RISK & INSURANCE®

Hardening Defense in Depth Cyber Risk Management Principles with Integrated Regulatory Risk Management

Sponsor:

THANK YOU TO OUR SPONSOR

SPONSOR: RISKONNECT

- Riskonnect, a Thoma Bravo portfolio company, is the trusted, preferred source of integrated risk management technology, offering a growing suite of solutions on a world-class cloud computing model that enable clients to elevate their programs for management of all risks across the enterprise.

- Riskonnect, which was recognized as a Leader in The Forrester Wave™: Governance, Risk, and Compliance Platforms, Q1 2018, allows organizations to holistically understand, manage, and control risks, positively affecting shareholder value.

- For more information about Riskonnect, visit www.riskonnect.com or call +1-770-790-4700.

PRESENTERS

Lynn Heiberger

COO | Unified Compliance

Rajesh Unadkat

AVP, Strategic Marketing GRC | Riskonnect

Cameron Jackson

Sr. Director, Market Strategy & Development | Riskonnect

Moderator:

Dan Reynolds

Editor-in-Chief

Risk & Insurance®

RISK&INSURANCE

Sponsor: riskonnect. Integrated Risk Management Solutions™

Riskonnect Overview: Company Profile

280+ World-Class Customers

65% Client Growth Over 4 Years

50% User Growth YOY

Users in 80+ Countries

Decade of Consistent Growth and Client Success

MISSION

Empower business professionals to make better strategic decisions while managing risks across their entire organization with greater transparency and efficiency.

RISK&INSURANCE

Sponsor: riskonnect. Integrated Risk Management Solutions™

Riskonnect Overview: 2018 FORRESTER WAVE™ LEADER

Riskonnect Recognized as a Leader in
The Forrester Wave™:
Governance, Risk, and Compliance Platforms.

Earned the highest possible scores in the following criteria:

- End User Experience
- Risk and Control Management
- Integration Capabilities
- Organizational Context
- Document Management
- Input/Output
- Distribution and Communication and Language Support

RISK&INSURANCE

Sponsor: riskonnect. Integrated Risk Management Solutions™

CIO JOURNAL.

CIOs Focused on Compliance as Global Rules Toughen, Says Microsoft Azure Data Chief

CIO JOURNAL.

The Morning Download: Europe's New Privacy Rule, in Unexpected Twist, Helps Facebook, Google

TECH

Yahoo's Successor to Pay $35 Million in Settlement Over Cyberbreach

Regulators, in a first, penalize public company that was the victim of a hack

ECONOMY | CAPITAL ACCOUNT

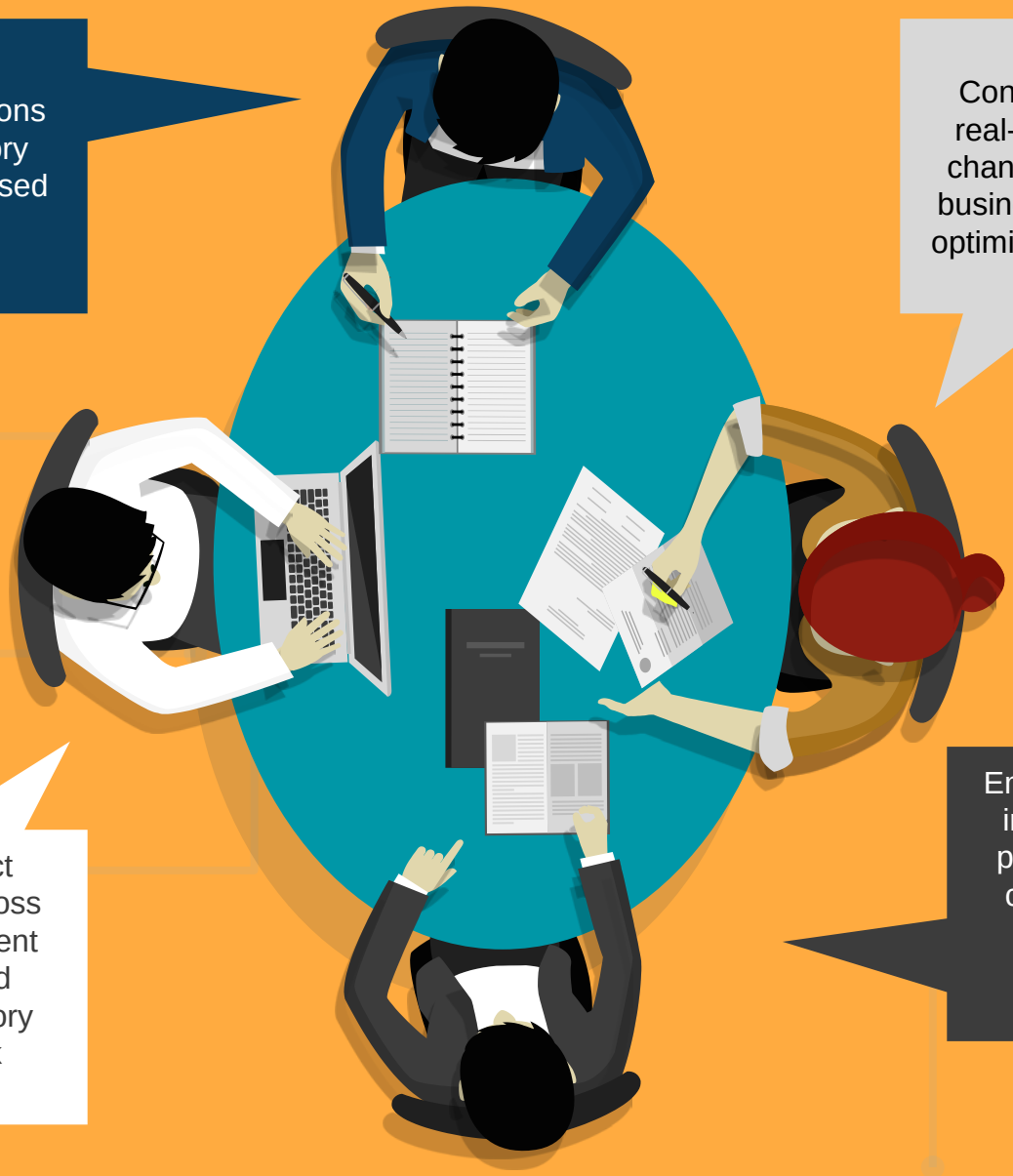
Financial Deregulation Throws Fuel on Already-Hot Economy

