
- Innovation/Competition
- Strategic Advances
- Strategic Planning

Market
- Economic and Geopolitical
- Foreign Exchange
- Hedging
- Interest Rate Risk
- Valuation (on and off BS)

Information Technology
- Availability
- IT Governance
- Policy and Legal
- Security
- System Changes

Liquidity
- Contingency Funding
- Funding Sources
- Product Concentration

Information Security
- Availability
- Confidentiality
- Integrity

Reputation
- Customer Loyalty/ Retention
- Ethics
- Privacy
- Public Perception
- Social Media

Credit
- Asset Quality
- Portfolio Concentration
- Products
- Geographic Concentration

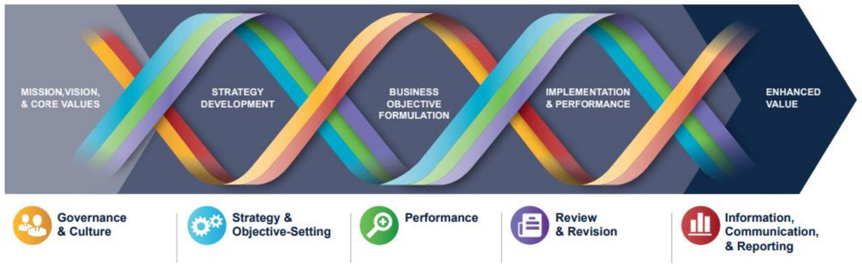
Operational
- Business Disruption
- Capital Expenditures
- External Fraud
- Financial Reporting
- Internal Fraud
- Merger Integration
- Model
- Policy/Procedures Compliance
- Pricing
- Resource M
- System Impl
- Third Party I
- Transaction:
- Workplace S

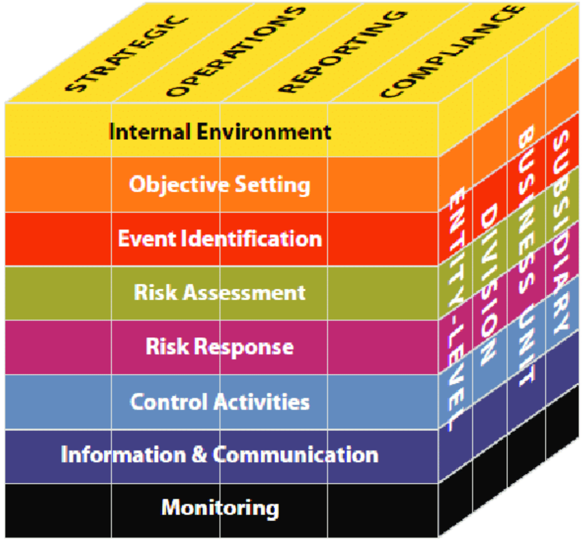
Legal
- Contractual/Obligations
- Fiduciary
- Litigation
- Regulatory
- Taxes

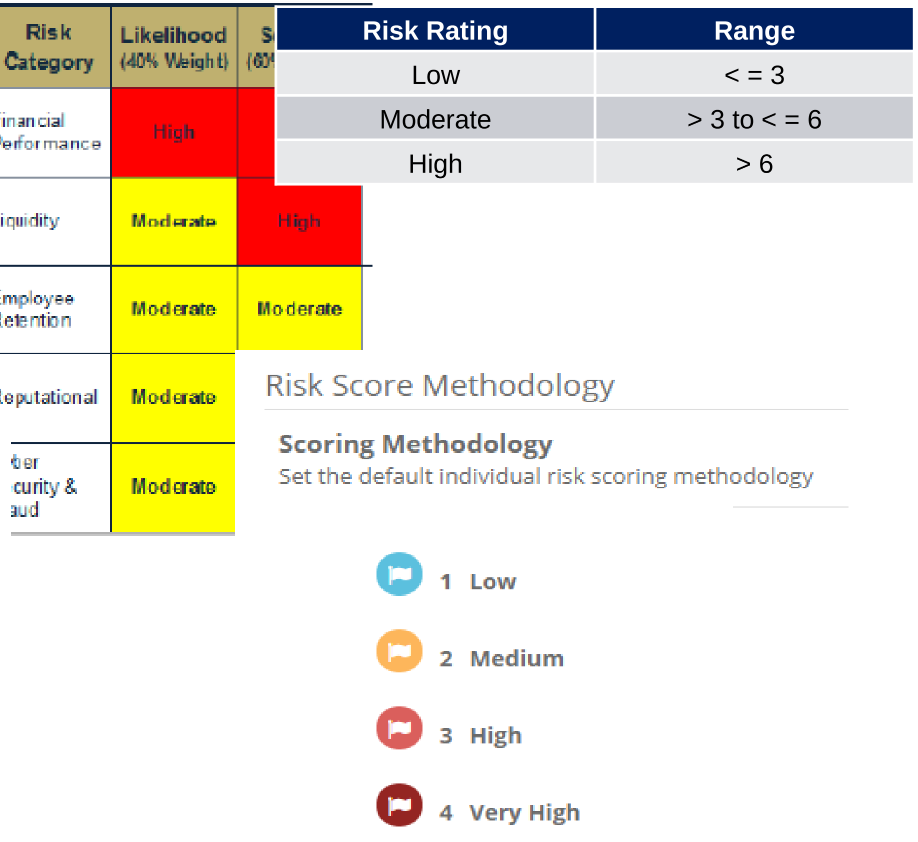
Regulatory Co
- BSA/AML
- Sanctions
- Lending Regula
- Deposit/Consur

