NAVEX™ Crowe

Cybersecurity, privacy, and third-party management

How to align risk management strategies across these three critical teams

- **Josh Reid**, Crowe Principal, GRC Technology Services Leader

  Vidit Shah, Crowe LLP, Consulting Manager

  Adam Billings, NAVEX, IRM, Product Specialist

Presenters

Josh Reid
Crowe Principal,
GRC Technology
Services Leader

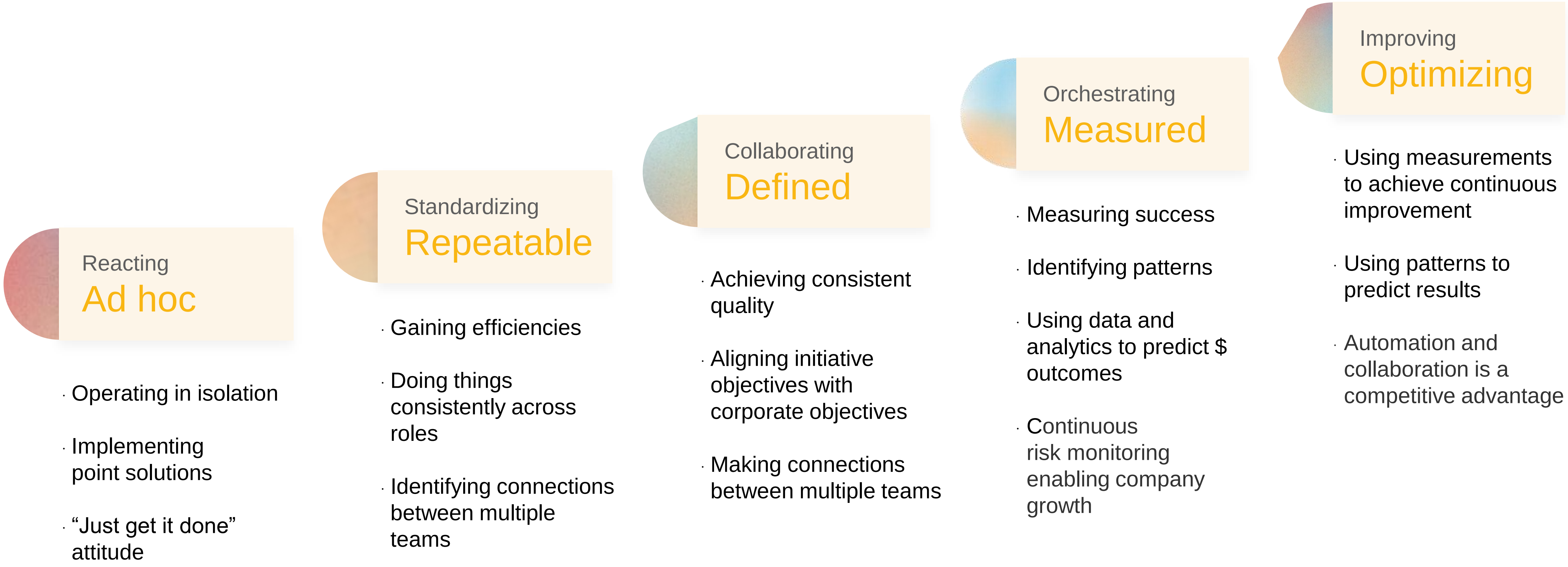
Vidit Shah
Crowe LLP, Consulting
Manager

Adam Billings
NAVEX, IRM, Product
Specialist

Your business provides value to our daily lives.

You can enable your risk management programs to help.

Integrated Risk Management (IRM) Maturity Model



Reacting
Ad hoc

- Operating in isolation
- Implementing point solutions
- “Just get it done” attitude

Standardizing
Repeatable

- Gaining efficiencies
- Doing things consistently across roles
- Identifying connections between multiple teams

Collaborating
Defined

- Achieving consistent quality
- Aligning initiative objectives with corporate objectives
- Making connections between multiple teams

Orchestrating
Measured

- Measuring success
- Identifying patterns
- Using data and analytics to predict $ outcomes
- Continuous risk monitoring enabling company growth

Improving
Optimizing

- Using measurements to achieve continuous improvement
- Using patterns to predict results
- Automation and collaboration is a competitive advantage

Poll question:

Where would you rate your risk maturity?