Moves to ease post-crisis rules spur lending and risk-taking even as industry is lowering its own standards

RISK&INSURANCE

Sponsor: riskonnect. Integrated Risk Management Solutions™

Risk-based decisions demand regulatory and framework based context.



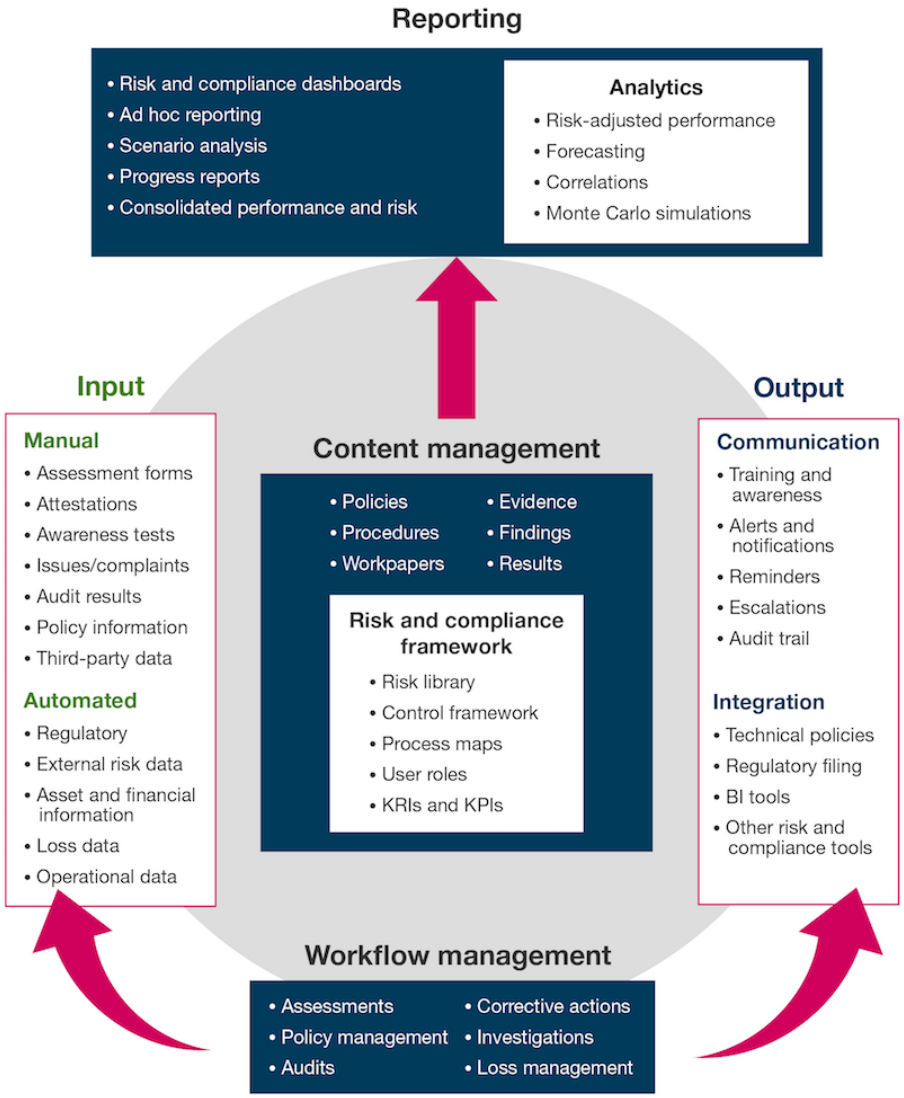
Connected POV to real-time regulatory change supports our business strategy and optimizes performance

Business Impact Assessments across all risk management functions should measure regulatory and framework implications