(multiple)

ENTERPRISE RISK MANAGEMENT


MISSION,VISION, & CORE VALUES
STRATEGY DEVELOPMENT
BUSINESS OBJECTIVE FORMULATION
IMPLEMENTATION & PERFORMANCE
ENHANCED VALUE
Governance & Culture
Strategy & Objective-Setting
Performance
Review & Revision
Information, Communication, & Reporting





#	Risk Category	Likelihood (40% Weight)	S (60'
1	Financial Performance	High	
2	Liquidity	Moderate	High
3	Employee Retention	Moderate	Moderate
4	Reputational	Moderate	
	ber curity & aud	Moderate	

Risk Rating	Range
Low	< = 3
Moderate	> 3 to < = 6
High	> 6

Risk Score Methodology

Scoring Methodology

Set the default individual risk scoring methodology

- 1 Low
- 2 Medium
- 3 High
- 4 Very High

Polling Question #3

What are the challenges your organization is experiencing (select all that apply)

- Resources

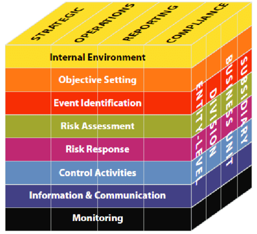
- Top down buy-in

- Defined process

- Tool to support the process

Organizational Alignment

*Adapted Chart from the Institute of Internal Auditors**



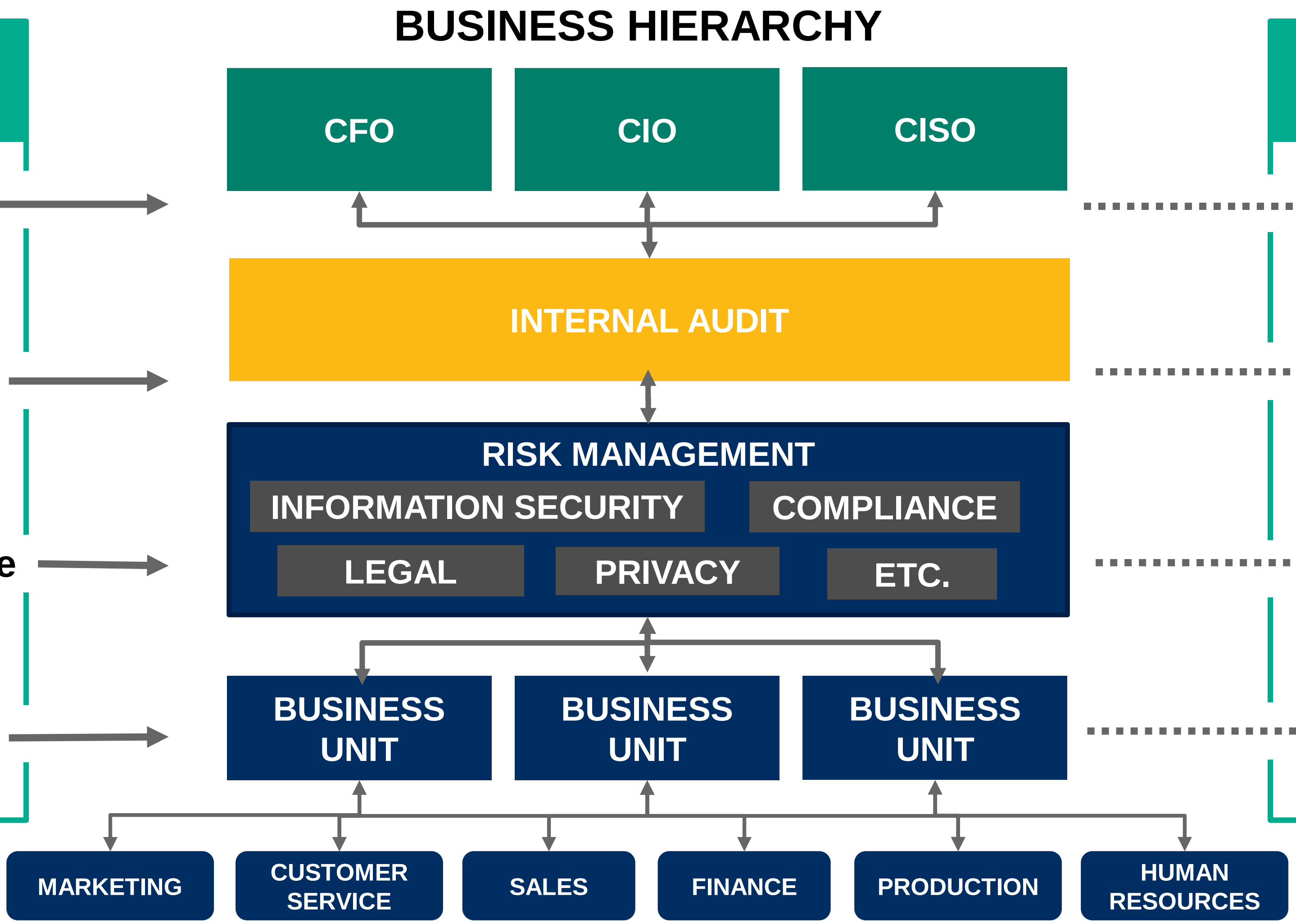
ROLE

Leadership

Third Line Of Defense

Second Line Of Defense

First Line Of Defense



BUSINESS HIERARCHY

CFO

CIO

CISO

INTERNAL AUDIT

RISK MANAGEMENT

INFORMATION SECURITY

COMPLIANCE

LEGAL

PRIVACY

ETC.

BUSINESS UNIT

BUSINESS UNIT

BUSINESS UNIT

MARKETING

CUSTOMER SERVICE

SALES

FINANCE

PRODUCTION

HUMAN RESOURCES

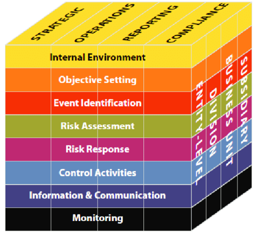
RESPONSIBILITY

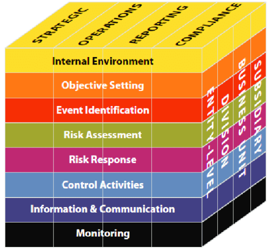
Strategic Decision Making

Assurance Over Controls