○ 1. Reacting – working in isolation, “Just get it done” approach

○ 2. Standardizing – gaining efficiencies, identifying connections with other teams

○ 3. Collaborating – establishing connections with other teams

○ 4. Orchestrating – continuous risk monitoring and collaboration is enabling company growth

○ 5. Optimizing – automation and collaboration is a competitive advantage

Confidential Information and Proprietary – Do not distribute

There is often a void when it comes to collaboration and sharing information.

Organizational challenges that inhibit risk collaboration:

People

- Internal politics result in risk teams focusing only on their specific area
- Risk is not a topic business leaders want to discuss

Process

- Risk management frameworks lack maturity and consistency
- Sharing risk information is manual and time-consuming

Technology

- Risk information is managed in disparate systems
- Manual tools are used for gathering risk information

Poll question:

What is the biggest challenge to stronger risk management collaboration at your company?

○ 1. Internal politics

○ 2. Business leaders don’t want to discuss risk

○ 3. Lack of a risk management framework

○ 4. Manual information sharing

○ 5. Disparate systems

○ 6. Manual reporting tools

○ 7. All of the above

“

How can this void impact your company?

Inconsistent collaboration can create a bottleneck.

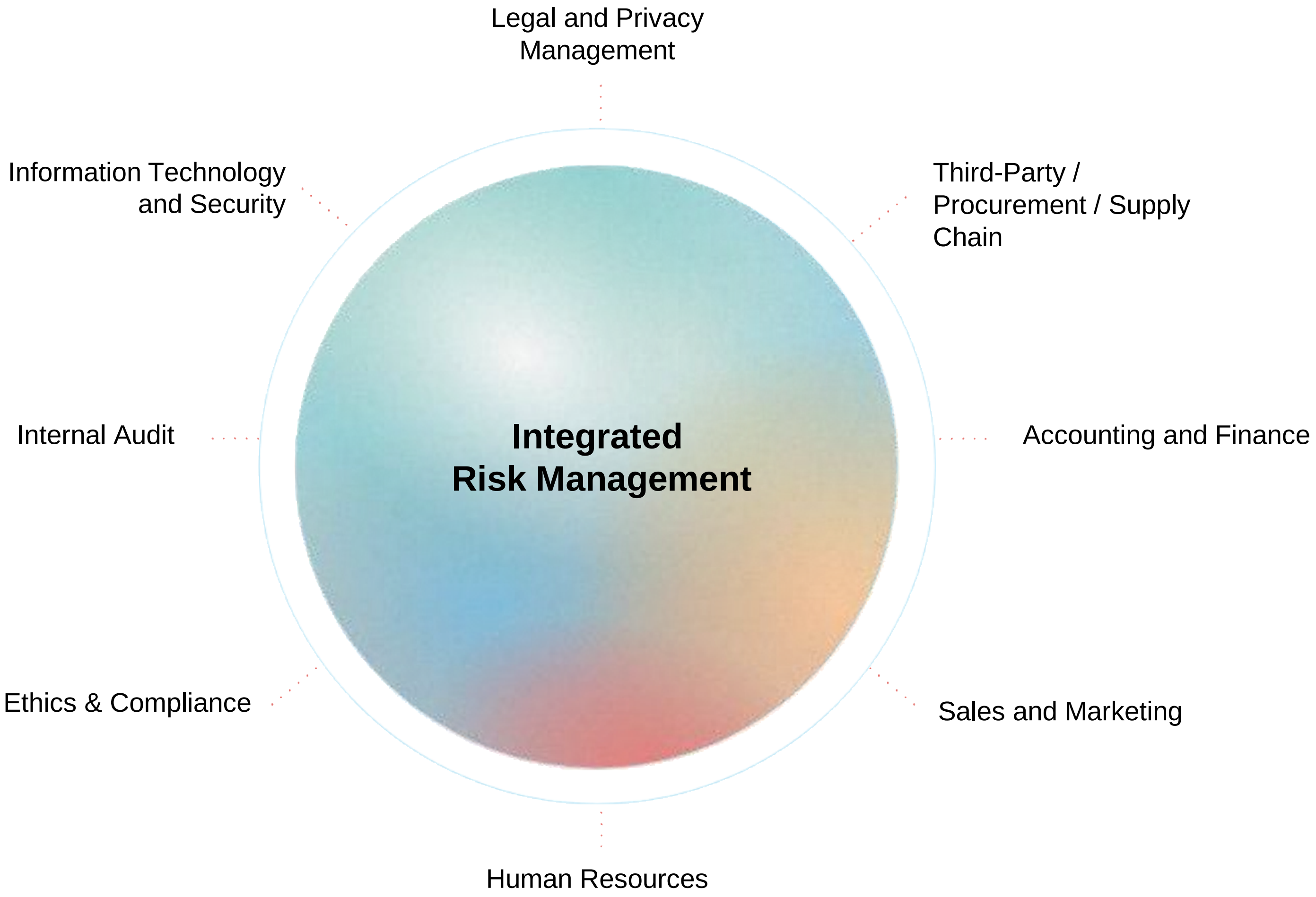
- Risk and compliance management activities are time consuming.
- Second and third lines spend significant time gathering information rather than analyzing and advising on risk and compliance topics.
- Traditional risk and compliance reporting (red/yellow/green) is often based on subjective analysis and is reactive in nature.
- Redundant remediation activities result in higher corporate costs.
- Manual risk assessments, compliance assessments, and audits require second and third lines to "do it again" next year.