Embedding regulatory intelligence into the planning and design components of risk management and audit programs is essential

riskonnect.
Integrated Risk Management Solutions™

The Criticality of Content Intelligence



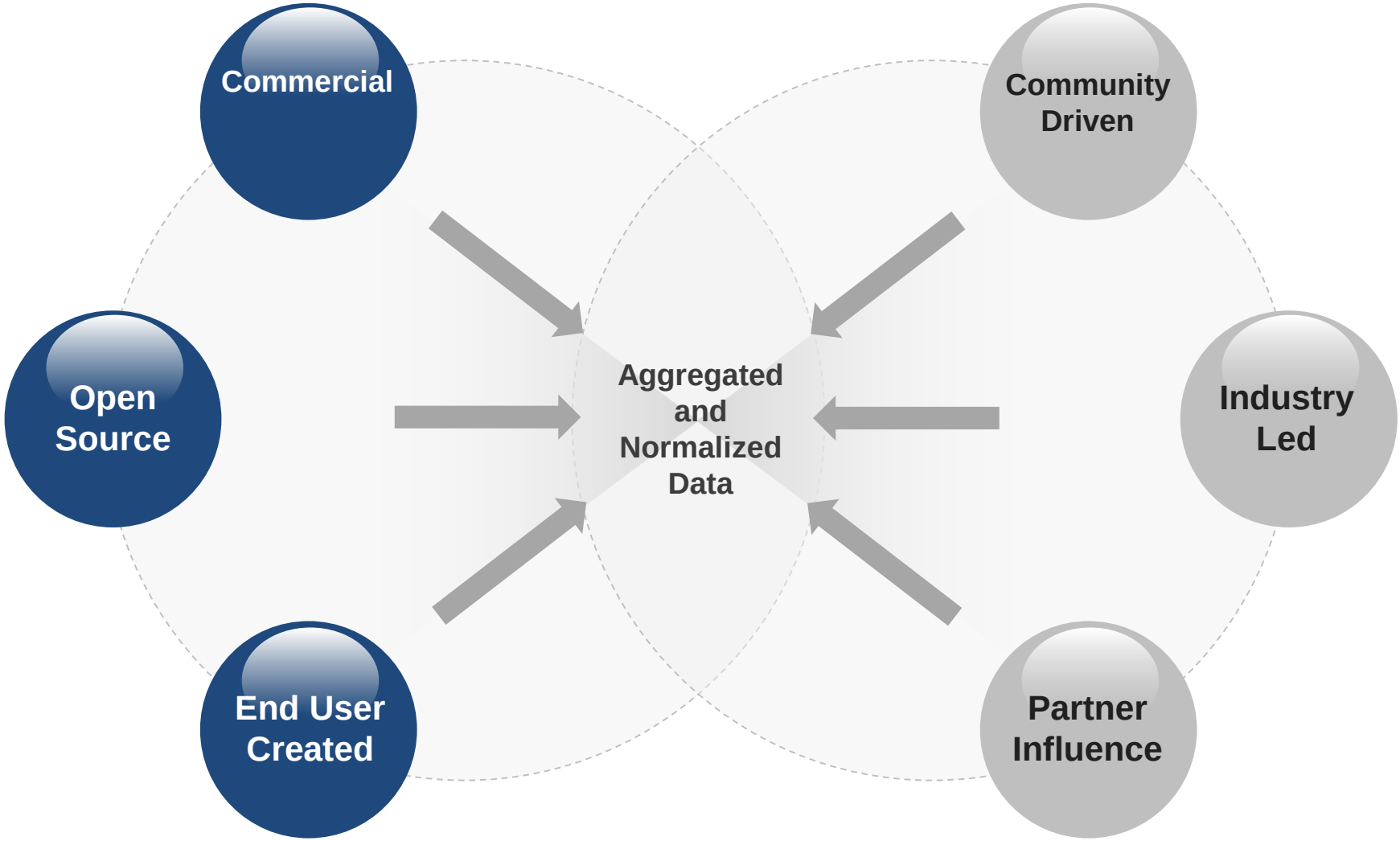
FORRESTER®

RISK&INSURANCE

Sponsor: riskonnect. Integrated Risk Management Solutions™

Multiple vendors offer UCF, but how does one differentiate?

Multi-Source Intelligence



Profiling Intelligence Sources

Success with Content Intelligence - The End User Experience

- Simple User Experience
- Personalization
- Automation
- Robust and Flexible Analysis (e.g. Gap Analysis, Rationalization, Redundancy)
- Defensible Positioning

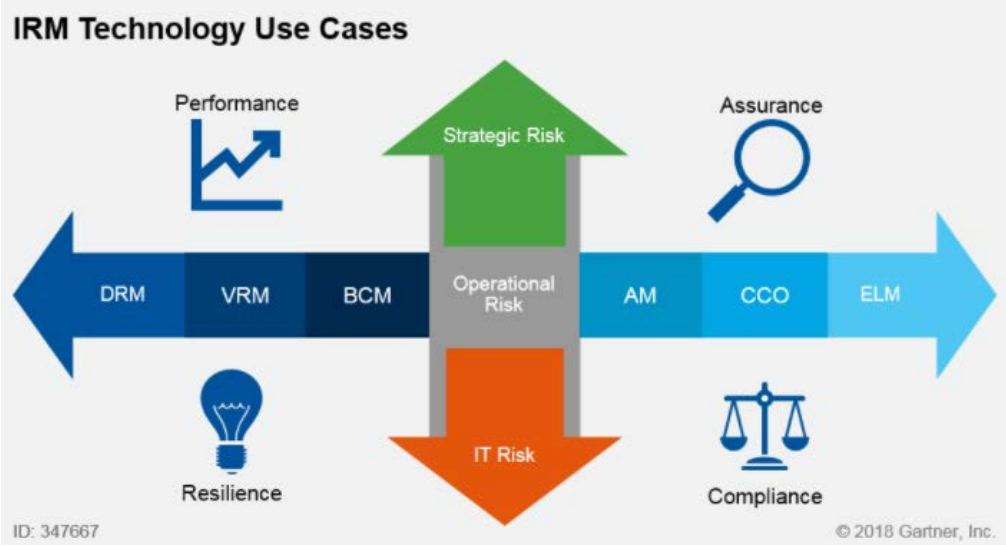
Content must be Intelligent and Simple

- Visualization and dynamic interactive reporting is key
- Content for the sake of content does not provide value
- Many to many data models that support bidirectional interaction helps
- Connecting content to data points (e.g. risks, controls, audit plans, issues, etc.) is where the value creation originates and intelligence is born
- Geographic and industry specific capabilities is always in demand