Ongoing Control Monitoring

Identify and Manage Risks





Privacy’s Role

Crowe Methodology for Privacy & Data Protection Compliance

Accountability & Governance

Determining the organization’s risk appetite in relation to data protection, enhancing accountability and governance through policies and standards.

RISK GOVERNANCE
(DP risk appetite and the link to wider Enterprise Risk Management framework)

DATA GOVERNANCE
(ownership, stewardship and control of personal data acquired and processed)

DATA PROTECTION POLICIES & STANDARDS
(enhanced policies and standards to govern the design of operational changes, in line with risk appetite)

Legal, Processes & Organization

Establishing the legal basis for use, the Data Protection Officer/Privacy Officer role, handling data subjects’ requests, managing third parties, responding to data breaches, and implementing the supporting organization, process and cultural changes.

CONSENT, USE & LAWFULNESS OF PROCESSING

INDIVIDUAL REQUESTS & RIGHTS
(SAR; RTBF; portability; restriction; rectification)

THIRD-PARTY MANAGEMENT
(legal docs; DD; oversight, 4th parties, supplier network)

BREACH MANAGEMENT & NOTIFICATION

DATA PROTECTION OPERATING MODEL
(DPO/Privacy role; privacy by design; DPIA; line 1 & 2 responsibilities)

TRAINING AND AWARENESS
(delivery of enhanced DP training to meet needs, plus communications and culture change)

Information Security & Data Retention

Understanding and defining the approach to information security and personal data retention.

