



Houlihan
Lokey

Governance, Risk, and
Compliance
Market Update

1H 2025

Executive Summary:

GRC Market Update

Houlihan Lokey Governance, Risk, and Compliance Advisory Update

Houlihan Lokey has remained highly active in the governance, risk, and compliance (GRC) sector in the past 12 months with multiple closed/announced M&A advisory engagements as well as platform-building strategic moves:



- **Advised GRMS on its sale to Achilles.** The deal strengthens Achilles' position as a global leader in supply chain risk management and enables it to offer unparalleled insights and tools to enhance supplier relationships ([press release](#); see page 9).
- **Advised Brycer on its strategic investment from TA Associates.** The partnership aims to accelerate Brycer's growth as the company continues its mission of improving public safety through proactive compliance services and technology. TA's investment will enable Brycer to further enhance its technology platform, increase staff, execute strategic M&A, and expand its service offerings. ([press release](#); see page 10).
- **Advised PROtect and Spire Capital on their sale to Sterling Investment Partners.** The partnership will enable PROtect to focus on its next phase of growth, delivering lasting value to customers, employees, and stakeholders ([press release](#)).
- **Hired Andrew Atherton** to lead Houlihan Lokey's global governance, risk, and compliance coverage efforts ([press release](#)).

GRC Market Update



- The GRC ecosystem is undergoing rapid innovation across the value chain, impacting organizations of all sizes. Advances in **GenAI, data and analytics, and the rising complexity of enterprise risks** are fueling the next wave of GRC transformation, as **companies accelerate their digitization and cybersecurity initiatives**.
- Amid rising regulatory scrutiny, cybersecurity threats, and evolving ESG and data privacy mandates, **the GRC landscape is under growing pressure**. These dynamics are **driving demand for integrated, data-driven solutions** that enhance visibility, streamline workflows, and strengthen both compliance and risk management.
- **The sector remains active**, but capital raising and M&A activity have moderated, with deal volumes declining YoY through Q2 2025—continuing the cautious trend seen in 2024. That said, with regulatory complexity and cyber risk intensifying, **we anticipate a rebound in strategic activity in the second half of 2025** as buyers and investors refocus on solutions that deliver operational resilience and compliance efficiency.
- **Houlihan Lokey's public GRC Index has proven resilient**, on par with the S&P 500 YTD.⁽¹⁾

⁽¹⁾ Data derived from S&P Capital IQ as of July 17, 2025. See page 61 for more details on index composition and performance.

Introduction

We are pleased to issue our Governance, Risk, and Compliance Market Update for 1H 2025.

The Governance, Risk, and Compliance (GRC) market is at a pivotal juncture, driven by escalating regulatory complexities, an evolving risk landscape, and the growing demand for AI-powered, integrated, data-driven solutions. As organizations across sectors navigate an increasingly intricate landscape of compliance requirements and risk management challenges, GRC solutions have emerged as critical tools to streamline processes, enhance transparency, and foster resilience.

GRC has moved away from being a static and reactive set of systems and frameworks. Today's proactive, data-driven GRC industry empowers organizations of all sizes to automate compliance, anticipate risks, and integrate and build resilience. When leveraged correctly, GRC solutions empower businesses to take calculated risks confidently, balancing potential rewards with carefully managed vulnerabilities, all driving continued innovation and economic growth. Demand for and interest in GRC technology and data assets remain strong as tailwinds continue to benefit the sector and encourage the adoption of technology solutions.

With this report, we redefine our coverage and provide a comprehensive analysis of the GRC market, exploring key trends and themes shaping its evolution. Through market maps, we delineate our view of the key subsectors within the GRC ecosystem, offering insights into the diverse solutions addressing regulatory compliance, risk assessment, and governance frameworks. Additionally, this report examines recent M&A and capital markets activity, highlighting the strategic moves and investments fueling innovation and consolidation across sub-sectors. Drawing on authoritative third-party reports, we contextualize market dynamics, growth projections, and emerging opportunities.

As our firm continues to execute transactions in this space, we invite you to contact us to discuss past transactions, future opportunities, or the ecosystem more broadly. We hope that this report serves as a vital resource for stakeholders seeking to understand the transformative potential of GRC and its role in shaping the future of organizational resilience and compliance.

Best Regards,



Andrew Atherton

Managing Director

GRC Sector Lead

Andrew.Atherton@HL.com



Table of Contents

01

Houlihan Lokey and GRC Advisory Overview

- [How We Cover GRC](#)
- [Houlihan Lokey GRC Experience](#)
- [ONE Houlihan Lokey](#)

04

Public Market Performance and Valuation Update

- [Index Performance](#)
- [Public Company Trading Detail](#)

02

End Market Themes and Key Subsector Trends

- [Key End Market Themes](#)
- [Key Subsector Trends](#)

05

Notable Deal Activity: Investors, Acquirers, and Transactions

- [Sponsorscape](#)
- [M&A and Capital Raise Activity](#)

03

Vendor Market Maps

06

Appendix: Houlihan Lokey Platform Overview

- [Houlihan Lokey Overview](#)
- [Recent and Upcoming Conferences](#)
- [Additional Houlihan Lokey Coverage Reports](#)



Houlihan Lokey and
GRC Advisory Overview

01

Highly Collaborative, Cross-Functional Global GRC Team

Global GRC Leadership



Andrew Atherton
GRC Sector Lead
Managing Director
San Francisco, U.S.
Andrew.Atherton@HL.com



Sascha Pfeiffer
Global Head of Technology
Managing Director
Frankfurt, DE
Sascha.Pfeiffer@HL.com



Alec Ellison
Global Head of FinTech
Chief Innovation Officer
New York, U.S.
Alec.Ellison@HL.com



Ryan Lund
Global Co-Head of Software
Managing Director
Miami, U.S.
Ryan.Lund@HL.com

Cross-Industry Coverage Partners



Keith Skirbe
Cybersecurity
Managing Director
San Francisco, U.S.



Mark Smith
Cybersecurity and GRC
Managing Director
Manchester, U.K.



Bobby Wolfe
Cybersecurity
Director
Tampa, U.S.



Joy Sioufi
Technology
Managing Director
Paris, FR



Shane Kaiser
Supply Chain Technology
Managing Director
New York, U.S.



Timothy Macholz
Supply Chain Technology
Director
San Francisco, U.S.



Mark Fisher
FinTech
Managing Director
London, U.K.



Tim Shortland
FinTech
Managing Director
London, U.K.



Chris Pedone
FinTech
Managing Director
New York, U.S.



Anton Rothe
GRC Software
Senior Vice President
Stockholm, SE



Mike Capocci
FinTech
Director
New York, U.S.



Ranon Kent
Global Head of Business Services
Managing Director
Los Angeles, U.S.



Brian McDonald
Co-Head of Education Technology
and Services
Managing Director
New York, U.S.



Nana Kyei
Education Technology and Services
Managing Director
New York, U.S.



Dudley Baker
Healthcare Technology
Managing Director
Dallas, U.S.

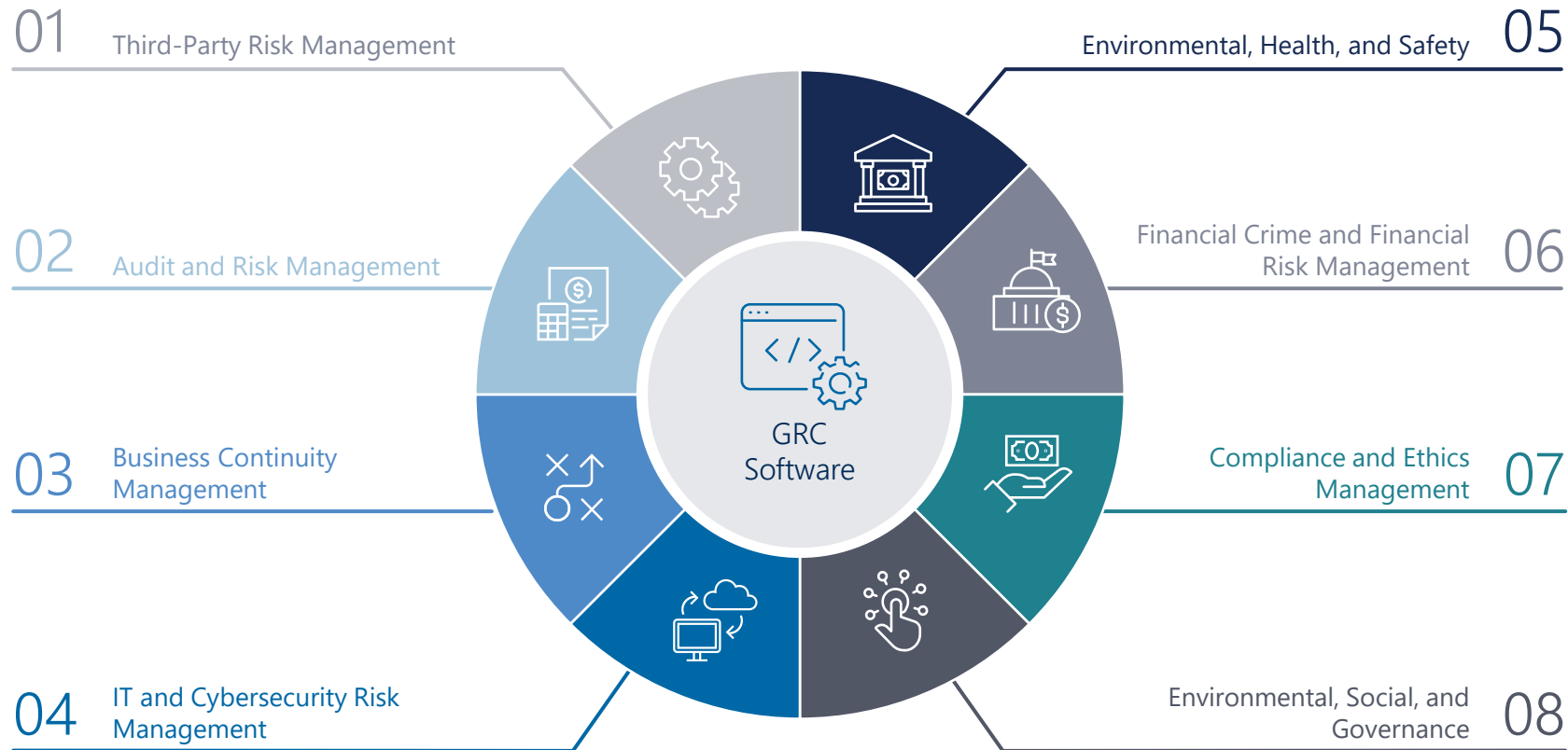


Luiz Greca
Healthcare Technology
Managing Director
Miami, U.S.

How We Cover Governance, Risk, and Compliance

At the early stages of digitization and automation, with significant opportunities for market growth.

Governance, Risk, and Compliance Applications



What Is GRC?

- **Governance:** Aligning processes and organizational activities with an organization's business goals.
- **Risk:** Identifying and addressing all the organization's risks.
- **Compliance:** Ensuring all activities meet global and local legal and regulatory requirements.

Used By

- Horizontal applications with use cases across all verticals and businesses of any size.
- Occasional vertical or geographic focus.

Different GRC Applications

- Digital and cyber threats, data privacy, and business continuity.
- Financial controls, reporting, audits, and compliance.
- Third-party, sourcing, and supply chain risks.
- Environmental compliance risks.
- Business disruptions, emergencies, and natural disasters.

Deep GRC Domain Expertise and Advisory Success

Houlihan Lokey has driven exceptional client outcomes throughout the GRC ecosystem.

PROtect
a portfolio company of
SpireCapital
has been acquired by
STERLING INVESTMENT PARTNERS
Sellside Advisor

GRMS
has been acquired by
Achilles
Sellside Advisor

ENVIANCE
a portfolio company of
Battery
has been acquired by
cority
Sellside Advisor

SUPPLYSHIFT
has been acquired by
sphera
Sellside Advisor

CGE PARTNERS
has acquired
enhesa.
Buiside Advisor

Hg
has acquired
Ideagen
Buiside Advisor

Apax
has acquired
Alcumus
a portfolio company of
inflexion
Buiside Advisor

inflexion
has acquired the Governance, Risk & Compliance software and services assets ("GRC") of
MARLOWE
Buiside & Financing Advisor

evision
has been acquired by
Wolters Kluwer Legal & Regulatory
Sellside Advisor

Atlas KNOWLEDGE
has been acquired by
MINTRAGROUP
Unlocking the Power of Competence
a portfolio company of
Riverside
Sellside Advisor

IDIQ
has sold a majority stake to
CORSAIR CAPITAL
Sellside Advisor*

enhesa.
a portfolio company of
CGE PARTNERS
has received a minority investment from
BregalSagemount
Sellside Advisor

BRYCER
has received strategic investment from
TA ASSOCIATES
Sellside Advisor

KPLER
has received a minority investment from
Five Arrows
INSIGHT PARTNERS
Sellside Advisor

VERAFIN
has completed a recapitalization with
SPECTRUM EQUITY
INFORMATION VENTURE PARTNERS
Fairness Opinion

IEQT
has acquired an investment in
RIMES
Financial Advisor

KINGLAND
has received a minority investment from
abry partners
Financial Advisor & Placement Agent

sambasafety
a portfolio company of
ABRY PARTNERS
has been acquired by
STONE POINT CAPITAL
Sellside Advisor

BIMM INSTITUTE
a portfolio company of
SOVEREIGN CAPITAL PARTNERS
has been acquired by
ICG
Sellside Advisor

Mini-case studies on following pages.

Note: Client is at the top of each tombstone.

Tombstones represent transactions closed from 2018 forward.

*Selected transactions were executed by Houlihan Lokey professionals while at other firms acquired by Houlihan Lokey or by professionals from a Houlihan Lokey joint venture company.

Financial Advisor to GRMS

Houlihan Lokey served as the financial advisor GRMS on its sale to Achilles.



Client Profile

GRMS is a global leader in providing customizable supplier risk management programs. It offers companies the ability to proactively manage and continuously monitor their suppliers for key areas of risk. GRMS' services include the adjudication of data, collection, physical review, and verification of documents with a support system that assists suppliers in obtaining compliance with a client's unique requirements. Since 2010, GRMS has served companies in more than 120 countries, ranging from mid-sized businesses to Fortune 500 firms.

Houlihan Lokey's Role

Houlihan Lokey served as the exclusive financial advisor to GRMS.

Transaction Snapshot

The acquisition of GRMS strengthens Achilles' position as a global leader in supply chain risk management, enabling it to deliver even greater value to organizations seeking to address complexities in supply chain risk management, compliance, and performance. The Achilles platform, with the addition of GRMS' expertise, will now offer unparalleled insights and tools to enhance supplier relationships and mitigate risk across financial stability, ESG, health and safety, geopolitical risk, cybersecurity, compliance, adverse media, and decarbonization.

The transaction closed on December 17, 2024.

The GRMS logo, consisting of the letters 'GRMS' in a bold, black, sans-serif font, is centered within a white square.

“

GRMS has built an outstanding reputation for delivering excellence in supplier risk assessment. This acquisition enhances our ability to provide unparalleled value to our customers by combining our global reach with GRMS' deep understanding of supplier risk management in the U.S. market.

Paul Stanley, CEO
Achilles

”

Exclusive Financial Advisor to Brycer

Houlihan Lokey served as the exclusive financial advisor to Brycer on its strategic investment from TA Associates.



Client Profile

Founded in 2011, Brycer is a leading provider of inspection, testing, and maintenance (ITM) compliance software for fire prevention bureaus, water municipalities, state building departments, and other regulatory organizations. Brycer's cloud-based solutions help streamline building inspection processes for fire protection systems, backflows, elevators, and other critical infrastructure. The company's flagship product, The Compliance Engine, equips Authorities Having Jurisdiction (AHJs)—such as fire prevention bureaus, water municipalities, and state building departments—to efficiently collect, manage, and track ITM reports for all commercial properties in their respective governing areas.

Houlihan Lokey's Role

Houlihan Lokey served as the exclusive financial advisor to Brycer. This transaction further strengthens the firm's leadership in the GRC technology space.

Transaction Snapshot

Brycer received a majority investment from TA Associates. The partnership aims to accelerate Brycer's growth as the company continues its mission of improving public safety through proactive compliance services and technology. The transaction included comprehensive up-front due diligence and preparation of key materials and analyses, which enabled a faster timeline, reduced diligence burden on management, and proactive messaging throughout the process. The transaction took six weeks from launch to signing, resulting in an exceptional outcome for the company.