Confidential Information and Proprietary – Do not distribute

“

Companies are finding innovative ways to improve collaboration and automation across risk management teams.

The future of risk management?
Improved collaboration and automation.


Legal and Privacy Management
Third-Party / Procurement / Supply Chain
Accounting and Finance
Sales and Marketing
Human Resources
Ethics & Compliance
Internal Audit
Information Technology and Security
Integrated Risk Management

Here’s how you can do it:

People

- Establish a GRC committee to promote collaboration
- Talk about risk in the context of business performance

Process

- Create a library of risks across business areas
- Align risk ratings and taxonomies across risk functions

Technology

- Gather risk information from first- and second-line business systems
- Monitor risks and team performance using KRIs and KPIs

Poll question:

What is the greatest strength of your risk management program?

○ 1. A strong GRC committee that drives strategy

○ 2. Risk is discussed in the context of business performance

○ 3. A consistently managed library of risks

○ 4. Well-aligned risk ratings and taxonomies

○ 5. A mature IRM platform that efficiently gathers risk information

○ 6. Risks and performance are monitored using KRIs and KPIs

○ 7. All of the above

○ 8. None of the above

Evolve from Agile GRC to Cognitive GRC.

Agile GRC: Improved usability, configurability, and integrations

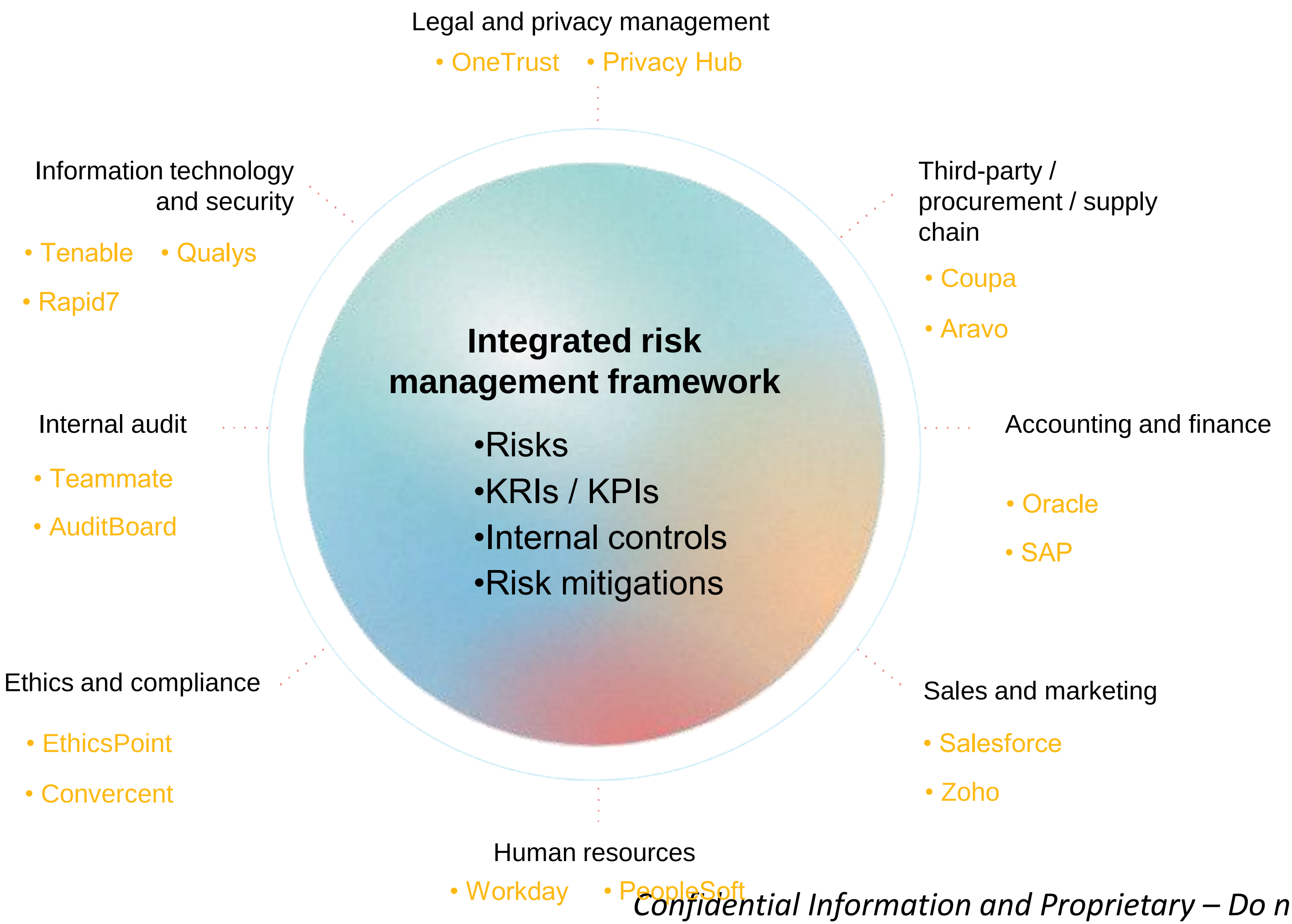