INFORMATION SECURITY
(electronic and physical)

DATA RETENTION
(deletion; obfuscation; pseudonymisation)

Data Definition, Mapping, & Transfer

Understanding, defining and documenting the personal data that the organization acquires and processes.

DATA DEFINITION & MAPPING
(documenting and classifying uses, locations and internal/external movements of personal data)

CROSS-BORDER DATATRANSFERS
(adequate protections for cross-border transfers)

Unlocking Insights

Polling Question #4

How many different Governance, Risk and Control software applications are being used in your organization?

- One
- Two to four
- Five or more
- None or unknown

Integrated Risk Management

CONNECT ENTERPRISE DATA

Centralize visibility into data

Agile Architecture

Data Inventories

Data Population

APPLY RISK METHODOLOGY

Identify risk and measure impact

Risk Frameworks

Risk Identification

Scoring Methodologies

TRACK RISK REMEDIATION

Mitigate and track risk over time

Risk Tracking

Workflows

Extend To Line Of Business

REPORT & MONITOR RISK

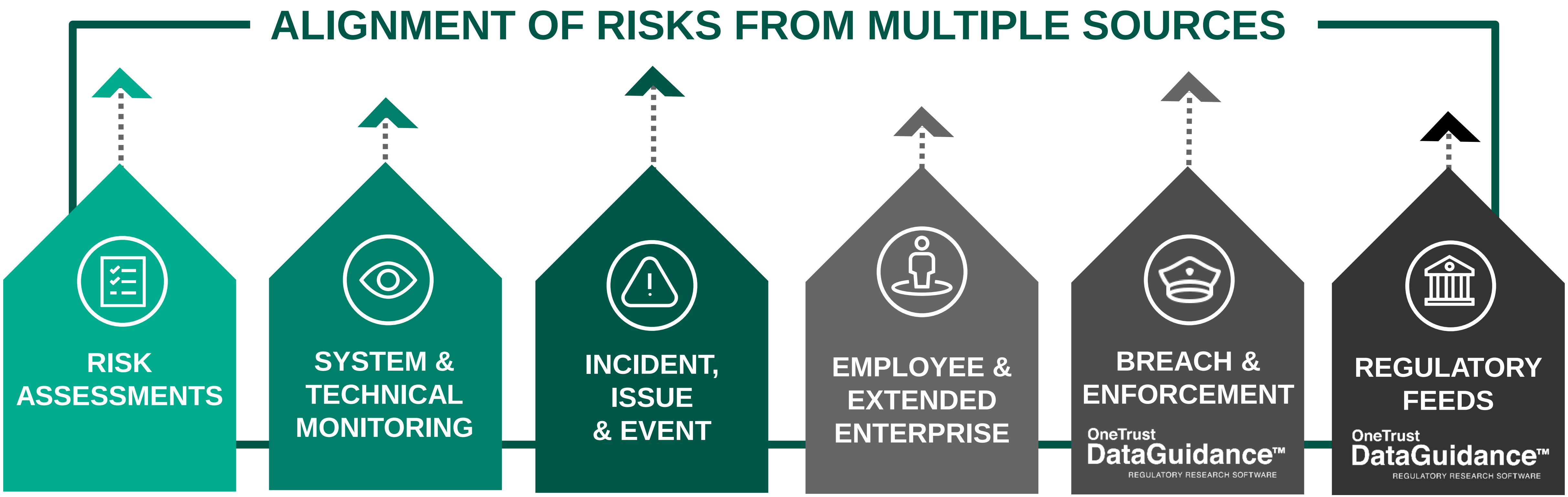
Report to C-Level Executives

Continuous Monitoring

Reporting

Market Activity

Enabling Integrated Risks



ALIGNMENT OF RISKS FROM MULTIPLE SOURCES

RISK ASSESSMENTS

Assessment on an IT system, or Vendor risk assessment

SYSTEM & TECHNICAL MONITORING

Identify vulnerability from security scanning tool

INCIDENT, ISSUE & EVENT

Create risks based on analyzing issues and incidents

EMPLOYEE & EXTENDED ENTERPRISE

Self-reported risks and issues from customers & employees

BREACH & ENFORCEMENT

OneTrust DataGuidance™ REGULATORY RESEARCH SOFTWARE

Measure yourself against the latest enforcement actions and industry breaches.