“

As local governments have become increasingly focused on mandating regular preventive inspections, Brycer has emerged as a true pioneer in the ITM software market. The company's proven ability to provide innovative solutions that simplify complex compliance processes has made it a valuable, trusted partner for AHJs nationwide.

Todd Crockett, Managing Director
TA Associates

”

Exclusive Buyside and Financing Advisor to Inflexion

Houlihan Lokey served as the exclusive buyside and financing advisor to Inflexion on its strategic acquisition of Marlowe PLC's Governance, Risk, and Compliance software and services assets.



Client Profile

Founded in 1999, Inflexion is a leading middle-market private equity firm investing in high-growth, entrepreneurial businesses with ambitious management teams and working in partnership with them to accelerate growth. Inflexion's flexible approach allows it to back both majority and minority investments, investing £10 million to £500 million of equity in each deal.

Houlihan Lokey's Role

Houlihan Lokey served as the exclusive buyside and financing advisor to Inflexion. This transaction further strengthens the firm's leadership in the GRC technology space.

Transaction Snapshot

Inflexion acquired the Governance, Risk, and Compliance software and services assets of Marlowe PLC. Post acquisition, the stand-alone business will pursue an ambitious organic growth strategy through cross-selling of services, launching new software, and investment in sales and marketing. This will be complemented by M&A to broaden the product offering and support international growth.

inflexion

“

This Governance, Risk, and Compliance business operates in a fragmented, high-growth market and has the potential to scale into a global leader. We look forward to utilizing our strong sector experience and working with the management team to accelerate its growth both organically and through M&A.

Flor Kassai, Managing Partner and Head of Buyout
Inflexion

”

Our Tech M&A Team Is No. 1 Globally With Unparalleled Reach



AMERICAS

Atlanta
Baltimore
Boston
Charlotte
Chicago
Dallas
Houston

Los Angeles Miami

Minneapolis
New York
San Francisco
São Paulo
Washington, D.C.

EUROPE AND MIDDLE EAST

Amsterdam
Antwerp
Dubai
Frankfurt
London
Madrid

Manchester
Milan
Munich
Paris
Stockholm
Zurich

ASIA- PACIFIC

Beijing
Gurugram
Hong Kong SAR
Mumbai

Shanghai
Singapore
Sydney
Tokyo

No. 1

Global Tech M&A Advisor⁽¹⁾

14

Tech Locations Worldwide

140+

Tech Financial Professionals

~30

Tech Managing Directors

Houlihan Lokey has unparalleled experience advising on SaaS transactions.

The grid consists of 50 individual cards, each representing a SaaS transaction. Each card features the logo of the company involved, a short text description of the transaction, and the role of Houlihan Lokey. For example, the first card shows TitanHQ (a portfolio company of Livingbridge Oyster) merging with redstor (a portfolio company of BregalMilestone), with Houlihan Lokey acting as the Sellside Advisor. Other cards include transactions like VISTA:IR/SYNOVA merging with COMPLY365, flooid being acquired by inflexion, and many others. The roles listed include Sellside Advisor, Buy-side Advisor, and Financial Advisor.

Deal Momentum

No. 1
Global Tech M&A Advisor⁽¹⁾

101
Tech Deals in CY24

850+
Private Equity firms in the past five years have chosen Houlihan Lokey to advise on M&A or capital raises for their portfolio companies.

Tombstones represent transactions closed from 2013 forward.

*Selected transactions were executed by Houlihan Lokey professionals while at other firms acquired by Houlihan Lokey or by professionals from a Houlihan Lokey joint venture company.

(1) LSEG (formerly Refinitiv). Excludes accounting firms and brokers.

ONE HOULIHAN LOKEY

GLOBAL CONFERENCE

ONE Houlihan Lokey New York

Conference



May 13–15, 2025



New York Marriott Marquis



Business Services | Industrials | Oil and Gas



Consumer | Healthcare



Financial Services | FinTech | Tech



Missed the NYC event?
Join us in London, Nov. 18–20.

Houlihan Lokey was proud to host the largest showcase of dynamic businesses through a series of multiday conferences in 2025, one of which was hosted at the New York Marriott Marquis this past May. This premier event brought together the brightest minds in their industries and offered unmatched opportunities for networking, relationship building, and knowledge sharing.

This event highlighted key themes from across more than 160 sectors within multiple industries and services, including:

- Business Services
- Capital Solutions
- Consumer
- Financial Services
- Financial Sponsors
- FinTech
- Healthcare
- Industrials
- Oil and Gas
- Tech

ONE Houlihan Lokey is designed to connect decision-makers, highlight cutting-edge insights, and enable meaningful discussions amid evolving market dynamics. Across all three days, we welcome participants for:

- **Powerful Insights:** Hear from a multitude of companies spearheading change in their respective industries.
- **Unparalleled Networking Opportunities:** Engage with thousands of attendees from across global markets.
- **Meaningful Engagement:** Targeted one-on-one meetings will offer exclusive opportunities for connecting with senior capital providers.

Conference Highlights

4,000+ 380+

Conference Attendees Participating Companies

100+ 80+

Panels and Presentations Sectors Represented

2,680+ 1x1 Meetings



ONE HOULIHAN LOKEY

GLOBAL CONFERENCE

Introducing ONE Houlihan Lokey London

Conference



November 18–20, 2025



London Hilton on Park Lane



Consumer | Healthcare



Business Services | Industrials | Oil and Gas



Financial Services | FinTech | Tech

The 2025 ONE Houlihan Lokey Global Conference in New York was a tremendous success, hosting more than 4,000 attendees and 380 participating companies across three days of insightful discussions, 1x1 meetings, and compelling content.

Building on this momentum, Houlihan Lokey is proud to present the next event in its series of premier multiday conferences throughout 2025, showcasing dynamic businesses and industry leaders. This event will take place at the London Hilton on Park Lane this November, bringing together the brightest minds for unparalleled networking, relationship building, and knowledge sharing. This event will highlight key themes from across more than 160 sectors within multiple industries and services, including:

- Business Services
- Consumer
- Financial Sponsors
- Healthcare
- Oil and Gas
- Capital Solutions
- Financial Services
- FinTech
- Industrials
- Tech

ONE Houlihan Lokey is designed to connect decision-makers, highlight cutting-edge insights, and enable meaningful discussions amid evolving market dynamics. Across all three days, we look forward to welcoming you for:

- **Powerful Insights:** Hear from a multitude of companies spearheading change in their respective industries.
- **Unparalleled Networking Opportunities:** Engage with thousands of attendees from across global markets.
- **Meaningful Engagement:** Targeted 1x1 meetings offer exclusive opportunities for connecting with senior capital providers.



Interested in participating in the event? **Contact a team member to find out more.**

ONE Houlihan Lokey NYC Conference Highlights

4,000+ Conference Attendees

380+ Participating Companies

100+ Panels and Presentations

80+ Sectors Represented

2,680+ 1x1 Meetings





GRC End Market Update
and Key Subsector Trends

02

01.

Key Market Themes Driving Change Across the Value Chain

GRC Market Themes and Technology Environment (Pages 18–29)



Expansion and Complexity of Risks (Page 18)

Escalating geopolitical, climate, financial, and supply chain risks are increasing the complexity of required solutions.



Growing and Complex Regulatory Environment (Pages 19–20)

Advancements in technology and a shifting global order continue to push regulatory activity into more advanced frameworks.



Rise of AI and Automation in GRC (Pages 21–24)

Transforming GRC capabilities by enhancing efficiency and enabling organizations to navigate regulatory landscapes.



Increasing Importance of Data Analytics (Page 25)

Organizations can move from reactive, legacy approaches to proactive, agile risk management by adopting data-first policies.



Integration of Cybersecurity and GRC (Pages 26–27)

Regulatory pressure, growing threat surfaces, and board-level scrutiny are pushing organizations to seek cyber strategies.



The Enduring Relevance of EHS in an Evolving Risk Landscape (Pages 28)

From frontline safety to enterprise risk, EHS continues to anchor compliance strategies across sectors.



ESG Compliance Is Not Going Away (Page 29)

ESG compliance remains a key pillar for organizations globally, driven by regulatory mandates, investor scrutiny, and reputational risk.



Expansion and Complexity of Risks

Escalating geopolitical, climate, financial, and supply chain risks are driving demand for more sophisticated GRC solutions, as companies and investors alike recognize the need for integrated, adaptive frameworks to manage growing operational complexity and regulatory scrutiny.

IT and Cyber Risk

Involves threats to data security and IT infrastructure, such as cyberattacks, data breaches, or ransomware.

Key Statistic: In Q1 2025, cyberattacks per organization increased by 47%.

Examples

- Data Breach That Compromises Customer Data
- Malware Attack Disrupting Operations

Potential Impacts

- Data Loss
- Operational Downtime
- Financial Costs
- Erosion of Customer Confidence

Solutions

- GRC Platforms Fully Integrated With Cyber Tools to Monitor Threats
- Assess Vulnerabilities
- Document Incident Responses

Third-Party Risk

Potential threats an organization faces from its relationships with external entities—vendors, suppliers, contractors, partners, or service providers.

Key Statistic: The number of third-party breaches rose 49% year over year, increasing threefold since 2021.

Examples

- Hacked Software Provider
- Supplier's Inventory Impacted by a Natural Disaster
- Labor/Environmental Law Violation

Potential Impacts

- Data Breaches
- Operational Disruption
- Reputational Damage
- Compliance Risk
- Supply Chain Disruption

Solutions

- Third-Party Risk Management
- Cybersecurity Risk Management

Business Continuity Risk

Vulnerabilities that threaten an organization's ability to maintain essential operations and services. These risks often overlap with operational, geopolitical, or cybersecurity risks, but are distinct in their focus on recovery and adaptability.

Key Statistic: Continuity breaks cost between \$5,600 to \$16,000 per minute.

Examples

- Natural Disasters
- Cybersecurity Attacks
- Geopolitical Events
- Supply Chain Breakdown
- Employee-Related Risks

Potential Impacts

- Physical Asset Loss
- Operational Downtime
- Financial Loss
- Customer Impact
- Reputational Damage
- Employee Morale

Solutions

- Risk Assessment and Mapping
- Business Continuity Planning
- Real-Time Monitoring
- Incident Management

Regulatory Risk

Potential for an organization to face negative consequences due to changes in laws, regulations, or standards, or from failing to comply with them.

Key Statistic: The average U.S. firm spends between 1.3% and 3.3% of its total wage bill on regulatory compliance.

Examples

- Noncompliance
- Regulatory Changes
- Interpretation Risk

Potential Impacts

- Financial Penalties
- Operational Restrictions
- Damage to Credibility

Solutions

- Real-Time Monitoring
- Mapping of Internal Policies to Regulations
- Automating Compliance Checks
- Training

Safety Risk

Risks that arise from conditions, actions, or oversights that could lead to harm—such as injuries, illnesses, or fatalities—or damage to property and the environment.

Key Statistic: Workplace injuries and illnesses cost U.S. employers more than \$175 billion annually.

Examples

- Workplace Accidents
- Environmental Hazards
- Transportation Risks
- Product Safety

Potential Impacts

- Human Cost
- Financial Loss
- Legal and Regulatory Fallout
- Reputational Damage
- Operational Disruption

Solutions

- Risk Identification
- Compliance Tracking
- Incident Reporting
- Training Audit and Inspection
- Root Cause Analysis

Deep Fake and Impersonation Risk

Threaten businesses by enabling realistic impersonations that can deceive, mislead, and damage an organization's trust and finances.

Key Statistic: 42% of executives and board members have been targeted at least once by a fake image or video.

Examples

- Synthetic Competitor Claims
- Counterfeit Investor Pitches
- Forged Internal Memos

Potential Impacts

- Legal Liabilities
- Financial Losses
- Brand Reputation Damage
- Loss of Investor Trust

Solutions


- AI-Based Authenticity Checks
- Corporate Digital Forensics
- Strict Content Validation

Growing and Complex Regulatory Environment


The GRC landscape is evolving rapidly, driven by technological advancements, heightened cybersecurity concerns, and a global push for sustainability and ethical accountability.

Notable Regulations

Resilience


 **Digital Operational Resilience Act (DORA)**
Effective January 2025, DORA mandates that financial institutions in the EU enhance their ICT (Information and Communication Technology) risk management frameworks. It requires robust incident reporting, third-party risk oversight, and regular stress testing to ensure resilience against cyber threats and operational disruptions.

[Focus: Cybersecurity and Operational Resilience for Financial Entities](#)


 **Operational Resilience Framework (FCA/PRA)**
Financial firms must identify “important business services” and set impact tolerances (e.g., maximum downtime before harm occurs). Requires stress testing, scenario planning, and mapping of critical dependencies (e.g., third-party vendors).

[Focus: Operational Resilience](#)


Cybersecurity

 **NIST Cybersecurity Framework (NIST CSF)**
Provides a structured approach based on five core functions—Identify, Protect, Detect, Respond, and Recover—to strengthen security posture across industries.


[Focus: Manage Cybersecurity Risk](#)

 **Cybersecurity Maturity Model Certification (CMMC)**
Establishes tiered levels of maturity to ensure appropriate protection of sensitive federal information across defense contractors.

[Focus: Cybersecurity Protection for Defense Contractors](#)

 **Network and Information Security Directive 2 (NIS2)**
Builds on the original NIS Directive to enhance resilience, cooperation, and accountability across member states.


[Focus: Cybersecurity Resilience in Infrastructure Sectors](#)

 **Others: SOC2, ISO 27001**

Data Privacy

 **GDPR**
Global benchmark that continues to shape privacy laws worldwide (e.g., U.S. state laws, Brazil’s LGPD), with fines up to €20 million or 4% of turnover. Extraterritorial reach that impacts any firm handling EU data, driving global compliance standards.

[Focus: Data Privacy](#)

 **California Privacy Rights Act (CPRA) Amendments**
Building on the CCPA, the CPRA (fully effective since 2023 but with ongoing refinements in 2025) introduces stricter requirements for data minimization, consumer opt-outs, and audits for high-risk data processing activities. Similar state-level laws are emerging nationwide.

[Focus: Enhanced Data Privacy Protections](#)



Key Trends Driving Regulation

Cybersecurity Emphasis

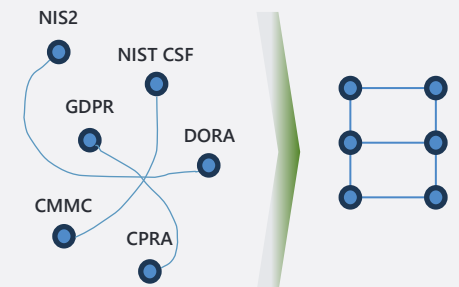
With breaches cumulatively costing billions annually, regulators are prioritizing resilience and rapid response (e.g., DORA, NIS2, SEC rules).

Average Total Cost of a Data Breach (\$ in M)



Global Convergence

While regional differences persist, there is a trend toward harmonizing standards (e.g., NIS2 and DORA aligning with global cybersecurity frameworks).



Growing and Complex Regulatory Environment (cont.)

Despite attempts at deregulation, the regulatory burden continues to expand and become more complex, imposing new requirements on organizations to adapt their risk management and compliance strategies.

Notable Regulations

ESG



Corporate Sustainability Due Diligence Directive (CSDDD)

Mandates human rights and environmental due diligence for large EU companies and certain non-EU firms with EU operations. 2025 marks a preparation year for compliance.

Entered into force in July 2024, with phased implementation starting in 2025 and obligations applying from 2027.

[Focus: Emerging Areas \(ESG\)](#)



Corporate Sustainability Reporting Directive (CSRD)

Applies to 50,000+ EU companies, plus non-EU firms with significant EU revenue (€150 million+). Requires detailed ESG disclosures (e.g., climate risks, social impacts), reshaping risk management (Web ID 4).

In effect since 2024, forcing firms to integrate ESG into GRC frameworks now.

[Focus: Emerging Areas \(ESG\)](#)

EHS



Occupational Safety and Health Act (OSHA)

U.S. law ensures safe working conditions across industries like construction, manufacturing, and healthcare. Employers must provide a workplace free from recognized hazards (e.g., falls, machinery risks, chemical exposures).