Key Foundational Use Cases

Integration of Content Intelligence into fundamental risk management activities:

- Policy Management
- Risk Assessment
- Business Process Modeling
- Control Design, Operation and Monitoring
- Issue and Remediation Management
- Reporting



Unified Compliance Framework – a Common Controls Framework

- Regulatory Nature of the Insurance Industry
- How to Simplify the Process of Compliance
- Harmonizing Controls to a Framework
- Common Language for Communication
  - Tagging Citations
  - Matching Controls
  - Creating a List of Authority Documents

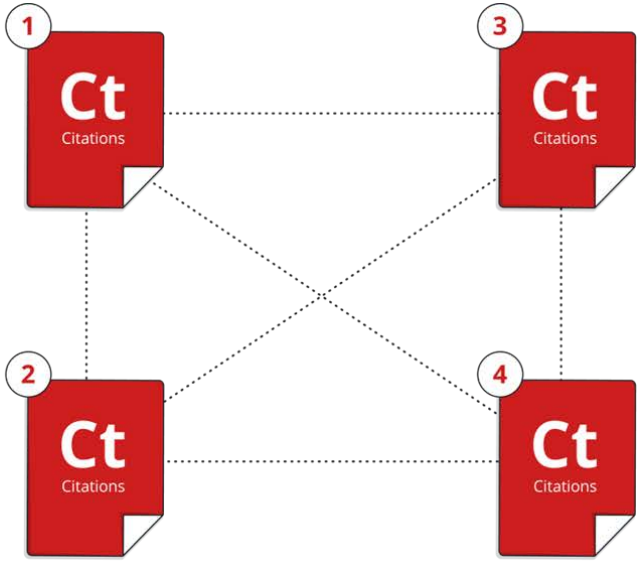
Regulatory Nature of the Insurance Industry

- Need to Keep Data Private – Federal and State
  - State Privacy Laws
  - 45 CFR Part 164 – Security and Privacy
- Comply with Requirements and Best Practices
  - NIST 800-53r4
  - ISO 27001
- Applies to All Insurance
  - Insurance Data Security Model Law, NAIC MDL-668
  - Standards for Safeguarding Customer Information Model Regulation, NAIC MDL-673
  - Privacy of Consumer Financial and Health Information Regulation, NAIC MDL-672

Simplify the Process of Compliance – Identify Overlap

A data subject who can prove he/she has a legitimate interest may, upon request from the data controller, receive free of charge, without excessive waiting periods, and at reasonable intervals, the following: access to any personal data about him/her in the data controller's possession; confirmation... *(Art 28(1), Art 28(3), Art 28(5), Law of 2 August 2002 on the Protection of Persons with Regard to the Processing of Personal Data)*

Individuals have the right to request access to personal data; the request must be granted within a reasonable time period. *(Art 20, Japan Handbook Concerning Protection Of Personal Data, February 1998)*



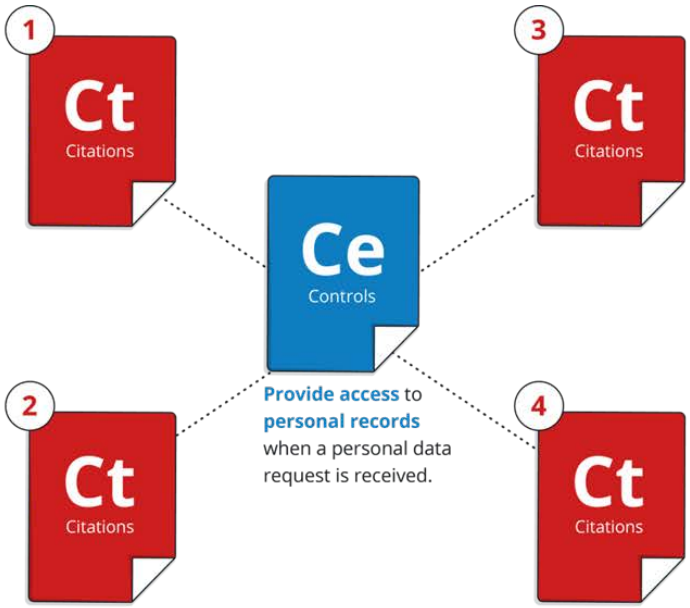
When a data subject requests information on the processing of his/her personal data, the data controller must provide it without undue delay. The information must contain the purpose of the processing; the categories subject to processing and their source; the recipients or categories of recipients;... *(Art 12(1), Art 12(2), Czech Republic Personal Data Protection Act, April 4, 2000)*

It is mandated that public institutions shall, upon request by a concerned party, reply to inquiries on, permit review of, and make duplicates of the personal data file maintained by it, unless an exception applies. *(Art 12, Taiwan Computer-Processed Personal Data Protection Law 1995)*