Cognitive GRC: Data-focused, cross-functional automation

Areas where Cognitive GRC can improve your organization:

- Internal and external monitoring and profiling
- Benchmarking and measurement
- Predictive analytics
- Virtual subject matter experts
- Robotic process automation

> “Cognitive GRC will take GRC from the back-office and the front-lines to new worlds of understanding, insight, and action.
>
> - Michael Rasmussen, GRC analyst at GRC 20/20 Research, LLC

Data will be the “new oil” for your risk management program.



Legal and privacy management

- OneTrust
- Privacy Hub

Information technology and security

- Tenable
- Qualys
- Rapid7

Third-party / procurement / supply chain

- Coupa
- Aravo

Integrated risk management framework

- Risks
- KRIs / KPIs
- Internal controls
- Risk mitigations

Internal audit

- Teammate
- AuditBoard

Accounting and finance

- Oracle
- SAP

Ethics and compliance

- EthicsPoint
- Convercent

Sales and marketing

- Salesforce
- Zoho

Human resources

- Workday
- PeopleSoft

What can data do for you today?

- Monitor KRIs/KPIs using data from first- and second-line systems
- Evaluate external risks related to third parties, regulations, and economic indicators
- Predict emerging risks and trends using artificial intelligence
- Utilize robotic process automation to perform remediation activities
- Leverage risk quantification and data analytics to report economic risk exposure

Poll question:

Which technologies does your risk management program use today?