[Focus: Workplace Safety](#)



REACH Regulation (Registration, Evaluation, Authorization, and Restriction of Chemicals)

Effective since 2007 under Regulation (EC) No 1907/2006, REACH governs the production, import, and use of chemicals in the EU to protect human health and the environment. Its extraterritorial reach affects global supply chains, and 2025 sees tighter scrutiny on emerging contaminants like PFAS (forever chemicals).

[Focus: Chemical Safety and Environmental Protection](#)

Artificial Intelligence



EU AI Act

Risk-based approach that classifies AI systems (e.g., high-risk like hiring tools face strict rules; banned uses like social scoring). Fines up to €35 million or 7% of turnover—higher than GDPR. Global effect likely to influence AI regulation elsewhere, akin to GDPR's effect on privacy.

[Focus: Data Bias Mitigation](#)



ISO 42001

Provides a framework for organizations to manage AI systems responsibly, ensuring they are trustworthy, transparent, and aligned with legal and ethical requirements.

[Focus: Data Bias Mitigation](#)



AI Risk Management Framework (AI RMF)

Aims to promote the development and deployment of trustworthy AI by providing guidance that is adaptable across various sectors and use cases.

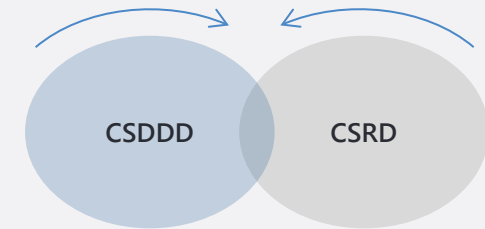
[Focus: Data Bias Mitigation](#)



Key Trends Driving Regulation

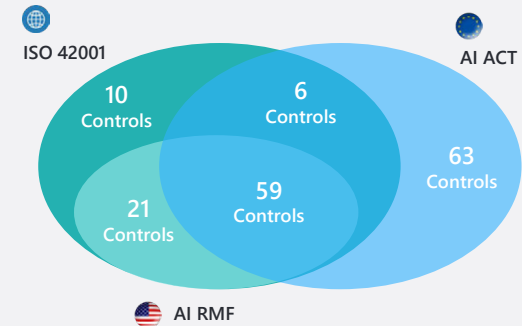
Sustainability Integration

ESG considerations are no longer optional, with laws like the CSDDD embedding them into corporate risk and compliance obligations.



AI Accountability

The rise of AI-driven decision-making has spurred regulations like AI Act, NIST AI RMF, ISO 42001 to ensure transparency and mitigate bias.





AI's Impact on Governance, Risk, and Compliance: How AI Enhances GRC

AI is significantly transforming the GRC sector. It is capable of detecting patterns indicative of fraud or threats, enhancing efficiency, improving decision-making, and enabling organizations to better navigate complex regulatory landscapes.

1

Enhanced Risk Management

AI-powered tools can analyze vast amounts of data in real-time to identify potential risks more effectively than traditional methods.

- Machine learning algorithms can detect patterns indicative of fraud, cybersecurity threats, or operational vulnerabilities by sifting through financial records, employee behavior, or external market signals.
- Unlike static annual reviews, AI-driven dynamic risk scoring updates risk scores on the fly by integrating live data, offering a continuous, real-time assessment of risk.
- This allows organizations to proactively address risks before they escalate, reducing exposure and improving overall resilience.

2

Automation of Compliance Processes

AI streamlines repetitive tasks like monitoring regulatory updates, mapping them to internal policies, and flagging noncompliance issues.

- NLP enables AI to interpret complex legal texts and extract key insights, saving time and reducing human error. Tools can automatically audit contracts or ensure adherence to standards like GDPR, HIPAA, or SOX.
- Automated policy creation tools can draft compliance policies or adapt existing ones to new regulations by analyzing legal texts and organizational needs.
- This allows organizations to stay ahead of consistently evolving industry standards, regulations, and domestic and foreign laws, reducing exposure to potential penalties.

3

Improved Governance Through Data Insights

AI enhances governance by providing deeper insights into organizational performance and decision-making.

- Predictive analytics can forecast the impact of strategic choices, while AI-driven dashboards offer real-time visibility into key performance indicators (KPIs) and risk metrics.
- AI can also streamline reporting, generating regulatory reports by pulling data from multiple sources, formatting it to meet standards like GDPR or SEC requirements, and flagging gaps—all in real time.
- This empowers boards and executives to make informed decisions aligned with corporate objectives and ethical standards and to take the right number of risks as they grow their businesses.

4

Cost Reduction and Efficiency

By automating manual processes, AI reduces the need for extensive human resources, cutting operational costs.

- AI automates cumbersome and resource-intensive tasks such as document review, risk assessments, or incident reporting, freeing up staff to focus on higher-value strategic tasks.
- Machine learning algorithms can efficiently analyze large documents and datasets to detect compliance gaps or emerging risks, allowing organizations to respond proactively rather than reactively.
- Small and mid-sized firms, in particular, benefit from scalable AI solutions that level the playing field and allow them to meet GRC demands without massive budgets.

KEY USE CASES VARY
ACROSS INDUSTRIES:



Finance

Monitors Transactions for AML Compliance



Healthcare

Flags Patient Data Breaches



Supply Chain

Assesses Vendor Risks

Key Statistics:

62%

Of organizations report that AI has significantly helped improve the efficiency of their compliance procedures.

67%

Of organizations say they would increase investments in AI [for GRC] because of the value delivered.

50%+

Of major enterprises expect to use AI and ML to perform continuous regulatory compliance checks in 2025, up from less than 10% in 2021.

51%

Of organizations report that navigating regulatory compliance is one of their top challenges.



AI's Impact on Governance, Risk, and Compliance: Challenges and Risks of AI in GRC

While AI brings benefits, it also introduces new complexities to GRC. For instance:

Data Quality and Availability:

- AI systems rely heavily on large, clean datasets to function effectively.
- If the data is incomplete, outdated, or inconsistent, AI can churn out unreliable insights.
- A poorly trained model might misinterpret a regulation, leading to an avoidable noncompliance.

Complexity of Regulation:

- Regulatory laws and compliance requirements are constantly evolving and often vague or context-specific.
- AI might struggle to keep up with real-time updates or to interpret nuanced legal language.
- In such instances, human oversight becomes critical, offsetting some of the efficiency gains that AI is meant to deliver.

Bias and Ethics:

- AI systems can perpetuate biases in training data, leading to flawed risk assessments or unfair compliance decisions.
- Imagine an AI system flagging certain transactions as high-risk based on biased historical patterns—say, disproportionately targeting specific regions or demographics. That's not just an ethical issue; it could trigger legal or regulatory backlash.

Cybersecurity and Privacy:

- AI tools themselves can become targets for attacks, necessitating robust safeguards to protect sensitive GRC data.
- A breach could expose confidential data or, worse, let bad actors manipulate the AI to hide risks or compliance issues.
- Regulations like GDPR or CCPA mean that mishandling personal data with AI could itself violate rules.

Over-Reliance on AI Itself:

- AI can efficiently and accurately crunch numbers and spot patterns, but it lacks the judgment required to weigh ethical trade-offs or anticipate rare, high-impact events that don't show up in the data.
- A company leaning too hard on AI might sleepwalk into a compliance failure because "the system didn't flag it."

Lack of Explainability:

- Regulators and auditors often want professionals to provide clear reasoning behind decisions, but many AI models are black boxes that offer little insight into why the system flagged a specific risk or recommended a certain policy tweak.
- This can make it tough to defend AI-driven decisions in an audit or courtroom environment.

Cost and Integration:

- Building and maintaining AI for GRC requires specialized talent, costly infrastructure, and constant updates.
- Smaller organizations might struggle to justify the investment. Integrating AI into legacy systems can be a headache due to compatibility issues and process overhauls, which can lead to operational disruptions if botched.

Regulatory Uncertainty:

- As AI adoption grows, regulators are still catching up, creating ambiguity around accountability and transparency requirements.
- The lack of clarity may lead to costly repercussions and may even stall innovation, as companies may hesitate to invest in AI without assurance that their practices will remain compliant as regulations evolve.

The risks associated with this technological leap forward do not negate AI's potential to augment governance, risk, and compliance through efficiency and insights, but they demand careful management—**human oversight, regular audits, and robust data practices**—to prevent amplifying existing vulnerabilities.



Governance of AI Itself

Compliance for AI itself is a key focus in 2025, especially as regulators worldwide begin to focus on reining in AI deployment across various industries. The widespread adoption of AI is driving the need to manage its risks and ethical implications. Within the broader GRC framework, ensuring AI systems comply with laws, ethical standards, and organizational policies has become a stand-alone challenge—and a critical one. While all market participants are eagerly leveraging and using AI to manage risks and compliance, *they must simultaneously ensure the AI doesn't become a risk or compliance liability itself.*

What Is AI Governance?

AI governance refers to the structures and processes enterprises and regulators use to monitor and regulate AI systems and platforms. With a goal of balancing innovation and accountability, AI regulation and governance attempt to address risks like bias, privacy violations, security threats, and lack of transparency. While still in its early days, AI governance can integrate into GRC by aligning AI-related risks with broader enterprise governance, ensuring compliance with legal and ethical standards.

Advances in AI Compliance

AI Governance Tools

- Governance tools like IBM's watsonx.governance and Credo AI now offer end-to-end monitoring of AI systems across development, deployment, and performance.
- watsonx.governance flags high-risk use cases (e.g., hiring models) for human review and bias detection.
- Credo AI's 2024 update auto-triggers compliance checks when AI use shifts (e.g., from internal to customer-facing), aligning with frameworks like NIST AI RMF and ISO 42001.

Explainable AI (XAI)

- Regulators now require transparency in AI decision-making, including compliance with GDPR and the EU AI Act.
- XAI tools like Google's Explainable AI and H2O.ai's Driverless AI offer clear explanations and visualizations of model outputs.
- These tools help organizations meet the "right to explanation" and documentation standards.

Bias Detection and Mitigation

- Bias detection tools like IBM's Fairness 360 and Microsoft's Fairlearn scan AI models for bias in training data and outputs (e.g., race, gender).
- These tools integrate with GRC workflows to support compliance, such as NYC's mandatory bias audits for hiring AI.
- Example: These tools can identify and correct a bank's loan AI flagged for rejecting minority applicants.

Real-Time Compliance Monitoring

- Platforms like OneTrust's AI Governance module monitor AI metadata in real time against CCPA, GDPR, and other standards.
- They alert GRC teams to issues like unauthorized use of personal data as models evolve post-deployment.
- This enables continuous oversight to catch and correct compliance drift.

Regulatory Mapping and Simulation

- NLP-driven tools from Thomson Reuters and MetricStream map AI use to applicable regulations.
- They simulate "what-if" compliance scenarios (e.g., EU AI Act facial recognition ban) to identify risks early.
- Helps organizations pre-empt regulatory violations before they occur.

Challenges in AI Compliance

Black Box Problem:



Even with XAI, some deep learning models resist full explainability, risking noncompliance with transparency rules. GRC teams must balance performance versus auditability.

Regulatory Fragmentation:



The EU's strict AI Act clashes with lighter U.S. approaches (e.g., voluntary NIST guidelines), complicating global compliance. AI tools must adapt to jurisdiction-specific nuances.

Accountability Gaps:



Who's liable if an AI errs—the vendor, developer, or user? The EU's AI Liability Directive (proposed 2024) aims to clarify this, but GRC teams still scramble to define ownership.

Cost and Complexity:



Smaller firms struggle to afford compliance tech or keep up with evolving rules, widening the gap with larger players.

Rise of Deepfakes:



Increasingly difficult to distinguish authentic content from maliciously manipulated material.



Governance of AI Itself (cont.)

Some of the largest players across industries have already begun implementing AI governance solutions into their platforms. Varying severity and scope of regulations across the EU and the U.S. further enhance the need for dynamic AI governance solutions that ensure compliance with ethical laws and standards.

Real World Examples Across Industries



Finance:

Post-2024, J.P. Morgan deployed AI governance tools that audit trading algorithms to ensure compliance with SEC rules and avoid repeats of past fines (e.g., a \$920 million fine in September 2020 for market manipulation and a \$350 million fine in March 2024 for trading compliance failures).



Healthcare:

The Mayo Clinic has started incorporating advanced AI tools to proactively flag compliance risks in patient-facing AI tools, ensuring adherence to HIPAA regulations and preempting the EU AI Act's scrutiny for diagnostic models.



Big Tech:

In 2024, Google rolled out AI compliance dashboards that track its Gemini models, providing proof of adherence to internal ethics codes and external regulations—a GRC necessity as scrutiny continues to mount.





Insurance:

Many insurers have begun implementing AI models that include bias detection algorithms to remain compliant with anti-discriminatory legislation, such as Colorado Senate Bill 21-169, which mandates insurers demonstrate how they are testing their AI-driven systems to prevent discriminatory outcomes.

Varying AI Regulatory Landscape

As is the case across many risk vectors, the EU is leading the way from a regulatory perspective.

- In the U.S. at the federal level, AI regulation has been characterized by voluntary guidelines, executive actions, and sector-specific rules rather than sweeping legislation.
- While the U.S. lacks a unified federal framework, with a patchwork of regulations between the federal and state levels, the EU has put in place a comprehensive, unified approach with the EU AI Act adopted in March 2024, set for full enforcement in August 2026.
- The EU AI Act demands a structured, proactive playbook—classify AI, assess risks, document everything, and certify compliance.

Aspect	 EU AI Act	 U.S. Regulations
Scope	Unified, Risk-Based, Binding	Fragmented, Voluntary, and State Laws
Risk Approach	Tiered (Banned to Minimal)	No Formal Tiers, Case-Specific
Compliance	Mandatory Assessments, Disclosure	Voluntary (Federal), Some State Mandates
Penalties	Up to €35 Million/7% Revenue	Varies by State/Agency, Up to Millions
Tone	Precautionary, Rights-Focused	Innovation-First, Reactive



Unlocking GRC With Data Analytics

Data-driven GRC enables organizations to make informed decisions, identify potential risks, and ensure adherence to regulatory requirements, shifting from legacy reactive responses to proactive, agile risk management.

GOVERNANCE:

Strategic Insight and Overview



Allows for real-time KPI tracking.



Uses historical trends to predict resource demands.



Ensures accountability with auditable, transparent decision trails.



FIs use analytics to predict capital needs based on market trends, ensuring governance aligns with shareholder goals.

RISK:

Proactive Mitigation and Resilience



Forecasts threats via predictive modeling.



Quantifies risk likelihood.



Strengthens controls by prioritizing high-impact vulnerabilities.



Pharmaceutical companies use analytics to predict potential supply chain disruptions, ensuring the continuity of drug supply.

COMPLIANCE:

Regulatory Agility and Assurance



Anticipates violations with pattern analysis.



Monitors compliance in real time across vast datasets.

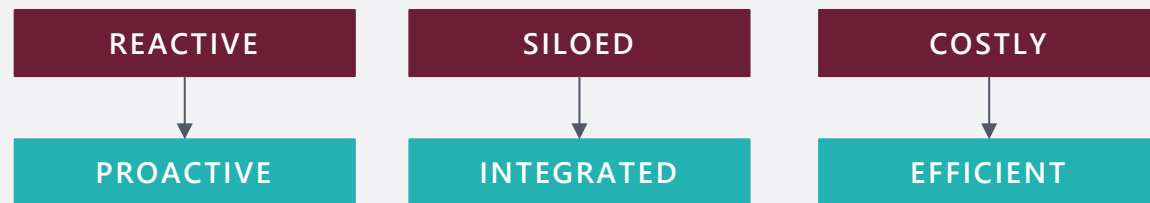


Prepares for audits with automated reporting and gap detection.



Hospitals use analytics to predict HIPAA breaches from patient data trends, ensuring compliance and avoiding fines.

Data analytics is having a transformative impact on GRC, addressing issues before they escalate, unifying GRC with a holistic data view, and reducing fines, manual effort, and resource waste.



Use of data analytics is becoming more commonplace, but most companies are still developing their approach.

78% of companies report using data analytics to manage compliance risk.

Only 9% of organizations consider themselves advanced within their compliance programs.

Companies with advanced analytics programs are **almost 2x more likely** to use analytics to perform risk-based transaction monitoring.



Cybersecurity and GRC Integration

Cybersecurity and GRC are not merely adjacent markets—they are deeply interconnected, representing two sides of the same coin that enable organizations to operate securely and resiliently in an increasingly risk-laden environment.