REGULATORY FEEDS

OneTrust DataGuidance™ REGULATORY RESEARCH SOFTWARE

Receive alerts for changes in regulations which may result in a new risk (ex. GDPR, CCPA amendments)

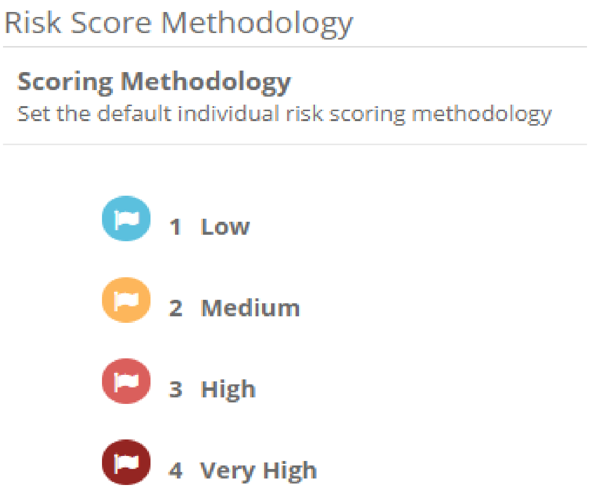
Quantify and Measure Risk

CHOOSE YOUR APPROACH TO MEASURING RISK

Consistent

Transparent

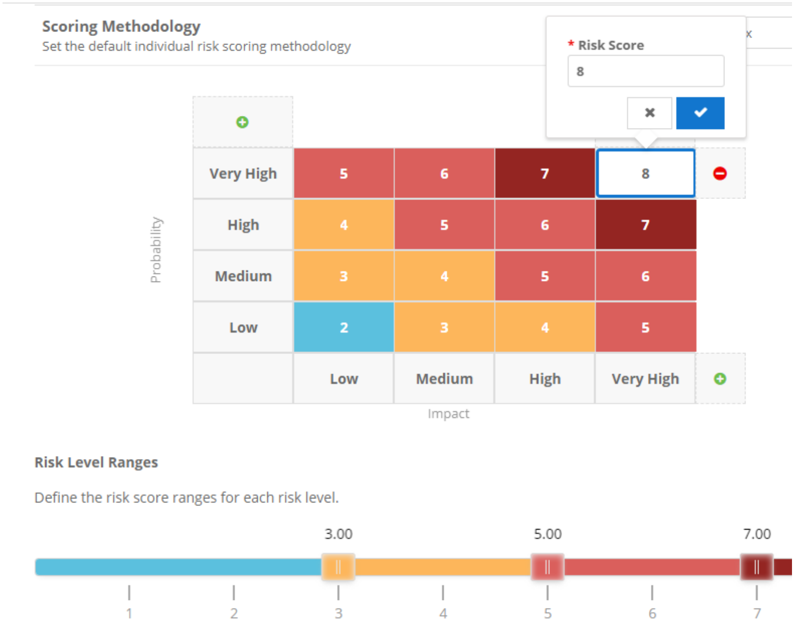
Data Driven Insights



Risk Score Methodology

Scoring Methodology
Set the default individual risk scoring methodology

1	Low
2	Medium
3	High
4	Very High



Scoring Methodology
Set the default individual risk scoring methodology

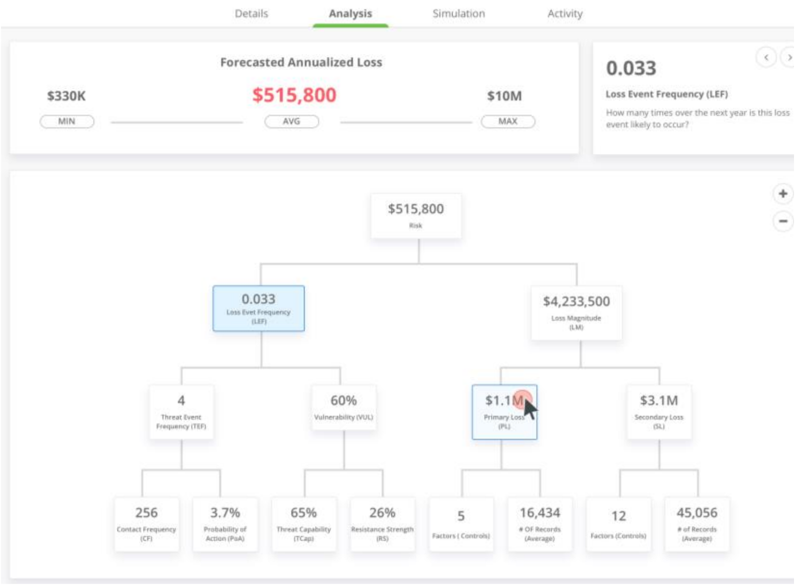
* Risk Score
8

Probability	Low	Medium	High	Very High
Very High	5	6	7	8
High	4	5	6	7
Medium	3	4	5	6
Low	2	3	4	5

Impact

Risk Level Ranges

Define the risk score ranges for each risk level.