○ 1. KRI monitoring platform

○ 2. KPI monitoring platform

○ 3. Artificial intelligence

○ 4. Robotic process automation

○ 5. Risk quantification

○ 6. Data analytics

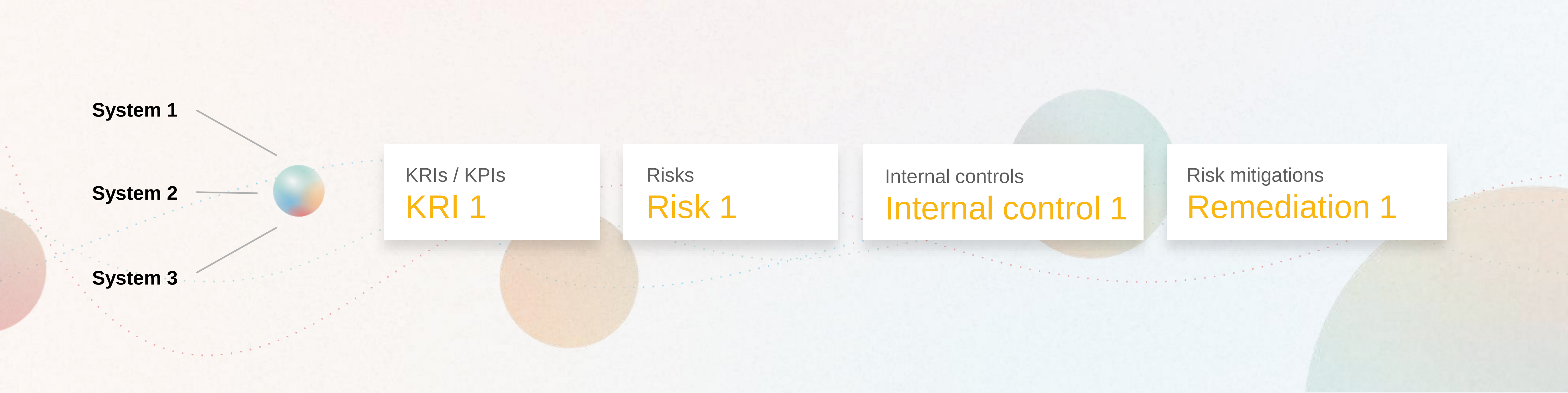
○ 7. None of these

“

How can I start using these technologies today?

Your path to collaboration and automation starts with a strong risk content framework.

- Set up your risk content framework to involve cross-functional teams.
- Identify ways to "inform" your risk content framework with business system data.
- Gather risk data from your business systems using automated connectors.
- Convert risk data to KRI metrics and monitor risk trends on a continuous basis.



Confidential Information and Proprietary – Do not distribute

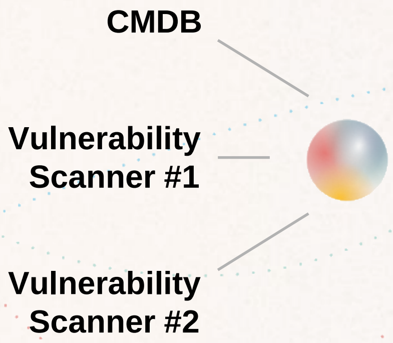
Example #1

Analysis of IT servers containing PII/PHI and open critical vulnerabilities.

Collaboration across teams…

● Information technology and security

● Legal and privacy management



KRIs / KPIs

% of IT servers that have open critical vulnerabilities and contain PII/PHI

Risks

IT systems and applications containing PII/PHI are not optimally secured with all available security patches installed.

Internal controls

IT servers containing PII/PHI should be scanned weekly. Critical vulnerabilities should be patched within one day of identification.

Risk mitigations

1. Review IT servers with PII/PHI from latest vulnerability scans.
2. Review logs on unpatched servers for potential breach activity.
3. Communicate results with IT and Privacy teams.