Overview

Cybersecurity is about protecting systems, data, and networks from attacks. GRC, meanwhile, is the broader framework: it's how a company sets rules (governance), spots and manages threats (risk), and stays legal (compliance). Where they meet is in the day-to-day operations of keeping an organization secure and accountable—cybersecurity brings the brute force of protection and response, and GRC gives it direction and an operational framework.

Cybersecurity and GRC Framework

Shared Goal

- **Cybersecurity** zeros in on digital threats like ransomware, phishing, and data breaches. It's the front line, detecting surges, such as a 400% spike in IoT attacks since 2020, and deploying tools.
- **GRC** takes a broader view, embedding cyber into a wider landscape of risk. It asks, "What's the business impact?"
- **Convergence:** Cyber flags issues like 50 cloud vulnerabilities; GRC prioritizes by fixing the 10 with GDPR implications. Together, they triage and tackle threats.

Compliance

- **Cybersecurity** handles execution—encrypting for HIPAA and stopping leaks for GDPR. It's the "how."
- **GRC** handles strategy—tracking laws, setting policies, and proving compliance. It's the "why" and "what."
- **Convergence:** In a breach, cyber isolates the threat, and GRC handles disclosure and policy updates. For GDPR, cyber encrypts, and GRC reports within 72 hours. One drops the ball, both pay.

Governance

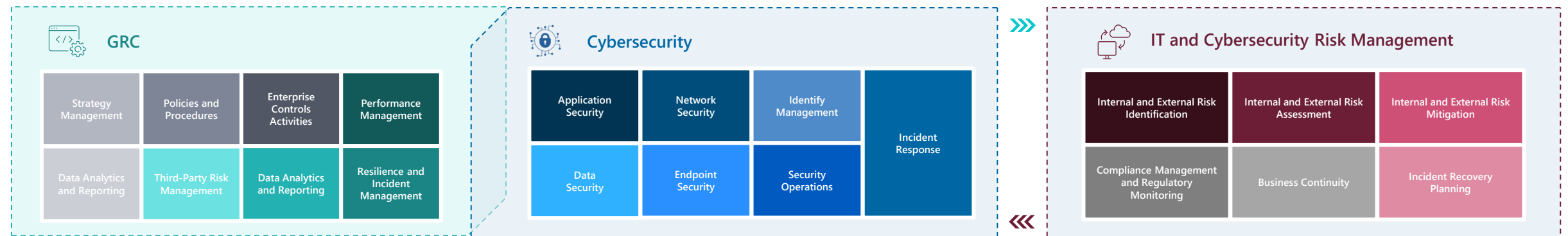
- **Cybersecurity** needs clear directives, for example – 30-day patch rules or mandatory 2FA.
- **GRC** defines the rules, aligning them to strategy, such as "We're going zero-trust" and business goals, like "Reduce risk by 20%".
- **Convergence:** Governance funds cyber ("Here's \$5 million"), cyber builds defenses, and GRC tracks ROI – breaches down 15%. It's a loop—cyber acts, and GRC audits and adjusts.

Data

- **Cybersecurity** protects it – stopping malware from exfiltrating records.
- **GRC** classifies and contextualizes it – PII, \$10 million liability if breached.
- **Convergence:** Cyber detects leaks; GRC calculates impact and updates the risk register. They co-own the data story.

Tech and Tools

- **Cybersecurity** uses SIEMs, firewalls, and threat intel.
- **GRC** uses dashboards, audit trails, and policy trackers—often with cyber data.
- **Convergence:** Cyber alerts, like DDoS attack, surface in GRC tools such as compliance gaps versus NIST 800-53. AI bridges both—cyber predicts attacks, and GRC estimates penalties.

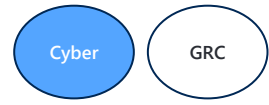




Cybersecurity and GRC Integration (cont.)

Cybersecurity defends against threats, but GRC provides the structure, priorities, and oversight to make those defenses effective. Without both, organizations manage risk with only half the picture.

CYBERSECURITY AND GRC ARE HIGHLY COMPLEMENTARY SOLUTIONS



Cybersecurity Without GRC

Disorganized and Short-Sighted

Lacks Strategic Direction

Cybersecurity teams can identify and patch hundreds of vulnerabilities, but without GRC to assess business impact and regulatory exposure, prioritization is arbitrary. For example, GRC may highlight that failing to patch 10 specific issues could trigger a \$20 million GDPR penalty.

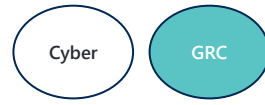
Lacks Documentation and Accountability

Cyber may contain an incident, but without GRC, there's no formal disclosure or audit trail. In the SolarWinds case, failure to document and report the 2020 breach led to an SEC lawsuit in 2023.

Lacks Long-Term Perspective

Cybersecurity is often reactive, focused on immediate threats. GRC provides the strategic roadmap—tying risk mitigation efforts to business goals and compliance obligations.

Example: A hospital neutralizes a cyberattack but fails to report the breach within HIPAA's 60-day window. The result: a \$1 million regulatory fine. Cybersecurity won the battle, but without GRC, the organization lost the war.



GRC Without Cybersecurity

Ineffective and Exposed

No Real-Time Data

GRC depends on threat intelligence from cybersecurity tools – SIEM logs, incident data. Without it, risk assessments are incomplete and often inaccurate.

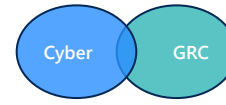
No Technical Execution

GRC defines policies, but enforcement relies on cybersecurity. A policy mandating data encryption is meaningless without the infrastructure behind it.

No Defense in Practice

An organization may appear compliant on paper but still be vulnerable. In Uber's 2016 breach, sensitive data from 57 million users was exposed despite documented policies—proof that compliance alone is not protection.

Example: A bank successfully passes SOX audits but lacks endpoint protection. A ransomware attack cripples operations and costs \$10 million. Compliance frameworks alone couldn't prevent the breach.



Cybersecurity With GRC

Risk Management Force Multiplier

Enhanced Precision

Cybersecurity detects specific threats—like a surge in phishing attacks—while GRC ties these signals to relevant controls, such as PCI-DSS, allocating resources efficiently and effectively.

Regulatory Alignment

Cybersecurity teams respond to incidents; GRC ensures timely disclosure and documentation – GDPR's 72-hour breach notification – reducing penalties and preserving trust.

Strategic Execution

GRC defines long-term risk frameworks (e.g., zero-trust architecture); cybersecurity implements them. According to Gartner (2024), organizations that do this well report up to 40% fewer incidents.

Case: After Sunburst, SolarWinds fused CrowdStrike (Cybersecurity) with ServiceNow GRC, and breach risks dropped 40%, taking the SEC off their backs. Alone, neither cuts it.

EQUIFAX® 2017 DATA BREACH

In 2017, Equifax, one of the largest credit reporting agencies in the U.S., experienced a massive data breach that exposed sensitive personal information of approximately 147.9 million Americans, 15.2 million British citizens, and about 19,000 Canadians. The breach occurred between mid-May and July 2017 but was not publicly disclosed until September 7, 2017.

Key Facts

Cause of Data Breach

Attackers exploited a known vulnerability (CVE-2017-5638) in the Apache Struts web application framework used by Equifax.

Data Compromised

The breach exposed names, Social Security numbers, birth dates, addresses, driver's license numbers, and, in some cases, credit card numbers.

Security Failures

Equifax's failure to maintain an accurate IT asset inventory and to renew an expired SSL certificate hindered its ability to detect and respond to the breach effectively.

Impact

Financial Consequences

Equifax agreed to a global settlement of up to \$700 million with the FTC, the Consumer Financial Protection Bureau, and 50 U.S. states and territories. This included up to \$425 million to help people affected by the data breach.

Reputational Damage and Regulatory Scrutiny

The breach severely damaged Equifax's reputation, leading to the resignation of key executives, including the CEO. The incident also prompted increased regulatory scrutiny of data security practices, not only for Equifax but also for other credit reporting agencies.



The Enduring Relevance of EHS in an Evolving Risk Landscape

From frontline safety to enterprise risk, EHS continues to anchor compliance strategies across high-risk and highly regulated sectors.

ENVIRONMENTAL:

Inconsistent Data and Reporting Leading to Regulatory and Legal Risk

> 70%

Of Institutional investors now incorporate environmental data into decisions...

30%

But a Minority trust companies' self-reported data.

80%

Increase in ESG greenwashing lawsuits in 2024, largely driven by false emissions or recycling claims.

Key Takeaways



Stakeholders are demanding more **transparency—tracking, managing, and reporting—into companies' air emissions, water quality, and waste compliance detail.**



Overabundance of environmental data without validation is creating reporting noise and inaccuracy.



Imperative for companies to **go beyond environmental data reporting** for compliance purposes, but also to view it as critical to **overall strategic initiatives.**



Increased regulatory mandates are creating the need for a **traceable system of record.**

HEALTH:

Rising Costs and Burnout Demand Urgent Employee Health Investments

~2.7M

Employees in the U.K. had work-related health issues in 2022/2023.

~20%

Of workers experience mental health issues annually.

43%

Of workers lack the mental health strategies to combat such issues.



Investing in health yields **measurable financial and productivity returns.**



Holistic health programs reduce injury risk and boost workforce resilience.



Centralized health data **eliminates reporting gaps.**



Studies have reported that **wearable devices** can help **reduce injury rates** and boost productivity.

SAFETY:

Workplace Safety Is a Critical Element Directly Impacting Financial and Operational Performance

\$167B

Annual Cost of U.S. job injuries.

~\$1.5M

Annual Cost per workplace fatality.

\$43K

Annual Cost per medically consulted injury.

~\$1.1K

Annual Cost of preventable workplace injuries.



Increased use of subcontractors is leading to an **increased need for comprehensive employee management.**



Poor safety performance leads to **bottom line erosion, not just insurance claims.**



Data overloads are **undermining workplace safety management.**



Digitization and analytics are **enabling proactive risk mitigation and workforce protection.**

The ESG Software Market in 2025: Growth, Headwinds, and Longevity

Despite current headwinds, ESG and sustainability are here to stay, driven by the entrenched drivers of global regulations, continued corporate and investor commitment, and general alignment with sound business strategy.

Current ESG Market Headwinds



- a) U.S. exits Paris Climate Accord and UN Framework Convention on Climate Change.
- b) Revokes Biden-era ESG executive orders, including the U.S. International Climate Finance Plan.
- c) Suspends select Inflation Reduction Act and Infrastructure Investments and Jobs Act disbursements.
- d) Executive order targeting state ESG initiatives and directing the U.S. Attorney General to take appropriate action to stop their enforcement.
- e) Declared a national energy emergency: halting offshore wind leases, opening Alaska to oil, gas, and LNG.



- a) The February 2025 Omnibus package reduces CSRD reporting scope and eases the CSDDD, potentially decreasing demand for ESG software.
- The new CSRD scope includes:**
1. Delayed reporting timelines.
 2. Fewer companies and up to 70% fewer data points.
 3. Simplified assessments focusing on materiality-based disclosures.
- The new CSDDD encompasses:**
1. One-year delay to 2028.
 2. Scope reduction to Tier 1 suppliers only.
 3. Reduced reporting to every five years.
 4. Liability removal and proportional penalties.



- a) U.S.-based corporations are reducing, pushing back, or eliminating ESG programs, practices, or language in corporate materials.
- Examples include:**
1. Companies from IBM to Victoria's Secret, reassessing their supplier diversity initiatives.
 2. Many companies, such as Warner Bros. Discovery, Major League Baseball, and UnitedHealth Group, are removing all references to DEI and diversity in corporate materials.
 3. Companies such as Bank of America and Paramount are ending targets for diversity hiring.



Despite Current Headwinds, ESG and Sustainability Are Here to Stay:

- **Private Sector Commitment**
- **Embedded Global Regulatory Foundation**
 - i. EU Leadership: Despite simplification under the Omnibus Bill, regulations such as SFDR, deforestation rules, and CSDDD keep ESG reporting demand strong.
 - ii. Asia-Pacific Growth: ESG disclosure mandates expand in Japan, Singapore, and India (e.g., India's BRSR).
 - iii. U.S. State-Level Resilience: California and New York sustain ESG progress with carbon reporting and data accountability laws.
- **Strategic and Financial Incentives**
 - i. Corporate sustainability initiatives are not slowing down. Companies of all sizes continue to focus on their sustainability commitments to drive real business value.

Business Value Available From Climate and Decarbonization Efforts

Revenue Growth	Increased Price Premium	Increased Market Share	New Revenue Streams to Meet Customer Demand
Cost Reduction	Lower Energy Use	Less Waste Generation	Lower Raw Material Costs via Circularity
Risk Reduction	Higher Energy Resilience	Stronger Brand Resilience	Lower Long-Term Costs for Climate Mitigation and Adaptation

37%

Of companies are increasing their climate ambitions, while 16% are decelerating their goals.

84%

Of companies studied are standing by their climate commitments.

80%

Of companies studied are demonstrating moderate to leading levels of governance maturity.

02.

Significant Investment Occurring Throughout the GRC Value Chain

Key Investment Trends Across Subsectors (Pages 31–50)



Key Subsector Trends:

Third-Party Risk Management

Third-Party Risk Management Highlights

Increasing Dependency on Third Parties

Modern organizations are more dependent than ever on third-party vendors for business-critical services, and supply chains are more complex than ever. Change is the only constant.

Increased Incidents Related to Vendors

Third-party vendors create unwanted exposure, causing greater disruption as the risks they bear are not being properly managed. According to the *Global Cybersecurity Outlook 2024* report by the World Economic Forum, 98% of organizations report having at least one third-party partner that has suffered a data breach in the past two years.

Real Economic Impact

Supply chain disruptions, third-party breaches, and noncompliant vendors and contractors have been and will remain destructive to business activity. Trillions of dollars in revenue per year are lost due to supply chain disruptions and third-party incidents.

Regulatory Scrutiny

Regulators are focused on growing third-party risks and applying more pressure to enterprises to better manage these risks. Regulations such as GDPR, HIPAA, CCPA, and other data protection schemes have high penalties for noncompliance and can be easily triggered in third-party incidents.

















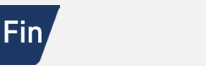
Pressures From Economic Volatility

Economic conditions mean tighter margins for suppliers and an increased risk of supplier disruption.



Top Recent Third-Party Risk Management Deals⁽¹⁾

(\$ in Millions)

Date	Company	Selected Investor(s)	Deal Type	Enterprise Value
Jan-25	 GRMS Global Risk Management Solutions	 Achilles	Buyout	--
Nov-24	 VISO TRUST	 BainCapital VENTURES	Capital Raise	\$7
Nov-24	 Prevalent™	 MITRATECH	Buyout	--
Aug-24	 veriforce	 Apax	Buyout	~\$33
Aug-24	 GoSupply	 Achilles	Buyout	--
Aug-24	 venminder	 CONTRACTS	Buyout	--
Aug-24	 CTAIMA	 Hg	Buyout	--
Apr-24	 nalanda	 ONCE FOR ALL	Buyout	\$373
Apr-24	 Avetta	 IEQT	Buyout	\$3,000
Jan-24	 SAYARI	 TPG	Capital Raise	\$235
Dec-23	 EXIGER	 CARLYLE / INSIGHT PARTNERS	Buyout	1,200
Sep-23	 certa	 Fin	Capital Raise	\$35



What We're Reading:

Third-Party Risk Management (cont.)

Third-party risk management has become essential as organizations are increasingly exposed to escalating cybersecurity, operational, and compliance risks.



The 2024 Third-Party Risk Management Study

Overview

The report highlights that organizations continue to struggle with effectively managing third-party risk due to outdated, manual processes and limited visibility across their vendor ecosystems. It discusses how many companies assess only a portion of their third-party relationships, leaving significant blind spots that can lead to operational, security, and compliance vulnerabilities.

Key Findings

The value of third-party risk management begins with identifying risks and extends to managing the lifecycle of the relationship between an organization and its vendors.

01	02	03	04	05	06	07
Sourcing and Selection	Intake and Onboarding	Inherent Risk Scoring	Internal Controls Assessment	External Risk Monitoring	Offboarding and Termination	SLA and Performance Management

Third-Party Risk Management Drivers

Several regulatory and compliance requirements mandate the management of third-party risk and can provide an effective framework for mitigating risk. Companies use these frameworks to implement third-party risk programs, which are driven by the following:



Compliance With Regulatory Requirements



Competitive Advantages of an Effective TPRM Program



Managing Internal Financial and Operational Risk



Cybersecurity Risk



Internal Purchasing/Efficiency Drivers



Meeting Customer Requirements



Streamlining Third-Party Risk Management: The Top Findings From the 2024 Benchmark Survey Report

Overview

The report emphasizes the growing reliance on third parties as organizations become more reliant on external vendors, highlighting the potential risk. It illustrates that many companies still lack the necessary integration between their GRC systems and vendor risk management processes, resulting in limited visibility and delayed responses to external threats.