Harmonize to a Common Control Framework

A data subject who can prove he/she has a legitimate interest may, upon request from the data controller, receive free of charge, without excessive waiting periods, and at reasonable intervals, the following: access to any personal data about him/her in the data controller's possession; confirmation... *(Art 28(1), Art 28(3), Art 28(5), Law of 2 August 2002 on the Protection of Persons with Regard to the Processing of Personal Data)*

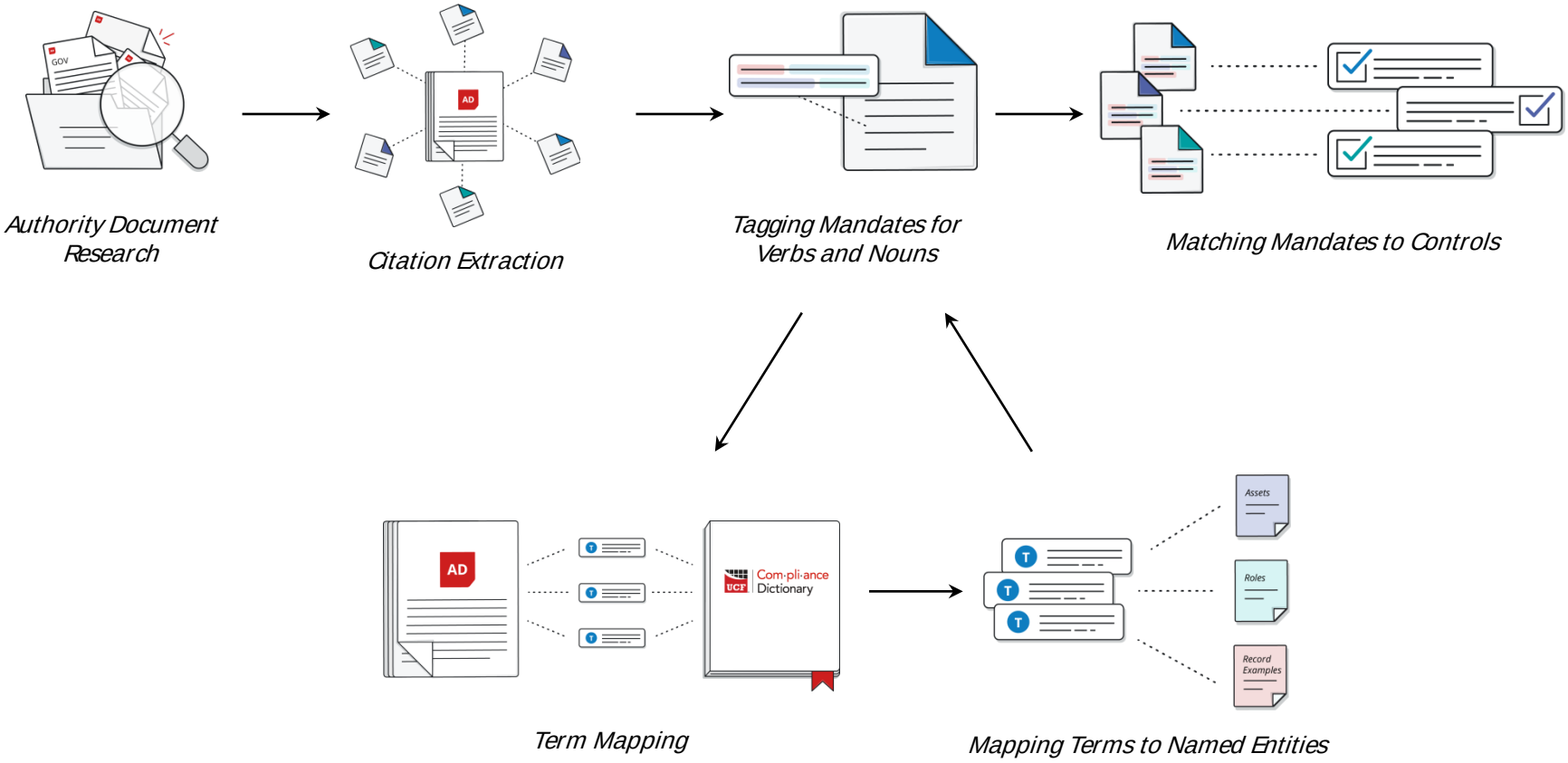
Individuals have the right to request access to personal data; the request must be granted within a reasonable time period. *(Art 20, Japan Handbook Concerning Protection Of Personal Data, February 1998)*



When a data subject requests information on the processing of his/her personal data, the data controller must provide it without undue delay. The information must contain the purpose of the processing; the categories subject to processing and their source; the recipients or categories of recipients;... *(Art 12(1), Art 12(2), Czech Republic Personal Data Protection Act, April 4, 2000)*

It is mandated that public institutions shall, upon request by a concerned party, reply to inquiries on, permit review of, and make duplicates of the personal data file maintained by it, unless an exception applies. *(Art 12, Taiwan Computer-Processed Personal Data Protection Law 1995)*