Example #2

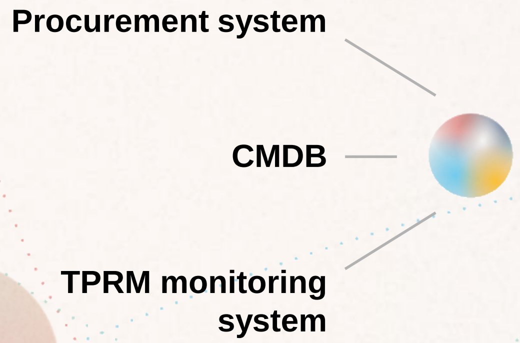
Analysis of third parties with high likelihood of information leaks and access to company PII/PHI.

Collaboration across teams…

● Information technology and security

● Legal and privacy management

● Third-Party / procurement / supply chain



Procurement system

CMDB

TPRM monitoring system

KRIs / KPIs

Total number of third parties with high likelihood of information leakage and access to IT servers containing PII/PHI.

Risks

The organization is unaware of what third parties are providing services and may be accessing systems containing PII/PHI.

Internal controls

The organization maintains a list of all third-party vendors and all external connections that are dependent on business processes involving PII/PHI.

Risk mitigations

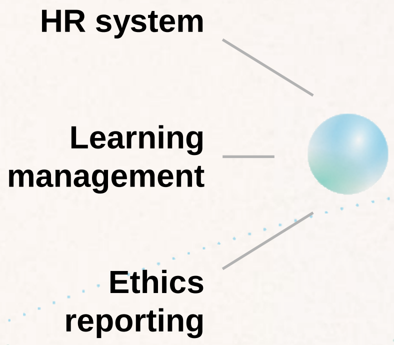
1. Notify relationship managers of risk pertaining to their third parties.
2. Review logs on third-party-accessible servers for potential breach/leakage activity.
3. Communicate results with relationship manager, third-party contact, and privacy team.

Example #3

Analysis of unconscious bias awareness training vs. ethics violations reported.

Collaboration across teams…

● Human resources ● Ethics and compliance



KRIs / KPIs

% of employees not completing unconscious bias awareness training vs. ethics violation reports

Risks

Employees are not adequately trained on unconscious bias awareness, resulting in increased violations

Internal controls

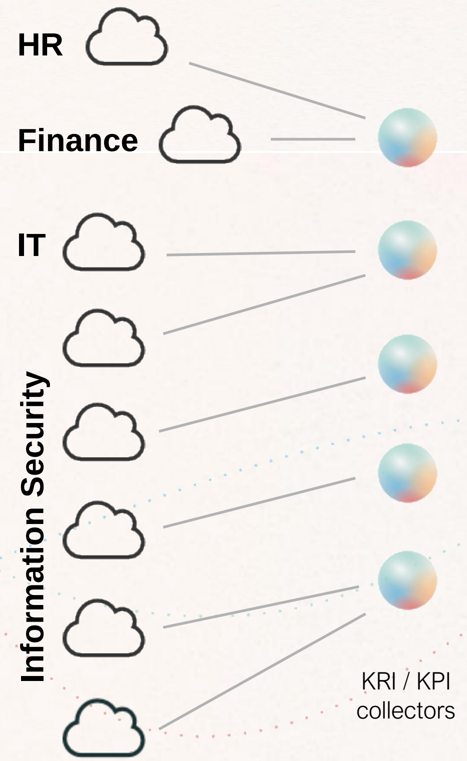
Employees complete unconscious bias awareness training on an annual basis