Key Findings

- 1 **Complex third-party incidents are on the rise and are becoming increasingly difficult to manage.**

62%

Of companies

report experiencing a supply chain disruption related to cybersecurity, a 13% year-over-year increase.

89%

Of companies

report experiencing or expect an audit finding related to third-party risk mgmt. that they cannot resolve promptly.

- 2 **While compliance violations are on the decline thanks to the broader adoption of risk and compliance software, significant growth potential remains.**

42%

Reduction

in compliance violations related to third-party risks, but data or privacy breaches caused by third-party vendors have increased by 22%.

85%

Of companies

report using a platform to manage compliance, only 25% leverage third-party modules within their GRC platforms.



What We're Reading:

Third-Party Risk Management (cont.)

Within third-party risk management, supply chain is one of the largest areas where comprehensive tools are needed to identify, mitigate, and combat risks.



- i. Global Supply Chains See Nearly 40% Annual Increase in Disruptions
- ii. Top Five Supply Chain Disruptions of 2024

Overview

Resilinc's reports highlight the heightened disruptions across supply chains, primarily driven by factory fires, labor disruptions, business sales, leadership transitions, and M&A activity. The report discusses how companies are responding in kind, by investing in AI, diversifying strategies, and accelerating nearshoring and reshoring efforts.

To strengthen resiliency, companies invested significant resources in AI, made strides to reduce dependency on single sourcing, and prioritized nearshoring. On the other hand, economic instability, climate change, geopolitical disruption, and bad actors continue to test supply chain resilience.

Key Statistics



38%

Global supply chain disruptions rose by 38% in 2024.



214%

Flood-related alerts surged by 214%, forest fires by 88% and hurricanes by 101%.



33%

Cyberattacks on supply chains rose by 33%.



47%

Labor disruptions experienced a 47% year-over-year increase, encompassing strikes, layoffs, and protests.

EXIGER

- i. Supply Chain Risk Management
- ii. Building Security and Resilience: Supply Chain Risk Management for Critical Infrastructure

Overview

Exiger's reports underscore its ability to leverage AI and real-time analytics to gain deeper visibility into supplier networks, uncover hidden vulnerabilities, and enhance resilience against disruptions, while also highlighting the need for robust supply chain risk management strategies to protect critical infrastructure sectors across the globe.

Key Findings

Systemic Risk in Interconnected Sectors

Critical infrastructure sectors are highly dependent, emphasizing the need for comprehensive risk identification and mitigation strategies.

Adoption of Advanced Technologies

Implementing AI-driven platforms provides organizations with the necessary tools to achieve granular visibility into supply chains.

Public-Private Collaboration

Effective risk management in critical infrastructure requires robust collaboration between government entities and private industry, enhancing the collective ability to respond and mitigate supply chain risk.

Key Statistics

83%

Of organizations

report experiencing raw material shortages in 2024, highlighting the need for improved supply chain resilience.

55%

Of companies

report lacking visibility into their supply chains.

67%

Of companies

have implemented digital dashboards for visibility.



Key Subsector Trends:

Audit and Risk Management

Audit and Risk Management Highlights

AI Powered Platforms

AI is revolutionizing GRC with every platform integrating and utilizing next-generation AI to automate audits, data collection, and assessments, track regulatory changes and power fraud detection, third-party risk management, and incident response.

Adoption of Agile No Code

True low-code/no-code GRC and audit management applications are continuing to take market share by offering highly configurable and adaptable solutions that can quickly meet an organization's needs.

Convergence of Functions



GRC and audit management providers of all sizes are expanding beyond their core functionality and adding additional GRC functionality to broaden their coverage of risk vectors.

Continuous Auditing and Monitoring

Enterprises solely relying on annual audits to ensure compliance are a thing of the past. Today's risk-aware enterprises are utilizing continuous auditing and monitoring of controls, data, and regulatory mapping to augment annual tests.

Top Recent Audit and Risk Management Deals⁽¹⁾

(\$ in Millions)

Date	Company	Selected Investor(s)	Deal Type	Enterprise Value
Apr-25	 anecdotes	DTCP	Capital Raise	\$55
Mar-25	 PROTECHT	PSG	Buyout	\$280
Jun-24	Camms.	 riskconnect.	Buyout	\$150
May-24	 AUDITBOARD	Hg	Buyout	3,000
Apr-24	 SPRINTO	Accel	Capital Raise	\$20
Apr-24	 Scrut Automation	MassMutual Ventures	Capital Raise	\$10
Feb-24	 COMPLIANCE.AI	ARCHER	Buyout	--
Aug-23	 hyperproof	RIVERWOOD CAPITAL	Capital Raise	\$40
May-23	Onspring	CAPITAL IP	Capital Raise	--



What We're Reading:

Audit and Risk Management (cont.)

In a complex and rapidly shifting regulatory environment, compliance automation is essential for reducing manual effort, minimizing risk, and ensuring consistent, real-time adherence to evolving requirements at scale.

Thoropass™

What to Look for in Automated Regulatory Compliance Software in 2025

Overview

This report emphasizes the benefits of automated regulatory compliance software, including its ability to streamline key processes, minimize manual effort, and improve operational efficiency while supporting regulatory adherence. The report also highlights core features of effective automation tools, such as workflow automation, continuous monitoring, and seamless integration with existing systems.

Key Findings



Real-Time Monitoring

Continuous real-time monitoring enables early detection of security threats, service disruptions, and compliance gaps, allowing teams to quickly mitigate risk.



Audit Management

Effective compliance software streamlines audit workflows and centralizes documentation, providing a single source of truth for all compliance-related materials. By automating key stages of the audit process, compliance solutions reduce manual effort and help ensure regulatory obligations are consistently met.



Advanced AI for Predictive Compliance

Advanced AI capabilities in compliance software can automate data collection and analysis, enhance risk assessment processes, and help predict potential compliance issues.



Adaptation to Remote Work Environments

The shift to remote work has introduced increasing challenges. Remote auditing practices and enhanced digital communication tools are only two of the dynamic strategies being implemented by companies to ensure compliance.

AUDITBOARD

Emerging Trends in Governance, Risk, and Compliance

Overview

This report offers a comprehensive analysis of how technological advancements and evolving regulatory landscapes are reshaping GRC practices. The report emphasizes the transformative role of AI in enhancing compliance efficiency, with many organizations integrating AI and machine learning to perform continuous regulatory compliance checks. This shift towards automation enables real-time monitoring and proactive risk management, reducing reliance on manual processes.

Key Findings

AI Integration

Organizations are increasingly adopting AI and machine learning to perform continuous regulatory compliance checks, moving away from traditional periodic assessments.

Data-Driven Compliance

The shift toward data-driven compliance is identified as a new foundation in GRC, enabling organizations to make informed decisions and maintain regulatory adherence.

Key Statistics



50%

Of major enterprises will use AI and machine learning to perform continuous regulatory compliance checks.



62%

Of organizations have reported that AI has significantly improved the efficiency of compliance procedures.



Key Subsector Trends:

Business Continuity Management

Business Continuity Management Highlights

Integration of AI and ML

As with other disciplines in the risk management and cyber ecosystems, AI and ML present immense opportunities for business continuity. AI and ML are being utilized to accelerate and automate historically burdensome data collection, data analysis, and workflow, while also driving predictive analytics to determine possible business discontinuity.

From Business Continuity to Operational Resilience

Since operational downtime is no longer an “if” but a “when,” business continuity is expanding its purview and reach by integrating with and incorporating broader risk management and disaster recovery.

Third-Party Risk and Supply Chain Risk Management

As third-party relationships proliferate and supply chains grow increasingly complex, BCM solutions are integrating with or expanding into vendor risk management. Many enterprises must now continuously monitor third-party suppliers to ensure resilience and continuity.

















Hybrid Work Is Here to Stay

Business continuity technology and planning will increase in importance as hybrid work remains in place, forcing many enterprises to configure business continuity plans for this new reality.



Top Recent Business Continuity Management Deals⁽¹⁾

(\$ in Millions)

Date	Company	Selected Investor(s)	Deal Type	Enterprise Value
Mar-25	 IPeople Healthcare	 RLDatix	Buyout	--
Dec-24	 COMPLYUP	 EXOSTAR®	Buyout	--
Nov-24	 CYERA	 SAPPHIRE VENTURES	Capital Raise	\$300
Oct-24	 Preparis	 MITRATECH	Buyout	--
Sep-24	 Axcient	 CONNECTWISE	Buyout	\$450
Jul-24	 infiniteblue	 everbridge™	Buyout	--
Jul-24	 naggin <small>a Motorola Solutions Company</small>	 MOTOROLA SOLUTIONS	Buyout	--
Jul-24	 everbridge™	 THOMABRAVO	Buyout	\$1,800



What We're Reading:

Business Continuity Management (cont.)

In today's evolving risk landscape, business continuity management is key to minimizing disruptions, protecting revenue, and ensuring resilience.

The Hacker News

Future-Proofing Business Continuity: BCDR Trends and Challenges for 2025

Overview

This report highlights the growing complexity of IT environments and those environments corresponding data protection challenges. As data becomes more dispersed across multiple platforms and locations, organizations face a widening attack surface while also contending with the rising costs and intricacies of business continuity. The report, based on insights from more than 3,000 global IT professionals, reveals a decline in confidence in current backup systems and a disconnect between recovery expectations and actual capabilities.

Key Findings



Disaster Recovery Increasing in Importance as Complexities Rise

Data backup and recovery should be a safety net for businesses, but for many, it has become a source of complexity and risk.



Lack of Confidence in Backup Systems

Trust in backup solutions is slipping, leaving many businesses questioning whether they can reliably recover from data loss.



Backup Management Is a Major Burden

Managing backups drains IT resources. As data volumes grow, IT teams are spending more time than ever maintaining backup systems, testing recovery processes, and troubleshooting failures.



Backups Are Continuously Exposed Due to Security Gaps

While backups are supposed to be the last line of defense against cyber and other threats, many contain serious security flaws that put data at risk.

Key Statistics

40%

Of IT teams feel confident in their backup systems.

~23%

Of businesses spend more than three hours per week on backups.

~30%

Worry their backup strategy is inadequate.

~35%+

Of organizations wouldn't even know if backups are skipped or missed.

50%+

Of organizations plan to switch backup providers.

~25%

Of workloads lack policies that limit unauthorized access to backups.

10+

Hours spent per week managing backups.

33%

Of businesses use dedicated password managers.



Key Subsector Trends:

IT and Cybersecurity Risk Management

IT and Cybersecurity Risk Management Highlights

Increasing Cyberattacks

With enterprises' attack surface expanding and cybercriminals becoming increasingly sophisticated, cyberattacks will only continue to increase in frequency and complexity. Additionally, costs associated with those attacks will continue to accelerate as attackers are focused on higher-value, targeted attacks.

Increasing Regulations Amid Focus on Data Privacy

Stricter global regulations will push organizations of all sizes to adopt more robust risk management frameworks. Europe is leading the way with the passage of the Digital Operational Resilience Act (DORA) and the NIS2 Directive (EU 2022/2555). Emerging regulations like the EU's AI Act and NIST framework will also require comprehensive cyber risk management strategies.

Advent of Artificial Intelligence

AI has the ability to be a force for both good and evil in cyber risk management, offering the promise of improved threat identification, automated data collection, data analysis, and operational workflows, while also providing cyberattackers with the same capabilities.

Talent Gap Persists

Just as attacks increase in strength and frequency, the cyber talent shortage continues to accelerate. Recent studies suggest a critical global cybersecurity workforce shortage of 2.8 million professionals.

Top Recent IT and Cybersecurity Risk Management Deals⁽¹⁾

(\$ in Millions)

Date	Company	Selected Investor(s)	Deal Type	Enterprise Value
Apr-25	anecdotes	DTCP	Capital Raise	\$55
Mar-25	HITRUST	BRIGHTON PARK CAPITAL	Buyout	--
Feb-25	SAFEBASE	DRATA	Buyout	--
Feb-25	VULCAN	tenable	Buyout	\$150
Dec-24	cybersixgill	BITSIGHT	Buyout	--
Dec-24	Recorded Future®	mastercard	Buyout	\$2,650
Sep-24	CYBER OWL	DNV	Buyout	--
Jul-24	Vanta	SEQUOIA	Capital Raise	\$150
Jun-24	DPOrganizer	DataGuard	Buyout	--
May-24	oak9	DRATA	Buyout	--
Apr-24	Harmonize	DRATA	Buyout	--
Apr-24	FASTPATH	Delinea	Buyout	--



What We're Reading:

IT and Cybersecurity Risk Management (cont.)

Cyber risk management protects organizational integrity, enhances data privacy, ensures regulatory compliance, and reduces financial and reputational exposure.



How Third Parties Became the Biggest Cyber Threat in 2024

Overview

Black Kite's report offers insight into the evolving cybersecurity landscape, highlighting how third-party vendors have increasingly become the entry point for cyberattacks. The report details how ransomware, credential misuse, and unpatched software vulnerabilities—including zero-day exploits—have severely impacted sectors such as healthcare, finance, and manufacturing, resulting in widespread disruptions and diminished trust. It also highlights key incidents from 2024 that underscore the growing urgency of third-party risk management.

Notable Cybersecurity Incidents in 2024

cencora

Cencora, a prominent pharmaceutical distributor, faced a significant cyberattack that disrupted operations and exposed sensitive patient information.



The company allegedly paid a \$75 million ransom payment, the largest on record, to recover encrypted data and ensure the attackers did not release the exfiltrated information.



WHY THIS MATTERS

This breach highlights the importance of robust cyber risk management, particularly in sectors that handle sensitive data. This incident is a reminder of how integrated systems can amplify attacks if breached.

Key Statistics

~52%

Of the breaches were attributed to unauthorized network access through third-party connections.

CROWDSTRIKE

CrowdStrike experienced a significant services outage caused by a faulty software update to its critical endpoint tool.



The estimated financial impact of the outage was more than \$5 billion and resulted in widespread system crashes on ~8.5 million devices globally.



While not an explicit cyberattack, this incident highlights how integral IT supply chains are and the need for fallback mechanisms for critical IT updates.

~67%

Of known attacks involved ransomware, highlighting the growing sophistication of cybercriminal tactics.

snowflake

Snowflake experienced a series of data breaches caused by unauthorized network access, which affected its clients and their downstream ecosystems.



Clients felt the brunt of the impact, with AT&T reporting exposed call logs of more than 109 million users, Ticketmaster facing significant disruptions to operations, and Santander Bank having to mitigate fraud and identify theft across the bank.



This breach highlights the increased risk of cloud-based ecosystems. Organizations that rely on third-party ecosystems cannot rely on any number of outside organizations but must deploy stringent security practices.

38%

Year-over-year increase in common vulnerabilities and exposures disclosed in 2024.

Key Subsector Trends:

Environmental, Social, and Governance

Environmental, Social, and Governance Highlights

Regulatory Divergence

While the U.S. will see reduced federal ESG focus under the Trump administration, the EU and U.S. state governments will continue to lead the focus on ESG compliance. Despite recent headwinds, ESG regulatory pressure will remain and drive market growth. Global companies must still comply with ESG regulations despite U.S. deregulation efforts.

Integration of ESG Into Core Business Strategy

ESG is shifting away from a compliance checkbox exercise to a critical component of core business strategy that will drive long-term value; ESG compliance is not only right but is also good for business.

ESG Reporting Software Adoption Will Continue

Lagging ESG reporting software adoption will accelerate and outpace industry growth as regulatory pressure and stakeholder scrutiny will continue. Investors, customers, and other stakeholders are increasingly demanding auditable and transparent ESG data.

ESG Is Now Embedded Into Other Risk Management Specialties

ESG, or sustainability, is now a key component of a broader view of risk as seen in the integration into supply chain risk management, vendor risk management, and product compliance tools.