Harmonizing Controls to a Framework



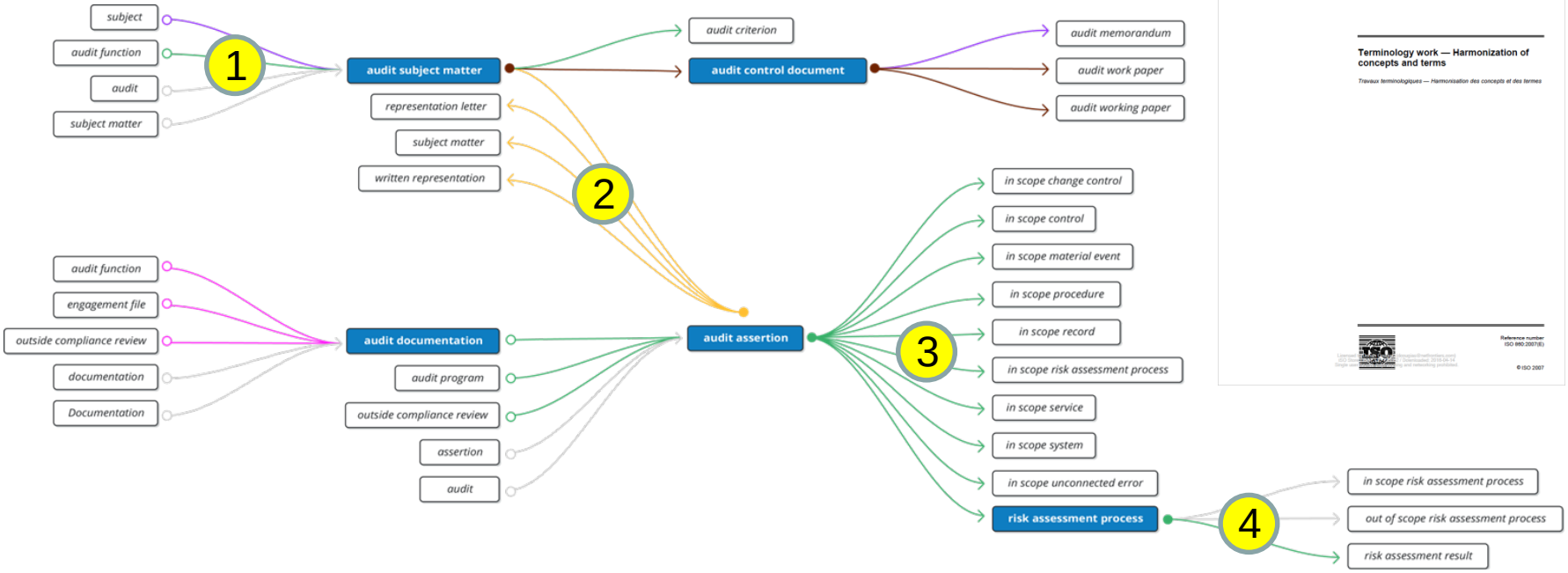
An Example with NIST 800-171

CITATION REFERENCE	NIST 800-171 CITATION GUIDANCE	CC ID	CONTROL TITLE
3.1.2	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	01411	Establish access rights based on least privilege.
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	01411	Establish access rights based on least privilege.

Different Words; Same Requirement

permitted to execute.

Common Language for Communication - Dictionary



INTERNATIONAL STANDARD **ISO 860**

Third edition
2007-11-15

Terminology work — Harmonization of concepts and terms

Travaux terminologiques — Harmonisation des concepts et des termes

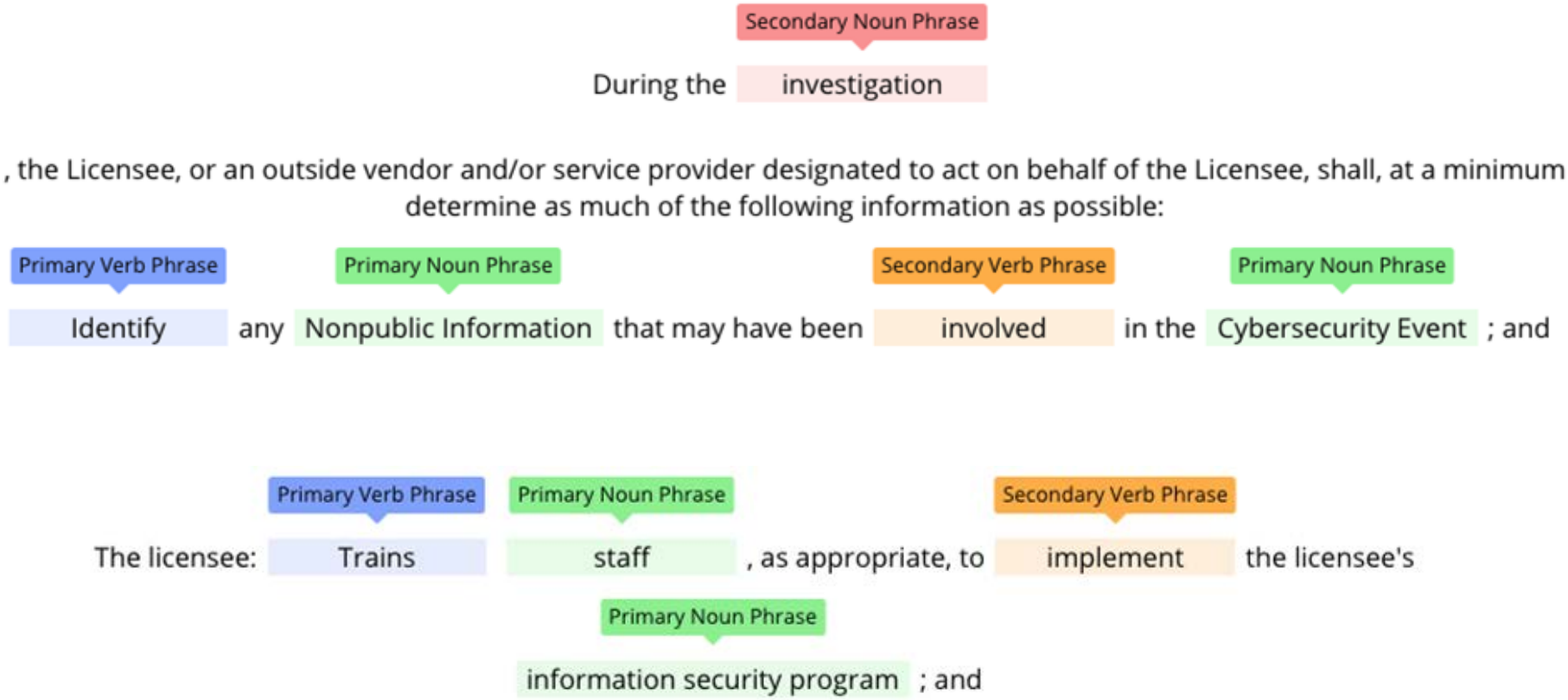
Reference number
ISO 860:2007(E)