Risk mitigations

Targeted training concepts required to raise awareness on unconscious bias

Crowe Risk and Performance Monitoring

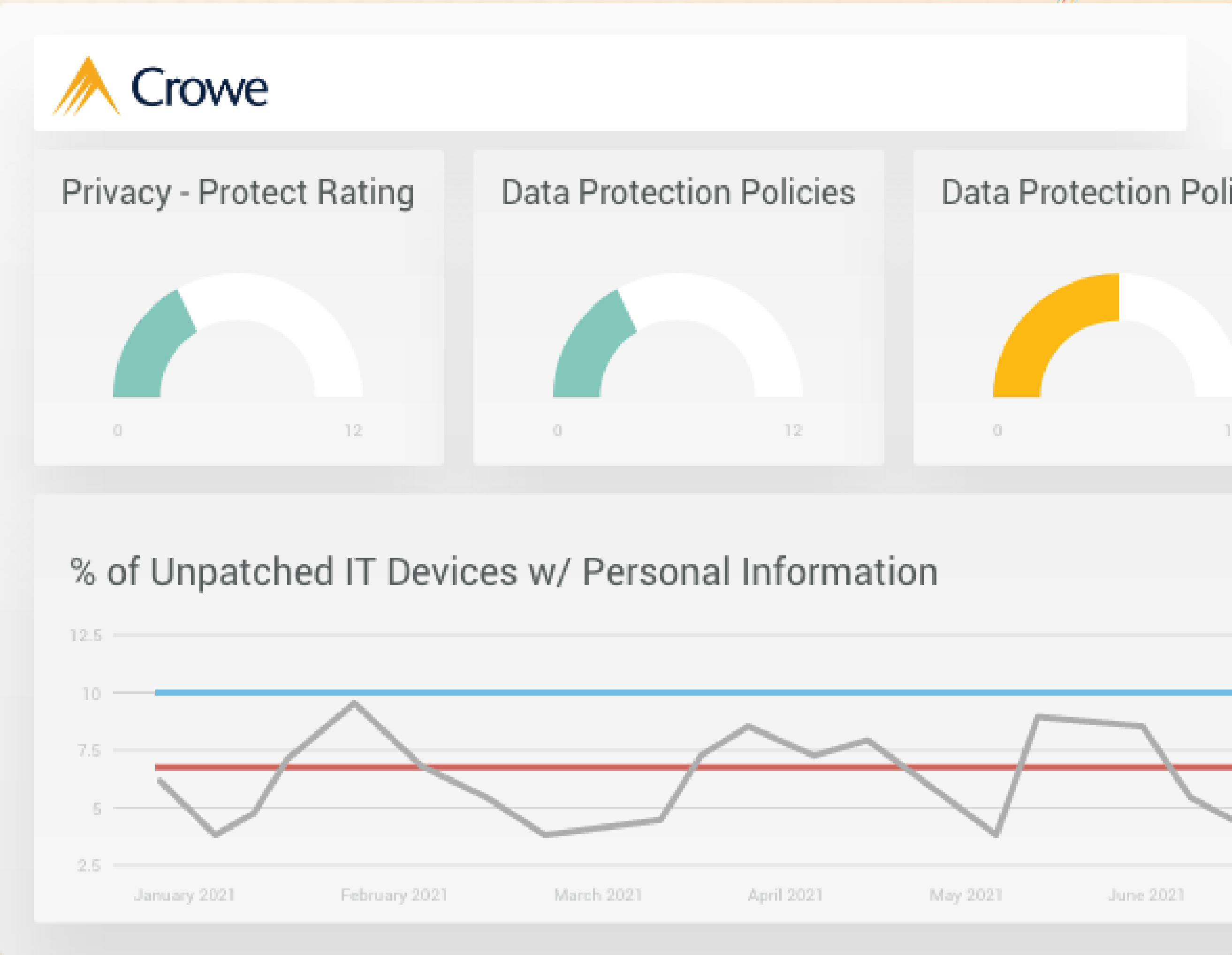
Efficiently manage content and remediation activities.