Forecasted Annualized Loss

$330K MIN

$515,800 AVG

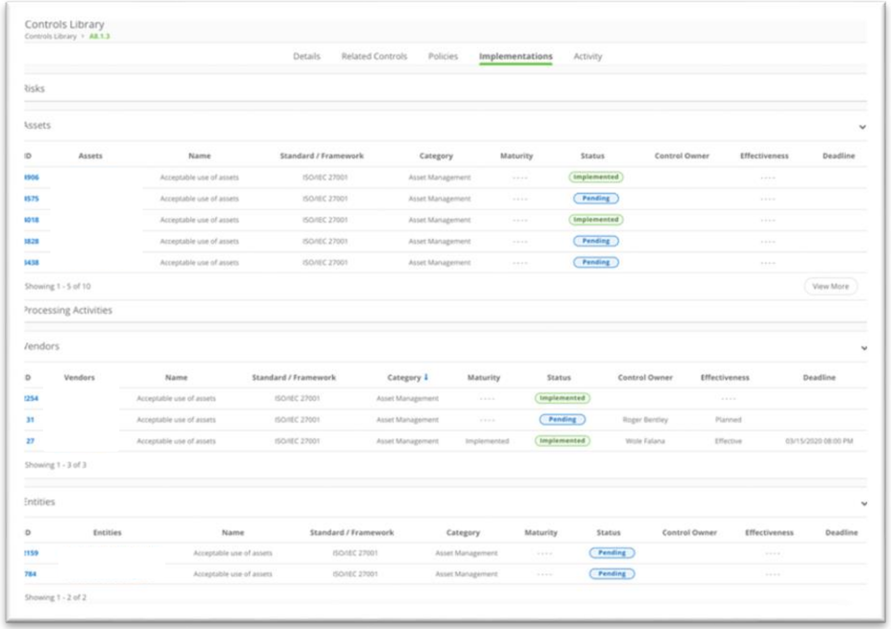
$10M MAX

0.033

Loss Event Frequency (LEF)

How many times over the next year is this loss event likely to occur?

Benefits of Dashboard Reporting



Controls Library

Controls Library > A8.1.3

Details | Related Controls | Policies | Implementations | Activity

Risks

Assets

ID	Assets	Name	Standard / Framework	Category	Maturity	Status	Control Owner	Effectiveness	Deadline
906		Acceptable use of assets	ISO/IEC 27001	Asset Management	----	Implemented		----	
575		Acceptable use of assets	ISO/IEC 27001	Asset Management	----	Pending		----	
018		Acceptable use of assets	ISO/IEC 27001	Asset Management	----	Implemented		----	
828		Acceptable use of assets	ISO/IEC 27001	Asset Management	----	Pending		----	
438		Acceptable use of assets	ISO/IEC 27001	Asset Management	----	Pending		----	

Showing 1 - 5 of 10

View More

Processing Activities

Vendors

ID	Vendors	Name	Standard / Framework	Category	Maturity	Status	Control Owner	Effectiveness	Deadline
254		Acceptable use of assets	ISO/IEC 27001	Asset Management	----	Implemented		----	
31		Acceptable use of assets	ISO/IEC 27001	Asset Management	----	Pending	Roger Bentley	Planned	
27		Acceptable use of assets	ISO/IEC 27001	Asset Management	Implemented	Implemented	Wole Falana	Effective	03/15/2020 08:00 PM