© ISO 2007

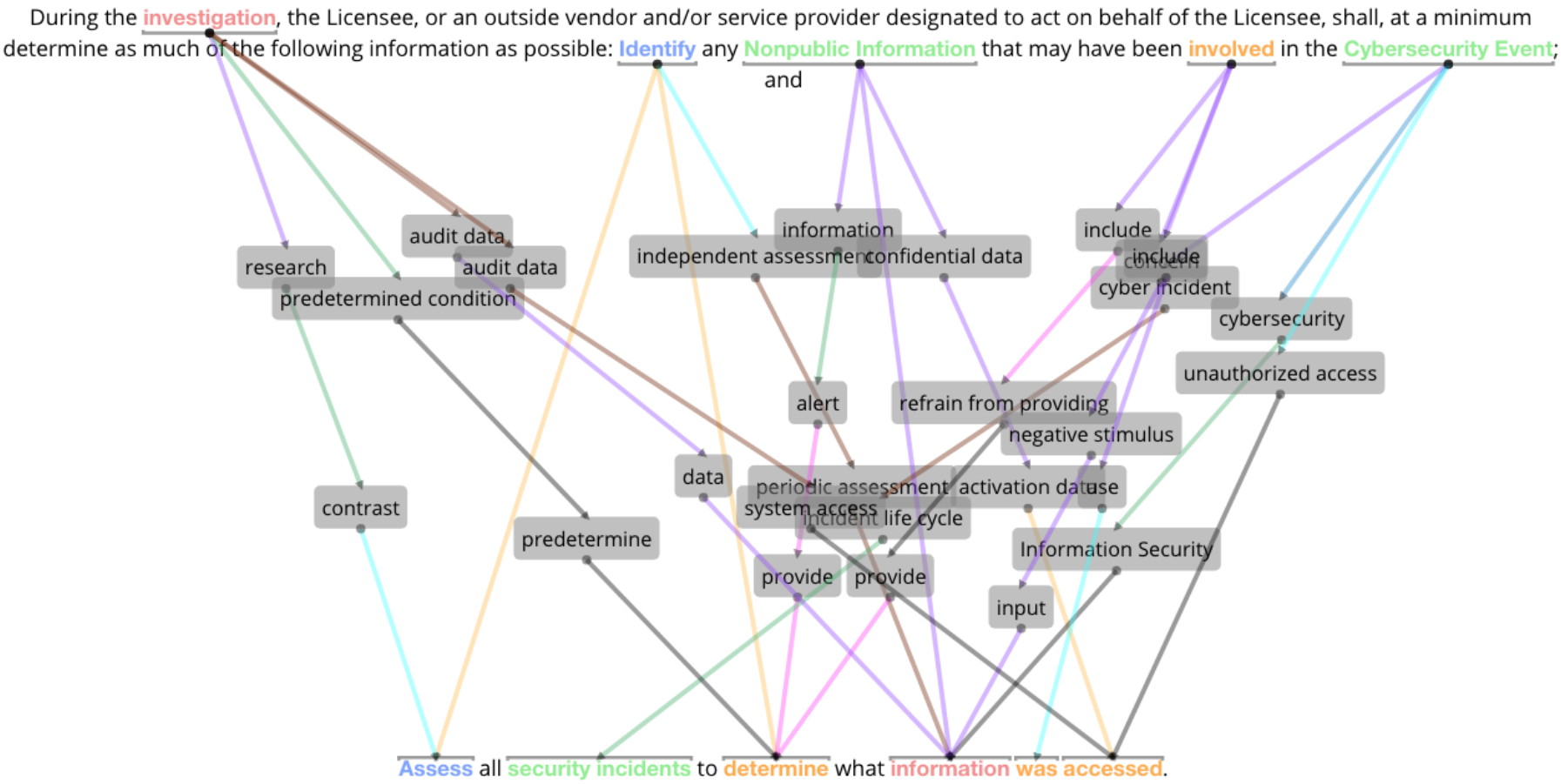
RISK&INSURANCE

Sponsor: riskonnect. Integrated Risk Management Solutions™

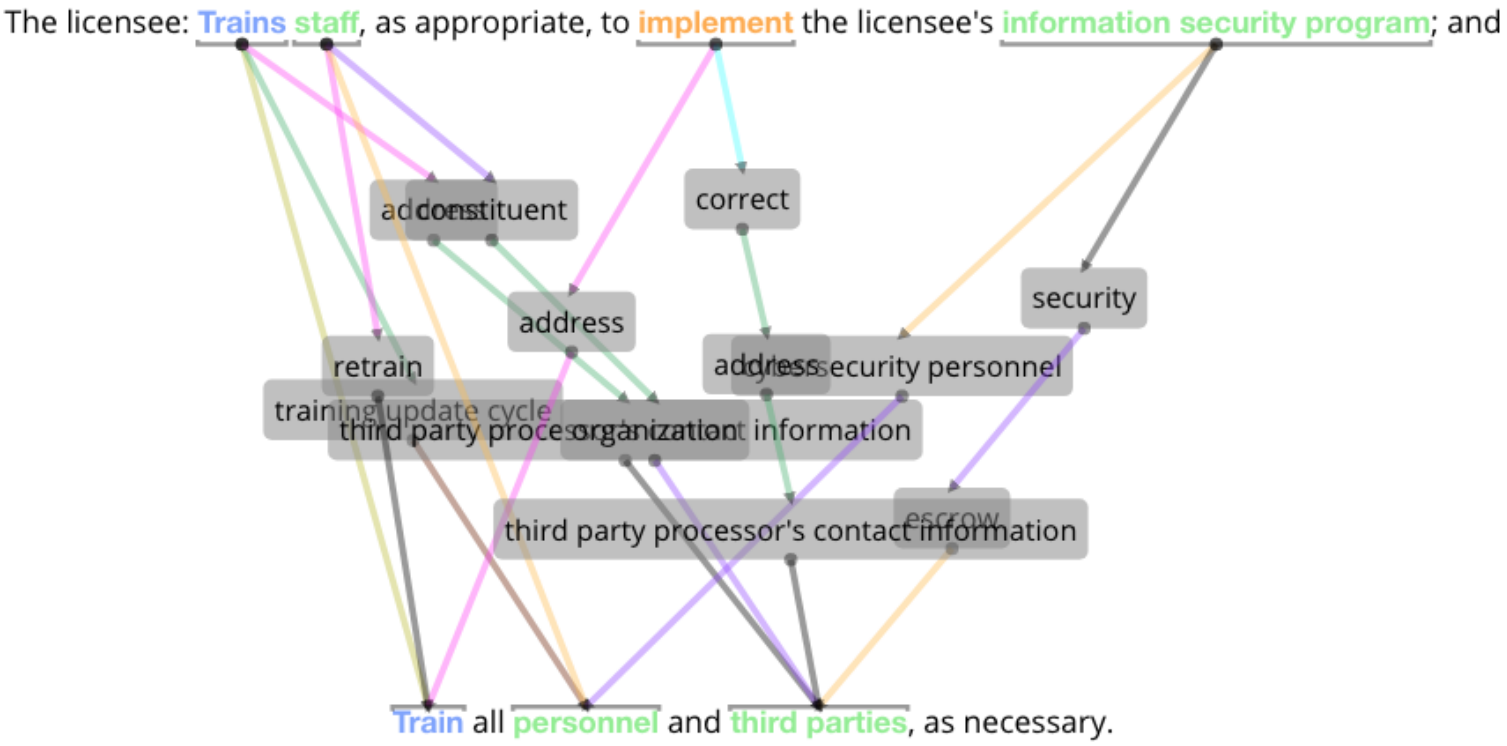
Common Language for Communication – Tagging Mandates



Common Language for Communication – Matching Controls



Common Language for Communication – Matching Controls



Common Language for Communication - Harmonization

- 01226 - Assess all security incidents to determine what information was accessed.
  - NAIC MDL-668 Section 5.B(3)
  - NAIC MDL-668 Section 5.B(1)
  - California OPP Notification of Security Breach Part III Timing of Notification ¶ 1
  - NIST 800-53 IR-9a
  - NIST 800-53 IR-9e
  - ISO 27001 A.16.1.4
- 00785 - Train all personnel and third parties, as necessary.
  - NAIC MDL-673 Section 7 ¶ 1.B.
  - NIST 800-53 AC-22b
  - NIST 800-53 PS-3(2)
  - ISO 27001 § 7.2 ¶ 1(c)
  - ISO 27001 § 7.2.2

The Solution (Riskonnect)

- Riskonnect's API based integration with CCH
- Customize UCF regulations & controls for your organization
- Compare regulatory standards for overlaps and gaps analysis
- Controls Assessment / Audit, Evidence Collection & Issue Reporting
- Issue Risk Measurement and Mitigation
- Save time and money by test once report many with Common Controls

QUESTIONS

SPONSOR: RISKONNECT

- Riskonnect, a Thoma Bravo portfolio company, is the trusted, preferred source of integrated risk management technology, offering a growing suite of solutions on a world-class cloud computing model that enable clients to elevate their programs for management of all risks across the enterprise.

- Riskonnect, which was recognized as a Leader in The Forrester Wave™: Governance, Risk, and Compliance Platforms, Q1 2018, allows organizations to holistically understand, manage, and control risks, positively affecting shareholder value.

- For more information about Riskonnect, visit www.riskonnect.com or call +1-770-790-4700.