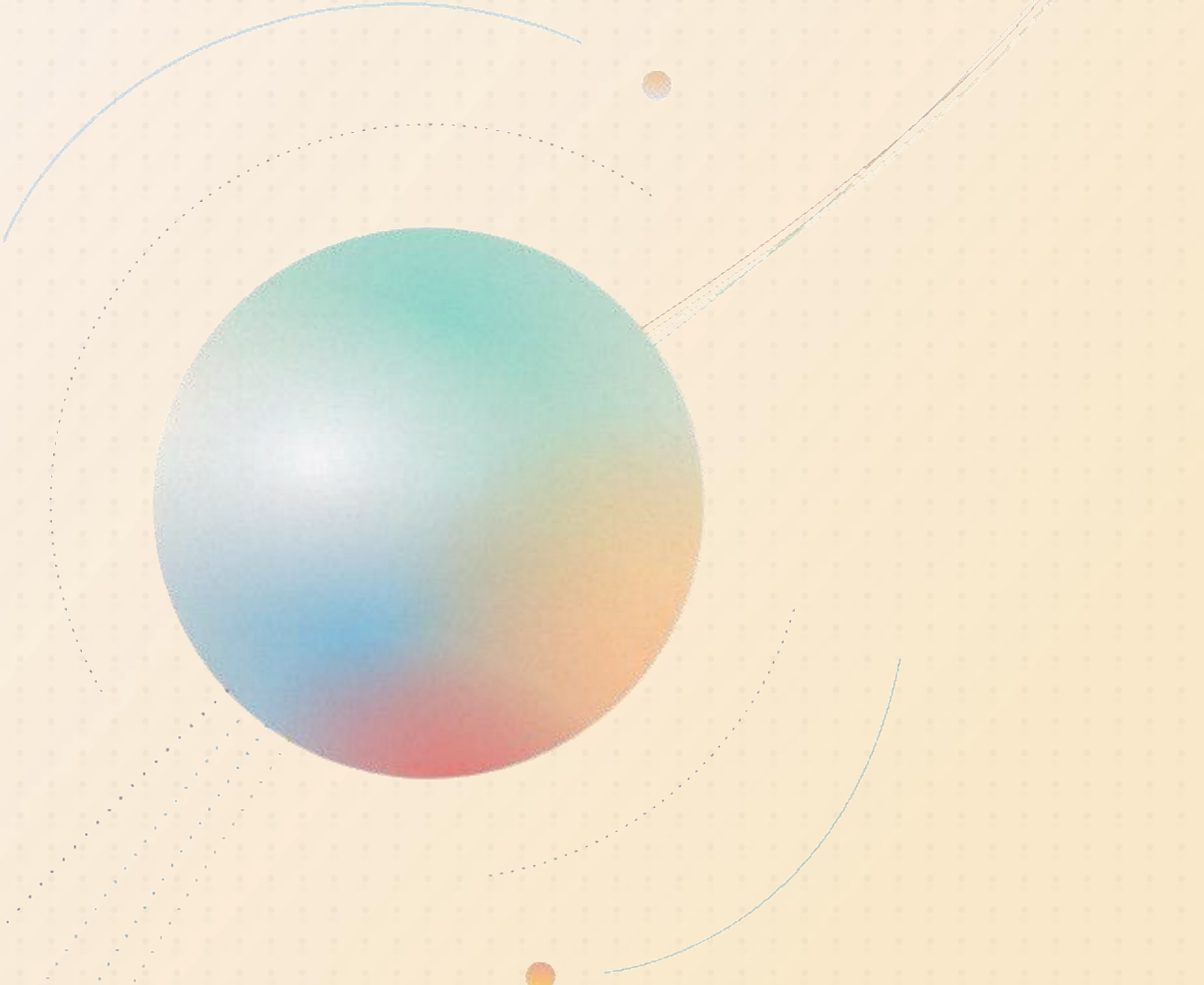
KRIs / KPIs	Risks	Internal controls	Risk mitigations
KRI 1	Risk 1	Internal Control 1	Remediation 1
KRI 2	Risk 2	Internal Control 2	Remediation 2
KRI 3	Risk 3	Internal Control 3	Remediation 3
KRI 4	Risk 4	Internal Control 4	Remediation 4
KRI 5	Risk 5	Internal Control 5	Remediation 5

Confidential Information and Proprietary – Do not distribute

Crowe Risk and Performance Monitoring



Questions?



We can help you take risk management to the next level.

Reach out to schedule a full demonstration.

Josh Reid

Crowe Principal
GRC technology services leader

josh.reid@crowe.com

Confidential Information and Proprietary – Do not distribute

Thank you.

NAVEX™