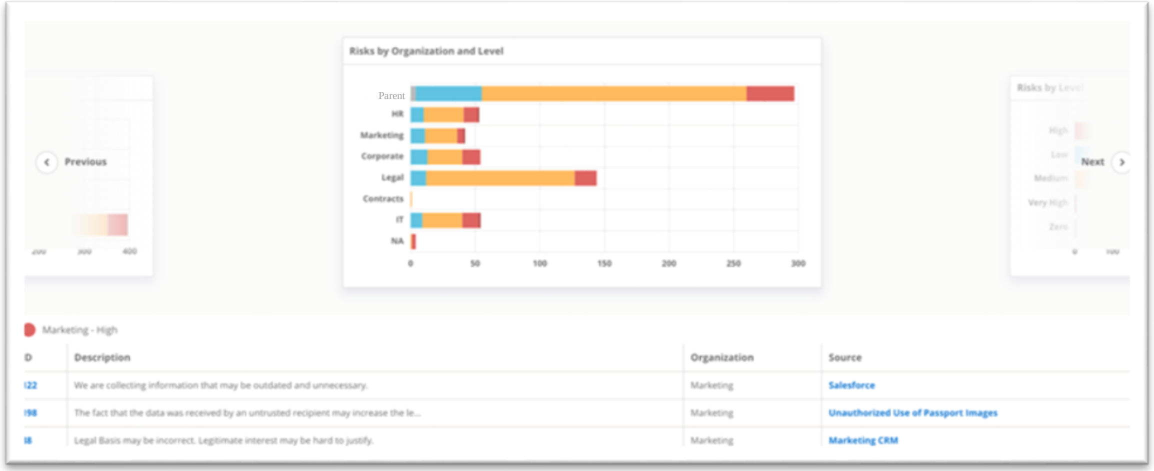
Showing 1 - 3 of 3

Entities

ID	Entities	Name	Standard / Framework	Category	Maturity	Status	Control Owner	Effectiveness	Deadline
159		Acceptable use of assets	ISO/IEC 27001	Asset Management	----	Pending		----	
784		Acceptable use of assets	ISO/IEC 27001	Asset Management	----	Pending		----	

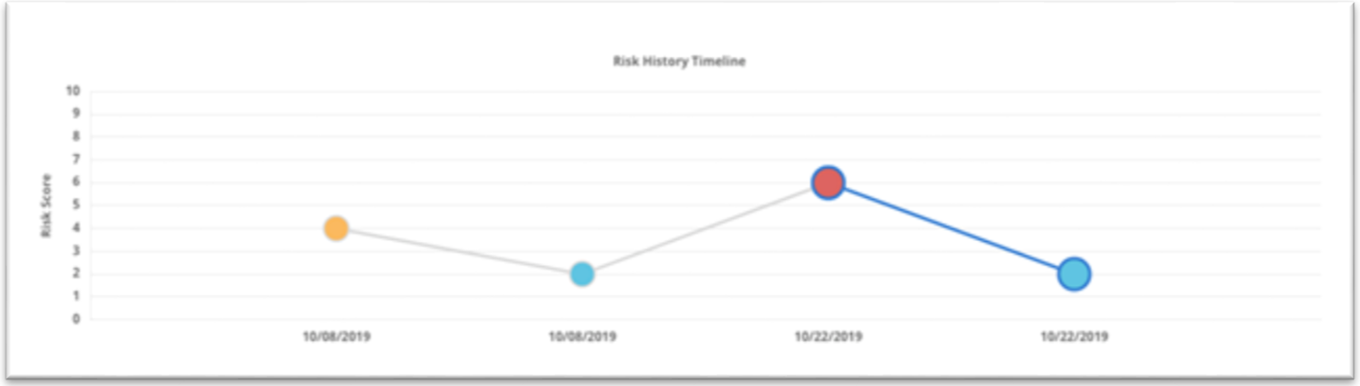
Showing 1 - 2 of 2

Making sense of the noise and tell a story to stakeholders on the management of risk across the organization.



Marketing - High

ID	Description	Organization	Source
22	We are collecting information that may be outdated and unnecessary.	Marketing	Salesforce
98	The fact that the data was received by an untrusted recipient may increase the le...	Marketing	Unauthorized Use of Passport Images
8	Legal Basis may be incorrect. Legitimate interest may be hard to justify.	Marketing	Marketing CRM



Smarter Decisions

Create impactful dashboards that allow for:

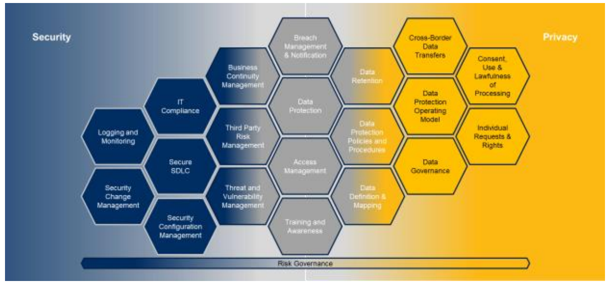
- Enhanced collaboration and communication
- Improved Focus and Alignment
- Accountability