Top Recent Environmental, Social, and Governance Deals⁽¹⁾

(\$ in Millions)

Date	Company	Selected Investor(s)	Deal Type	Enterprise Value
Feb-25	envirosuite	Ideagen	Buyout	\$144
Dec-24	GRMS	Achilles	Buyout	--
Dec-24	Daato	EQS	Buyout	--
Oct-24	Prescinto an IBM Company	IBM	Buyout	--
Oct-24	Shuttle	Sagard New Gen	Buyout	--
Aug-24	amcs	IEQT	Buyout	--
Jul-24	SUSTAIN @ LIFE	workiva	Buyout	~\$98
Apr-24	GRESB	GENERAL ATLANTIC	Buyout	--
Jan-24	Watershed	GREENOAKS CAPITAL PARTNERS	Capital Raise	~\$100
Jan-24	SUPPLYSHIFT	sphera	Buyout	--



What We're Reading:

Environmental, Social, and Governance (cont.)

ESG is evolving from broad commitments to enforceable standards, with ever-changing regulatory mandates, AI-driven reporting, and investor demand for reporting on financial impact.

S&P Global

Top 10 Sustainability Trends to Watch in 2025

Overview

The report identifies 10 key sustainability trends poised to influence global business strategies. These trends emerge amid a backdrop of geopolitical shifts, evolving energy policies, and heightened scrutiny of climate-related risks. The report underscores the necessity for organizations to adapt proactively to these dynamics to maintain resilience and competitiveness.

Top Trends to Watch in 2025 From S&P Global

- | | | | |
|---|--|----|--|
| 1 | Geopolitical Shifts and Policy Uncertainty | 6 | Nature and Biodiversity Considerations |
| 2 | Energy Transition Dynamics | 7 | Supply Chain Resilience |
| 3 | Escalating Physical Climate Risks | 8 | Just and Equitable Transition |
| 4 | Climate Finance and Investment | 9 | Artificial Intelligence Integration |
| 5 | Carbon Market Evolution | 10 | Advancements in Sustainability Reporting |

novisto

Top Five ESG Trends to Watch in 2025

Overview

The report argues that, in 2025, businesses are expected to face heightened scrutiny and evolving expectations in the ESG landscape. Key drivers include stricter regulations, increased stakeholder demands, and the necessity for transparent and accountable sustainability practices. Companies will need to adapt by enhancing their ESG strategies, investing in robust data management tools, and comprehensively addressing environmental and social challenges.

Top Trends to Watch in 2025 From Novisto

Greenwashing Crackdown

Regulators are tightening rules to combat false environmental claims, with new laws across the EU, the U.K., and Canada.

Focus on the 'S' in ESG

Social issues like equality and human rights are becoming more central to corporate ESG efforts.

Rise of ESG Software

Companies are rapidly adopting ESG platforms to meet growing data and disclosure demands.

Biodiversity Takes Center Stage

New standards are pressuring firms to measure and disclose their impact on nature and ecosystems.

Supply Chain Transparency

Laws are forcing companies to assess and report on environmental and labor practices throughout their supply chains.

 Wolters Kluwer

Ten Predictions for ESG and Sustainability in 2025 and Beyond

Overview

The report outlines key trends anticipated to shape ESG and sustainability practices in 2025 and beyond. It emphasizes the growing complexity of ESG regulations, the necessity for robust data management, and the strategic integration of ESG considerations into corporate operations.

Top Predictions for 2025 From Wolters Kluwer

- | | | | |
|---|---|----|--|
| 1 | Stricter ESG Regulations | 6 | Advancements in ESG Technology |
| 2 | Reevaluation of Product Claims | 7 | Enhanced Stakeholder Engagement |
| 3 | Increased Demand for ESG Assurance Experts | 8 | Focus on Supply Chain Sustainability |
| 4 | Growth in Nature-Based Financing | 9 | Adoption of Standardized ESG Metrics |
| 5 | Integration of ESG Into Financial Decisions | 10 | Emphasis on ESG Education and Training |



What We're Reading:

Environmental, Social, and Governance (cont.)

ESG is evolving from broad commitments to enforceable standards, with ever-changing regulatory mandates, AI-driven reporting, and investor demand for reporting on financial impact.



ESG in 2025: Significant Adaptation in Sustainability Emerges as Business-as-Usual

Overview

The article offers a forward-looking analysis of how ESG practices are expected to evolve in 2025. It aims to guide corporate leaders in adapting to the shifting ESG landscape, emphasizing the integration of sustainability into core business strategies and the increasing importance of corporate governance.

Key Predictions for 2025

The Term ESG Fades, Even as Material Risks, Opportunities, and Impact Endure

While the term "ESG" may become less prominent, the underlying principles of identifying and managing material risks and opportunities remain crucial. Companies are expected to embed these pillars into their strategies.

Corporate Governance Is More Critical in 2025

Increased global uncertainties and regulatory pressures underscore the necessity for robust corporate governance. Effective governance structures are vital for navigating complex ESG challenges and ensuring accountability.

ESG Integration Into Core Business Strategy Goes Mainstream (Finally)

ESG considerations are anticipated to become integral to business operations, driven by regulatory requirements like the EU's CSRD. This integration will influence product design, procurement, and decision-making processes.

Reverse of Federal ESG-Related Regulations and Rules Accelerates, Leaving Gaps

In the aftermath of the 2024 U.S. presidential election, anti-ESG rulemaking and legislation at the federal level in the U.S. will expand while pro-ESG activity will stall. The report sees ESG transparency in doubt more than ever before.

Growth in Greenwashing Litigation and Industry Collaboration Continues

There is a growing trend toward industry-wide collaboration to address ESG issues, promoting shared standards and practices that enhance sustainability outcomes across sectors.



Sustainability and Climate Trends to Watch for 2025: Key Insights for the Year Ahead

Overview

The report aims to equip investors and business leaders with insights into emerging ESG risks and opportunities. It emphasizes the integration of sustainability considerations into investment strategies, highlighting how factors like climate change, technological advancements, and evolving governance practices are reshaping capital markets.

Key Trends to Watch for 2025

The Climate Reality Check

Climate risk is intensifying, with insured natural catastrophe losses hitting \$95 billion in 2023, pushing investors to prioritize climate adaptation and resilience.

Social Risk in the Age of Tech Giants

Tech companies now make up nearly 30% of global equity indices, putting social issues like labor rights and data ethics at the forefront of ESG scrutiny.

The AI Data Dilemma

AI is transforming ESG analysis, but with only 41% of ESG disclosures being machine-readable, data quality remains a major constraint on effective AI adoption.

A Shareholder Governance Power Shift

Shareholder governance is gaining power, as more than 90% of U.S. shareholder proposals in 2024 demanded stronger board accountability, especially around ESG topics.

Carbon Markets at a Crossroads

Carbon markets are evolving, with voluntary markets shrinking by 60% in 2023 while compliance markets expand under stricter regulations like the EU's Carbon Border Adjustment Mechanism.

Private Capital's Decarbonization Role

Private capital is under pressure to decarbonize, particularly as private equity-backed firms contribute 8% of global emissions, yet most still lack Scope 3 disclosures.



Key Subsector Trends:

Compliance and Ethics Management

Compliance and Ethics Management Highlights

Promise of AI

AI tools are already being put to work across the ethics and compliance ecosystem, with tangible benefits being realized. Materially faster and predictive data analytics, previously impossible pattern recognition, and automation of compliance workflows are just a few examples of the promise of AI.

Perils of AI

For all its promise, the increasing usage of AI has the ability to open organizations to additional regulatory, legal, and reputational risks. Enterprise compliance teams must monitor internal risks, such as AI bias and improper use of confidential information, and external risks, like working with third-party vendors with weak data security and unethical use of AI.

Whistleblower Protections Grow

Recently, regulatory authorities have intensified their focus on corporate whistleblowing as a necessary tool for identifying and addressing corporate misconduct. Companies are expected to have and maintain effective means for confidential reporting of internal and external misconduct.

Increasing Importance of Cybersecurity Compliance

Even the most robust cybersecurity platforms can be breached due to insider threats, both intentional and unintentional. Most data breaches begin with phishing. Nearly 98% of cyberattacks rely on social engineering. Employees must be trained and undergo security awareness training.

Top Recent Compliance and Ethics Management Deals⁽¹⁾

(\$ in Millions)

Date	Company	Selected Investor(s)	Deal Type	Enterprise Value
May-25	 Vault	 Diligent	Buyout	--
Apr-25	 Ardent Sky	 Vector Solutions	Buyout	--
Mar-25	 complatric	 NTRACTS	Buyout	--
Feb-25	 SPARK COMPLIANCE a Diligent brand	 Diligent	Buyout	--
Dec-24	 Daato	 EQS	Buyout	--
Dec-24	 convercent	 EQS	Buyout	--
Oct-24	 Aer Compliance	 STAR COMPLIANCE	Buyout	--
Jul-24	 ENGORE COMPLIANCE	 ACA	Buyout	--
Feb-24	 COMPLIANCE.AI	 ARCHER	Buyout	--
Oct-23	 GAN INTEGRITY	 Apax	Capital Raise	--
May-23	 Paragon DATA LABS	 INTAPP	Buyout	~\$14



What We're Reading:

Compliance and Ethics Management (cont.)

As regulatory complexity and reputational risks escalate across industries, compliance and ethics management has emerged as a strategic growth driver.



2025 Global Study on Ethics and Compliance Program Maturity

Overview

The report provides a comprehensive analysis of corporate compliance programs worldwide. The study evaluates the maturity of Ethics and Compliance programs across six core dimensions: Culture, Written Standards, Enforcement and Incentives, Risk Assessment, Training and Communication, and Resources and Board Oversight. It aims to identify areas where organizations excel and where significant shortfalls exist, particularly in embedding ethical behavior into daily operations.

Key Findings

Cultural Alignment Underdeveloped

While 76% of companies conduct annual ethics or culture assessments, only 31% incorporate ethics into performance reviews, risking a disconnect between stated values and actual behavior.

Codes of Conduct Frequently Updated, Not Fully Embedded

71% revise their Code of Conduct every three years or less, yet many struggle to make it relevant and actionable across functions and regions.

Training and Impact Measurement Gaps Persist

Only 44% assess training comprehension and 37% track post-training misconduct trends, limiting insight into program effectiveness.

Investigations Remain Manual and Fragmented

More than 35% still use spreadsheets to track cases, and fewer than 30% leverage cross-functional teams, raising concerns about data quality and consistency.

Risk Assessment Practices Lack Depth

Just 19% assess talent-related risks, and fewer than one-third evaluate reputational or ethical misconduct risks in depth.



Global Business Ethics Survey: The State of Ethics and Compliance in the Workplace

Overview

The report offers a comprehensive analysis of workplace ethics and compliance across the United States. Drawing on data collected in 2013, 2017, 2020, and 2023, the report examines employees' perceptions and experiences related to ethical culture, misconduct, and compliance programs in publicly and privately held for-profit companies.

Key Findings

Most Ethics Outcomes Have Improved Since 2020

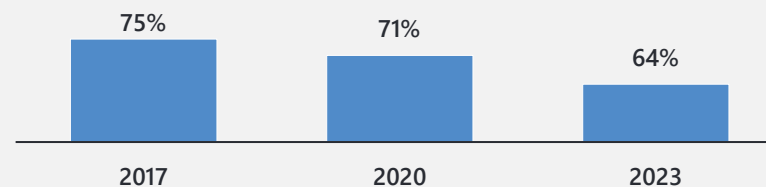
Reporting Rates Have Declined

Ethical Culture Strength—a Driver of Ethics Outcomes—Has Declined Since 2013

'On-The-Road' Employees Are at Heightened Risk

Ethics Management Has a Long Way to Go

Decline in Reporting Rates of U.S. Employees (2017–2023)



Top 10 Risk and Compliance Trends for 2025

Overview

This 2025 NAVEX e-book highlights the 10 most pressing trends shaping ethics and compliance programs. Based on expert insights, customer feedback, and regulatory developments, the report is designed to help compliance leaders anticipate and adapt to emerging challenges in a rapidly evolving risk landscape. It aims to guide organizations in enhancing their compliance effectiveness, protecting brand integrity, and aligning with stakeholder expectations.

Key Findings and Trends for 2025

- 1 Compliance Is a Business Imperative
- 2 New Technology = New Risk
- 3 Third-Party Due Diligence Under Scrutiny
- 4 Global ESG Mandates Boost Compliance Scope
- 5 Data-Driven Programs Deliver Results
- 6 Employee Expectations Are Changing
- 7 Hotlines Aren't Enough
- 8 Culture and Conduct Monitoring Grow Up
- 9 Boards Are More Engaged
- 10 Regulators Expect Proactivity



What We're Reading:

Compliance and Ethics Management (cont.)

As regulatory complexity and reputational risks escalate across industries, compliance and ethics management has emerged as a strategic growth driver.



Top Ethics and Compliance Failures of 2024

Overview

The article provides an annual analysis of significant corporate ethics and compliance breakdowns. It aims to highlight the real-world consequences of noncompliance for companies, their customers, and employees.

This annual feature serves as a cautionary tale for compliance professionals, emphasizing the importance of robust ethics and compliance programs. By examining notable failures, the article seeks to inform and guide organizations in strengthening their compliance frameworks to prevent similar issues.

Notable Case Studies

The article discusses several high-profile cases from 2024, including:



Boeing

Boeing agreed to pay more than \$1.1 billion to avoid prosecution for the 737 MAX crashes that killed 346 people. The deal includes a \$243.6 million fine, \$444.5 million to victims' families, and \$455 million for safety improvements—but critics argue it lacks accountability, as Boeing avoids a criminal conviction and independent oversight.



TD Bank

TD Bank was fined \$3.1 billion for failing to prevent money laundering, facing both criminal penalties and regulatory restrictions. Its U.S. operations are now barred from opening new branches or growing assets beyond \$434 billion without federal approval.



RTX/Raytheon

RTX's Raytheon unit agreed to pay more than \$950 million to resolve allegations of defective pricing, export control violations, and foreign bribery related to government contracts from 2009 to 2020, one of the largest settlements of its kind.



Hyundai Motor

Hyundai faced allegations of child labor violations in its U.S. supply chain. The U.S. Department of Labor sued Hyundai and its Alabama partners over these alleged violations, highlighting the need for strict compliance and oversight in labor practices.



Costa Coffee

Costa Coffee was involved in a tragic incident where inadequate allergen training led to a customer's death. An inquest found that some e-learning courses failed to warn companies when employees struggled through education and testing, leading to insufficient awareness and handling of allergen information.



Evolve Bank & Trust

Evolve faced a Federal Reserve cease-and-desist order over anti-money laundering and risk management failures. Its ties to collapsed FinTech partner Synapse left customers with frozen funds, exposing major oversight gaps.



Gunvor

Gunvor agreed to pay more than \$661 million to resolve investigations by U.S. and Swiss authorities into a bribery scheme in Ecuador. The company admitted to paying bribes to secure oil contracts, with internal compliance failures allowing the misconduct to continue unchecked for years.



FDIC

The FDIC faced internal scrutiny after an independent investigation uncovered a pervasive culture of sexual harassment and misconduct within the agency. The report, prompted by a *Wall Street Journal* exposé, revealed that senior officials tolerated inappropriate behavior for years, leading to widespread employee dissatisfaction and calls for leadership changes.



Key Subsector Trends:

Financial Crime and Financial Risk Management

Financial Credit and Financial Risk Management Highlights

Increasing Use of AI and ML

Generative AI and machine learning are already meaningfully transforming KYC and AML. These technologies are now being used for intelligent customer risk profiles, automated identity verification, automated transaction monitoring, and faster detection of criminal activities. AI and ML are already helping to improve accuracy, reduce false positives, and enhance efficiency.

AI and ML Benefit Fraudsters as Well, Specifically Through Deepfake Technology

AI and ML technologies can cut both ways, allowing fraudsters to deploy new tactics like deepfake technology, synthetic identities and voices, and true adversarial AI. This AI arms race between criminals and those seeking to stop them shows no signs of slowing down.

Regulatory Growth and Harmonization

Governing bodies and regulatory authorities globally are ramping up financial penalties for AML failures and are also tightening AML, KYB, and KYC regulations with a goal of harmonizing global standards. The EU's AML package and the Financial Action Task Force are pushing for global standards and greater data sharing globally.

Cybersecurity and Data Privacy Integration

Financial and cyber crimes are increasingly one and the same, as criminals not only utilize cyber crimes like ransomware and phishing to steal money but also use digital channels for the illicit movement of money. AML and cybersecurity frameworks must be merged, and stronger collaboration between cyber risk management and financial crime risk management must be the baseline.