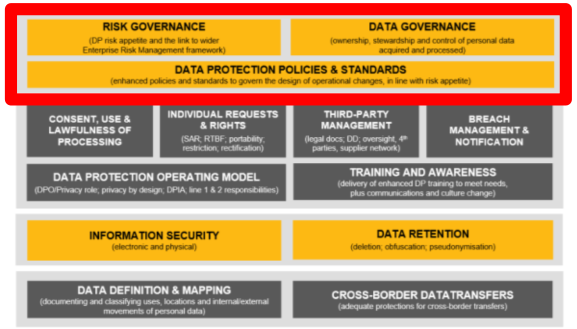
Insights

- *Have we identified the real key risks in our organization*
- *Are we getting the most out of our risk management programs*
- *How can we advance the maturity of our risk management programs quicker in a cost effective manner*
- *How can we align our risk management programs in a way that allows us to be more productive and efficient*

Recap: Smarter Decisions and the next step of Alignment

Manage Downside Risk AND Create Value


Security
Privacy
Breach Management & Notification
Cross-Border Data Transfers
Business Continuity Management
Data Retention
Consent, Use & Lawfulness of Processing
IT Compliance
Data Protection
Data Protection Operating Model
Logging and Monitoring
Third Party Risk Management
Data Protection Policies and Procedures
Individual Requests & Rights
Secure SDLC
Access Management
Data Governance
Security Change Management
Threat and Vulnerability Management
Data Definition & Mapping
Security Configuration Management
Training and Awareness
Risk Governance



RISK GOVERNANCE
(DP risk appetite and the link to wider Enterprise Risk Management framework)

DATA GOVERNANCE
(ownership, stewardship and control of personal data acquired and processed)

DATA PROTECTION POLICIES & STANDARDS
(enhanced policies and standards to govern the design of operational changes, in line with risk appetite)

CONSENT, USE & LAWFULNESS OF PROCESSING

INDIVIDUAL REQUESTS & RIGHTS
(SAR; RTBF; portability; restriction; rectification)

THIRD-PARTY MANAGEMENT
(legal docs; DD; oversight, 4th parties, supplier network)

BREACH MANAGEMENT & NOTIFICATION

DATA PROTECTION OPERATING MODEL
(DPO/Privacy role; privacy by design; DPIA; line 1 & 2 responsibilities)

TRAINING AND AWARENESS
(delivery of enhanced DP training to meet needs, plus communications and culture change)

INFORMATION SECURITY
(electronic and physical)

DATA RETENTION
(deletion; obfuscation; pseudonymisation)

DATA DEFINITION & MAPPING
(documenting and classifying uses, locations and internal/external movements of personal data)

CROSS-BORDER DATATRANSFERS
(adequate protections for cross-border transfers)

Each part of the organization has their own set of responsibilities and metrics. Having the people, process and the technology systems aligned is important. Embedding it into the culture such that everyone takes appropriate responsibility is a critical component of success in integrated risk management efforts and managing data ethically.

Polling Question #5

I would like to receive additional information from:

-Crowe (Process and technical enablement implementation)

-One Trust (Software as a Service offering Questions)

-Both

-No, thank you

* Explicit consent if you would like someone to continue to get information

Crowe

Thank You

“Crowe” is the brand name under which the member firms of Crowe Global operate and provide professional services, and those firms together form the Crowe Global network of independent audit, tax, and consulting firms. Crowe may be used to refer to individual firms, to several such firms, or to all firms within the Crowe Global network. The Crowe Horwath Global Risk Consulting entities, Crowe Healthcare Risk Consulting LLC, and our affiliate in Grand Cayman are subsidiaries of Crowe LLP. Crowe LLP is an Indiana limited liability partnership and the U.S member firm of Crowe Global. Services to clients are provided by the individual member firms of Crowe Global, but Crowe Global itself is a Swiss entity that does not provide services to clients. Each member firm is a separate legal entity responsible only for its own acts and omissions and not those of any other Crowe Global network firm or other party. Visit www.crowe.com/disclosure for more information about Crowe LLP, its subsidiaries, and Crowe Global. The information in this document is not – and is not intended to be – audit, tax, accounting, advisory, risk, performance, consulting, business, financial, investment, legal, or other professional advice. Some firm services may not be available to attest clients. The information is general in nature, based on existing authorities, and is subject to change. The information is not a substitute for professional advice or services, and you should consult a qualified professional adviser before taking any action based on the information. Crowe is not responsible for any loss incurred by any person who relies on the information discussed in this document. Visit www.crowe.com/disclosure for more information about Crowe LLP, its subsidiaries, and Crowe Global. © 2020 Crowe LLP.