Top Recent Financial Credit and Financial Risk Management Deals⁽¹⁾

(\$ in Millions)

Date	Company	Selected Investor(s)	Deal Type	Enterprise Value
Jun-25	acin	CUBE	Buyout	--
Apr-25	Demyst	feedzai	Buyout	--
Feb-25	Clari5	Perfios	Buyout	--
Jan-25	Alteryx	Chainalysis	Buyout	--
Jan-25	parallel MARKETS	iCapital	Buyout	--
Dec-24	FEATURE SPACE	VISA	Buyout	\$946
Dec-24	IDverse™	LexisNexis®	Buyout	--
Oct-24	effectiv	Socure	Buyout	\$136
Aug-24	BioCatch	PERMIRA	Buyout	--
Aug-24	neuroID	experian™	Buyout	\$145
Aug-24	puthaoras	MCO MyComplianceOffice	Buyout	--
Apr-24	onfido	ENTRUST	Buyout	--



What We're Reading:

Financial Crime and Financial Risk Management (cont.)

Anti-money laundering compliance in 2025 is being transformed by AI, digitization, and cross-border collaboration, enabling faster, more accurate detection while keeping pace with increasingly complex financial crimes.



**AML Trends and Technology:
Navigating the Future of AML in 2025**

Overview

The report examines how financial institutions can enhance their anti-money laundering (AML) and counter-financing of terrorism (CFT) programs in response to evolving regulatory landscapes, technological advancements, and emerging threats. It emphasizes a global shift toward risk-based compliance frameworks, the dual role of generative AI as both a tool for financial institutions and a potential asset for criminals, and the necessity for targeted detection of predicate crimes.

Key Findings

Global Scale of Financial Crime

In 2023, an estimated \$3.1 trillion in illicit funds flowed through the global financial system, highlighting the immense scale of money laundering and related activities.

Regulatory Evolution

Jurisdictions like the U.S., Canada, and the EU are advancing reforms to strengthen AML/CFT processes. These reforms emphasize risk-based approaches, broader jurisdictional alignment, and increased information sharing.

Generative AI's Dual Role

While generative AI offers enhanced capabilities for detecting financial crimes, it also presents new avenues for criminals to exploit, necessitating vigilant implementation and oversight.

Targeted Detection of Predicate Crimes

Financial institutions are encouraged to focus on specific red flags and upstream indicators unique to predicate crimes, enabling more precise identification and prevention of illicit activities.

Enhanced Collaboration

There is a growing emphasis on cross-institutional collaboration and information sharing, facilitated by frameworks like Section 314(b) of the USA PATRIOT Act, to effectively combat financial crimes.



**2025 Trends in AML and Financial Crime Compliance:
A Data-Centric Perspective and Deep Dive Into
Transaction Monitoring**

Overview

The report surveys global AML professionals to assess priorities, challenges, and the adoption of emerging technologies in anti-money laundering efforts. It provides actionable insights into how compliance teams are adapting to a rapidly evolving risk, regulatory, and technology environment.

Key Findings

Efficiency and Automation Take Priority

~75% of respondents are focused on increasing operational efficiency by reducing manual workloads and adopting automation, especially in transaction monitoring and KYC workflows.

AI Adoption Accelerating, but Still Maturing

While only 28.2% of institutions currently use AI, nearly 50% plan to implement it in 2025, mainly for transaction monitoring, sanctions screening, and risk scoring.

Compliance Monitoring Becoming More Real-Time

More than half (50.3%) of organizations now conduct real-time sanctions and watchlist screening, indicating a significant shift toward proactive, technology-enabled compliance.

Budget Growth Amid Uncertainty

Investments in AML tools are rising, but 41% of professionals remain unsure whether their budgets are sufficient to meet 2025 goals, underscoring tension between ambition and resources.

Key Statistics

90%

AI/ML Adoption by FIs in 2025

40%+

False Positive Reductions Due to AI

70%+

KYC Digitization Rates

15%

AML/KYC Usage via Blockchain Tech



What We're Reading:

Financial Crime and Financial Risk Management (cont.)

Anti-money laundering compliance in 2025 is being transformed by AI, digitization, and cross-border collaboration, enabling faster, more accurate detection while keeping pace with increasingly complex financial crimes.

ALESSA

AML Compliance Trends in 2025:
Key Insights and Industry Shifts

Overview

The article provides insights into how financial institutions are adapting their AML strategies in response to evolving financial crime risks, technological advancements, and regulatory changes. Based on surveys and interviews with industry professionals, the report highlights the following key findings shaping AML compliance in 2025.

Key Findings

Efficiency and Automation Are Priority

Approximately 75% of AML professionals are focusing on enhancing efficiency by reducing manual workloads and improving risk detection capabilities.

AI Adoption on the Rise

While only 28.2% of organizations currently utilize AI in their AML processes, nearly 50% plan to implement AI-driven solutions in 2025, particularly for transaction monitoring and sanctions screening.

Shift Toward Real-Time Sanctions Screening

With 50.3% of organizations conducting sanctions and watchlist screening in real-time, there's a significant move towards automated, dynamic compliance monitoring.

Inconsistent Risk Profiling Practices

Risk profiling remains inconsistent across institutions: 43.3% conduct annual reviews, while only 22.4% perform daily assessments, indicating a need for continuous monitoring and AI-driven risk scoring.

Budget Increases Amid Uncertainty

Despite increased investments in AML compliance, 41.3% of professionals are uncertain whether their budgets are sufficient to meet 2025 goals. Key areas of investment include transaction monitoring, KYC enhancements, and automation.



Top Financial Compliance Trends to Watch for in 2025

Overview

This report identifies key developments shaping the financial crime compliance landscape. It aims to equip financial institutions with insights to enhance their compliance strategies amid evolving challenges and opportunities and provides key predictions for the year.

Key Findings

Artificial Intelligence Begins to Bear Fruit in the Fight Against Financial Crime

With a 56% increase in AI-backed financial crimes, banks need to reassess existing tactics. The way to combat this is through a combined approach that integrates AI-powered solutions, human expertise, and high-quality data.

Private-Public Partnerships Highlight the Value of Strategic Collaboration

The increasingly complex criminal networks and transnational nature of financial crime have spawned a shift in the industry toward strategic collaboration, including Project Blood Orange (South Africa), COSMIC (Singapore), and more.

Regulatory Reach Gets Longer, Wider, and Deeper

Ongoing monitoring and robust risk assessment—for gatekeepers as well as for ESG risk—will be key to ensuring third-party relationships stand up to scrutiny in an evolving regulatory landscape.

Bribery and Corruption Take Top Billing

More than two-thirds of the 180 countries ranked in Transparency International's Corruption Perceptions Index have serious corruption problems. Managing risks from bribery and corruption remains a challenge worldwide.

Customers Continue to Set the Bar Higher

The digital transformation that took hold during COVID-19 has not abated. It has elevated expectations. Consumers want speed, convenience, security, low fees, and a personalized experience, all in a seamless, secure environment that doesn't make them jump through hoops for every interaction.



Key Subsector Trends:

Environmental, Health, and Safety

Environmental, Health, and Safety Highlights

Workforce Safety Remains a Business-Critical Challenge

Despite regulations and awareness, workplace health and safety issues continue to pose serious risks to people and to business performance. Workplace injuries and illnesses cost U.S. employers more than \$175 billion annually, including lost productivity, medical expenses, and legal fees.

Increasing Regulatory Compliance Risks

Workplace health and safety regulations are increasing in scope, depth, and complexity globally. OSHA compliance in occupational health and safety regulations is a complex and costly challenge, with fines of up to \$140,000 for repeat or willful violations.⁽²⁾

Fragmented Systems and Siloed Workflows

Most organizations rely on a patchwork of disconnected tools (spreadsheets, legacy software, and paper-based records) to manage EHS software.

Increased Use of Subcontractors


Firms globally, specifically in industries such as construction, logistics, oil and gas, and manufacturing, are rapidly expanding their use of third-party contractors over full-time employees, and EHS solutions must address third party and contractor risk management to provide a holistic view of a businesses workforce.

ESG and EHS Regulatory Convergence

The rise of ESG-related regulations is causing firms to collect and disclose supplier and contractor-related information on worker conditions, carbon footprint, and safety records.

Top Recent Environmental, Health, and Safety Deals⁽¹⁾

(\$ in Millions)

Date	Company	Selected Investor(s)	Deal Type	Enterprise Value
Feb-25	 envirosuite	 Ideagen	Buyout	\$144
Jan-25	 meddbase	 cority	Buyout	--
Oct-24	 SKILLKO	 hsi Health & Safety Institute	Buyout	--
Sep-24	 ANVL	 BENCHMARK GENSUITE	Buyout	--
Sep-24	 COMPLIANCE TRAINING ONLINE	 360 TRAINING	Buyout	--
Jul-24	 inx	 AKKR	Buyout	--
Apr-24	 Avetta	 IEQT	Buyout	\$3,000
Apr-24	 DAMSTRA	 Ideagen	Buyout	--
Jan-24	 CONTRACTOR COMPLIANCE	 velocityEHS	Buyout	--
Oct-23	 EVOTIX	 SAI360	Buyout	--
Jun-22	 Quentic	 amcs	Buyout	--

Sources: PitchBook, CB Insights, company filings, company websites, press releases.

⁽¹⁾ Includes M&A and capital raises.⁽²⁾ OSHA.



What We're Reading:

Environmental, Health, and Safety (cont.)

Workplace safety goes beyond meeting regulatory requirements—it's a critical element that directly impacts a company's financial performance.



Verdantix Market Size and Forecast:
EHS Software 2023–2029 (Global)

Overview

The report provides an in-depth analysis of the global environmental, health, and safety (EHS) software market. Aimed at software vendors, service providers, and investors, it outlines current market size, regional and sectoral breakdowns, and growth drivers through 2029. The report is based on vendor data, macroeconomic trends, and insights from 301 senior EHS decision-makers across 25 industries in 24 countries.

The Verdantix model macroeconomic drivers and insights gathered via research put the EHS software market at \$1.9 billion in 2023. Propelled by various factors, the market will grow by a CAGR of 14.6% to reach \$4.5 billion in 2029.

Key Findings



Cost to Business

Workplace injuries and illnesses cost U.S. employers more than \$175 billion annually, including lost productivity, medical expenses, and legal fees.



Human Cost of Mental Health Neglect

Approximately one in five workers experience mental health issues annually, yet only 57% of employers have a mental health strategy in place.



New Risks in Evolving Workspaces

Hybrid and remote setups increase risks such as poor ergonomics, burnout, and lack of emergency preparedness.

Growth Drivers



Rising ESG Reporting Mandates
(e.g., CSRD, TCFD, SBTi)



Increasing Use of Subcontractors and Contractor Safety Software



Expansion of EHS Software Adoption in Low-Penetrated Geographies



Accelerating AI Integration—Tools Like NLP, Video Analytics, and Chatbots for EHS Workflows

Industry Segment Dynamics



High-Risk Industries

Very high-risk industries (oil and gas, mining, chemicals) account for \$969 million (49%) of the 2023 market; they still lead in 2029 despite the slowest CAGR (11%).

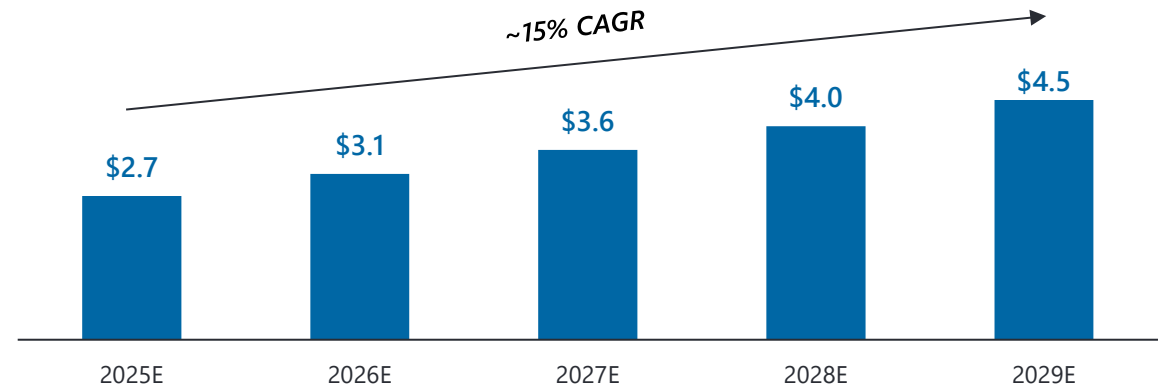


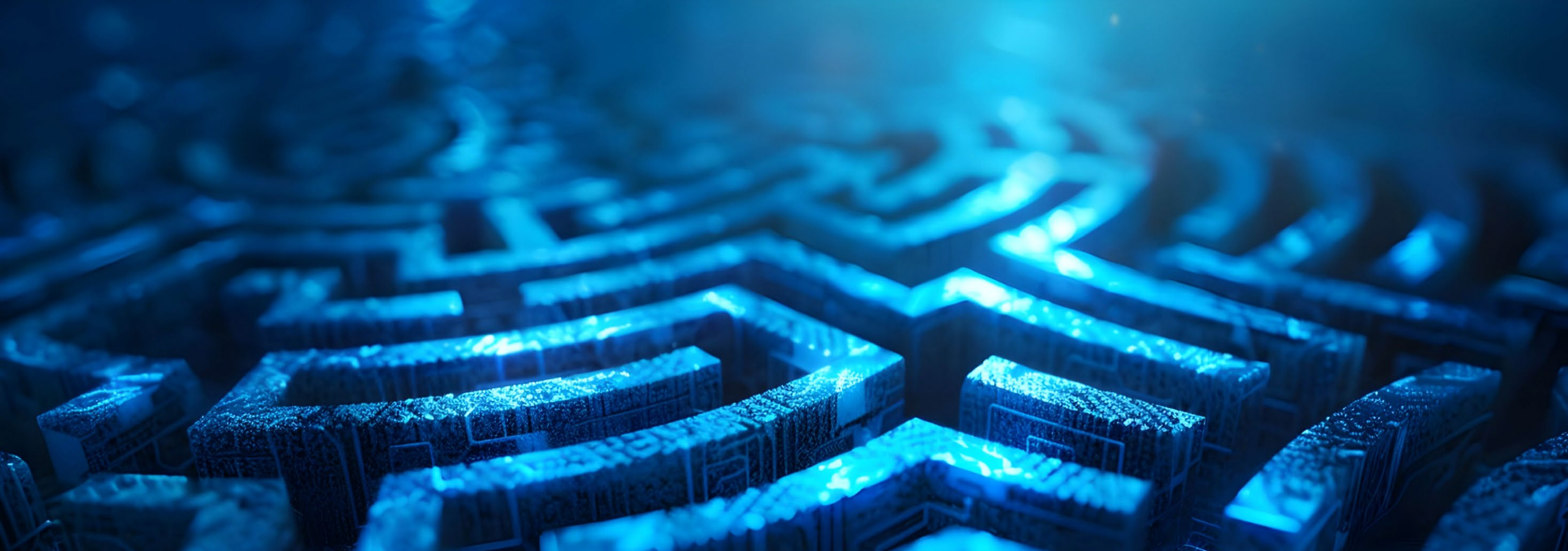
Low-Risk Industries

Low-risk industries (e.g., real estate, retail, hospitality) will grow fastest—up to 27% CAGR, driven by falling tech costs and rising compliance expectations.

Approximate Market Size

The EHS software market is a massive segment forecasted to grow at ~15% CAGR.





Market Maps

03

GRC Sector Landscape

Third-Party Risk Management

Environmental, Health, and Safety

Audit and Risk Management

Financial Crime and Financial Risk Management

Governance, Risk, and Compliance

Business Continuity Management

Compliance and Ethics Management

IT and Cybersecurity Risk Management

Environmental, Social, and Governance

Note: Market map lists are meant to be representative and not exhaustive.

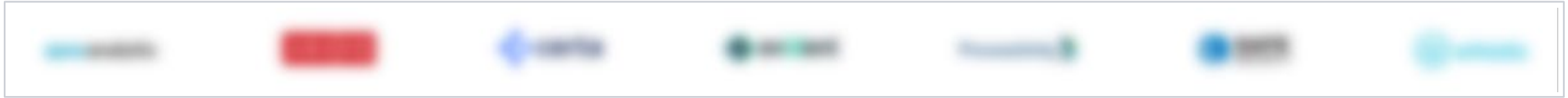
To view the full market map, please contact Andrew.Atherton@HL.com.



GRC: Third-Party Risk Management

Selected GRC technology companies (public, investor-backed, and privately held).

THIRD-PARTY RISK MANAGEMENT PLATFORMS



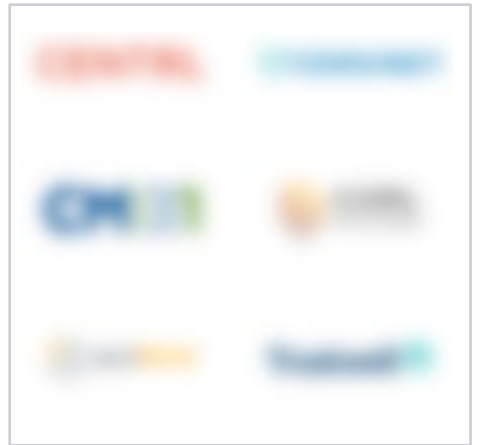
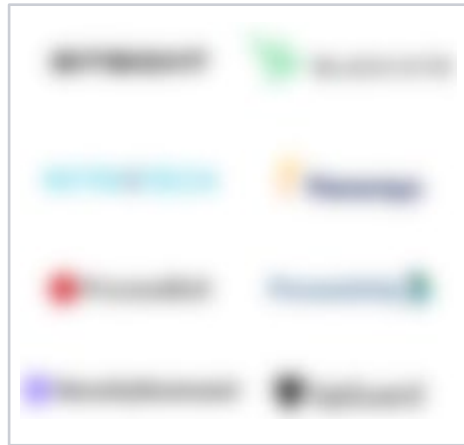
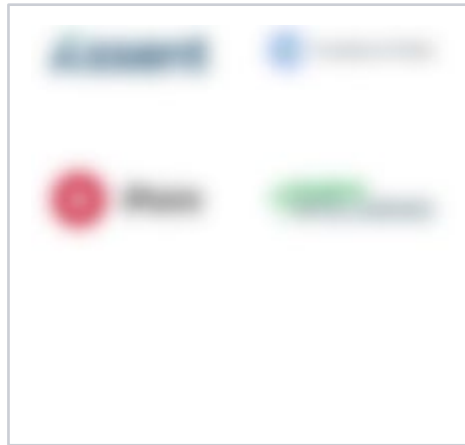
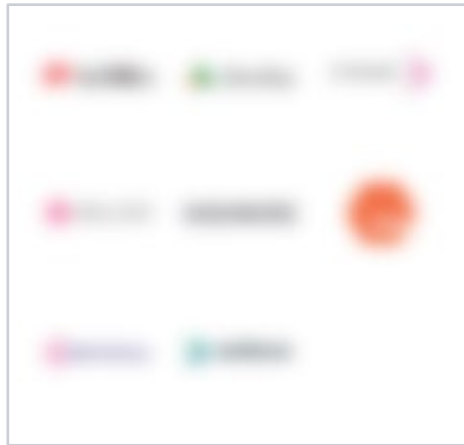
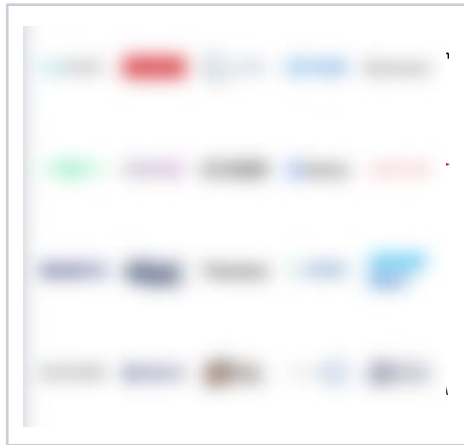
SUPPLIER AND SUPPLY CHAIN RISK MANAGEMENT

CONTRACTOR RISK MANAGEMENT

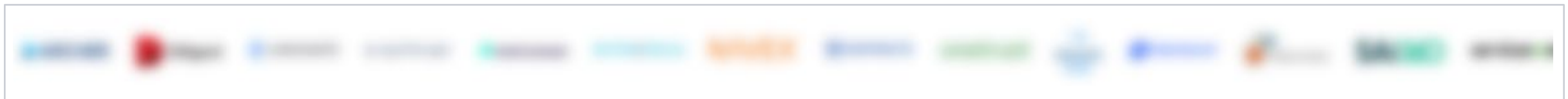
PRODUCT COMPLIANCE

THIRD-PARTY CYBER RISK MANAGEMENT

VERTICALLY SPECIFIC TPRM



BROADER GRC PLATFORMS



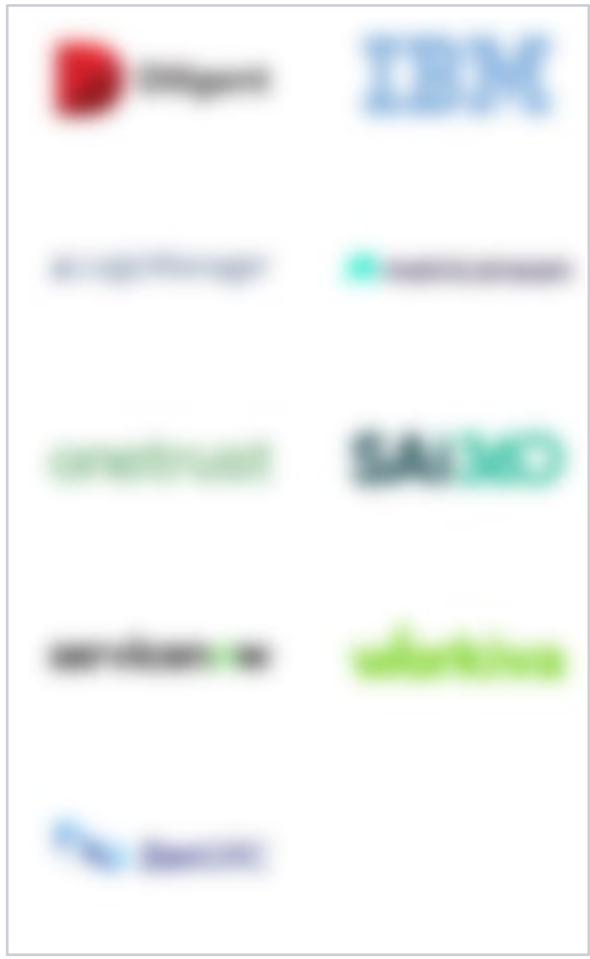
To view the full market map, please contact Andrew.Atherton@HL.com.



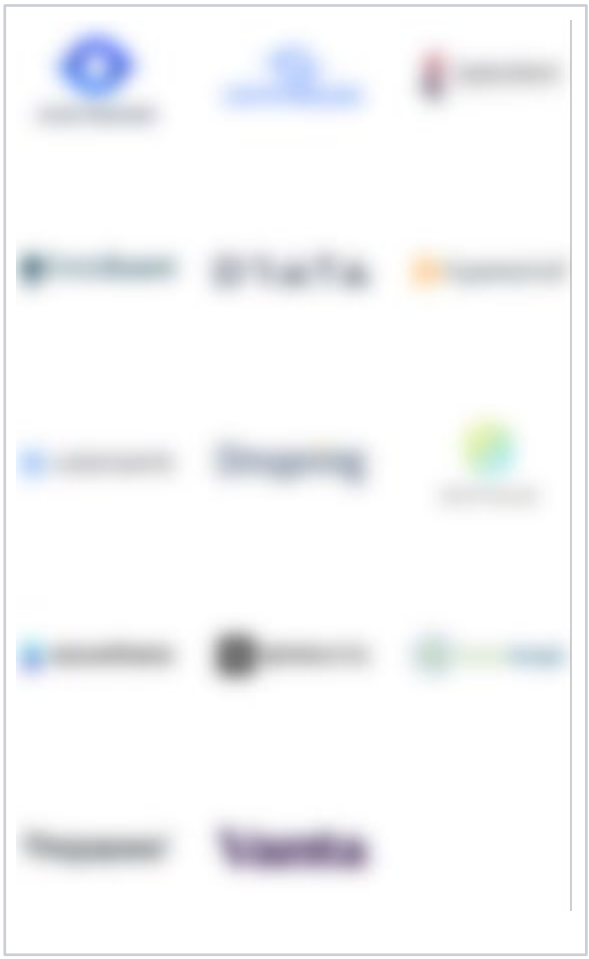
GRC: Audit and Risk Management

Selected GRC technology companies (public, investor-backed, and privately held).

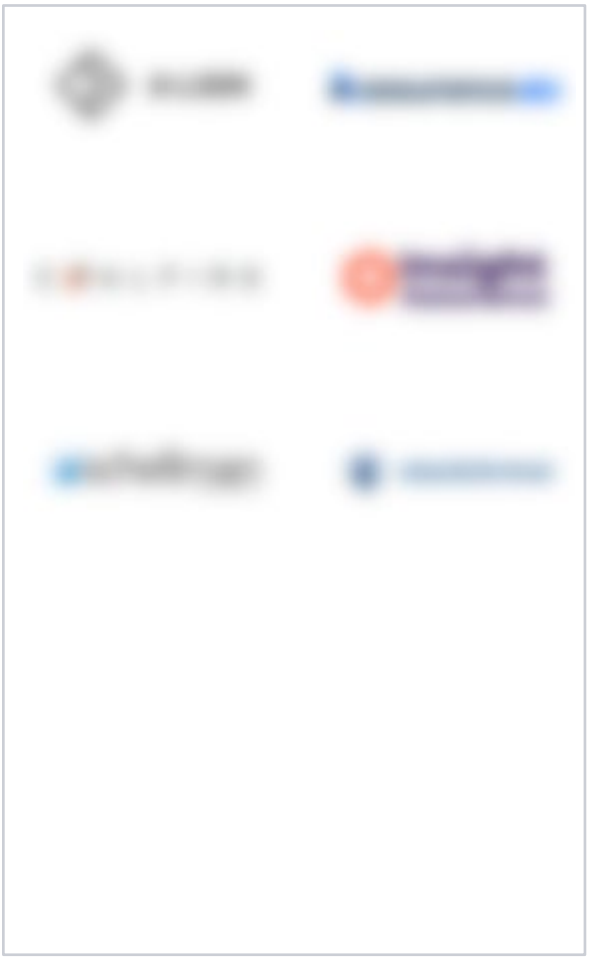
COMPREHENSIVE GRC PLATFORMS



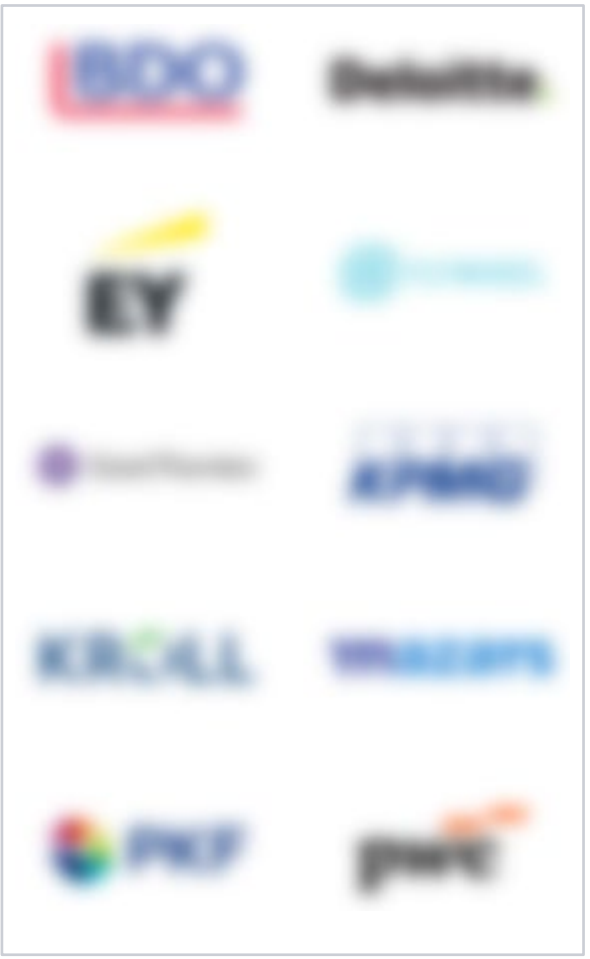
AUDIT-CENTRIC PLATFORMS



IT COMPLIANCE SERVICES



PROFESSIONAL SERVICES



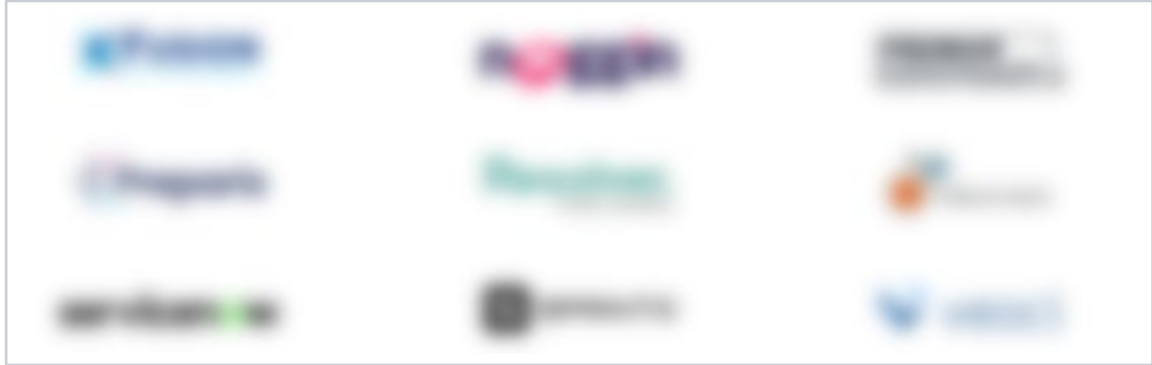
To view the full market map, please contact Andrew.Atherton@HL.com.



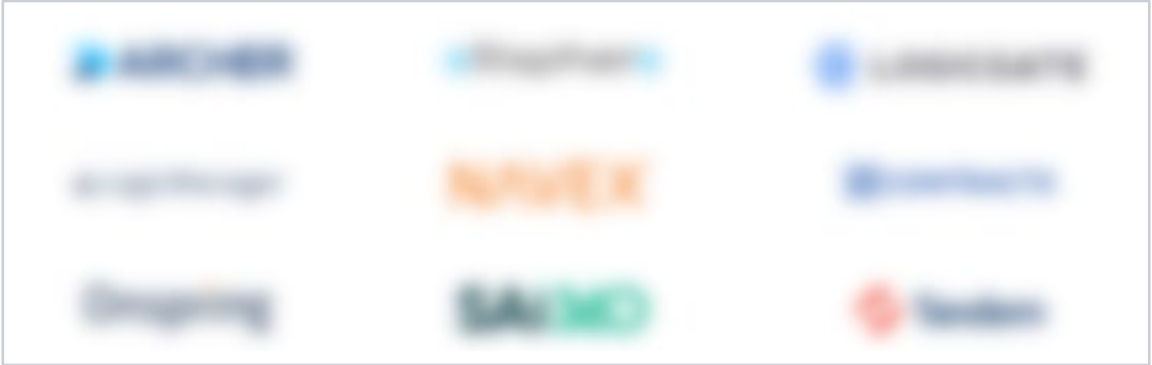
GRC: Business Continuity Management

Selected GRC technology companies (public, investor-backed, and privately held).

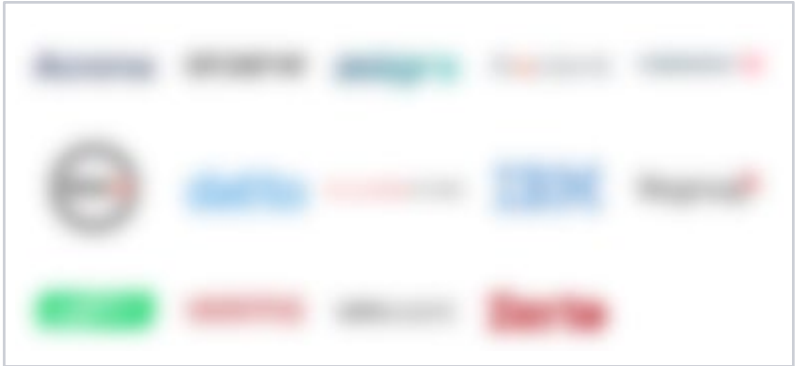
BUSINESS CONTINUITY PLANNING SOFTWARE



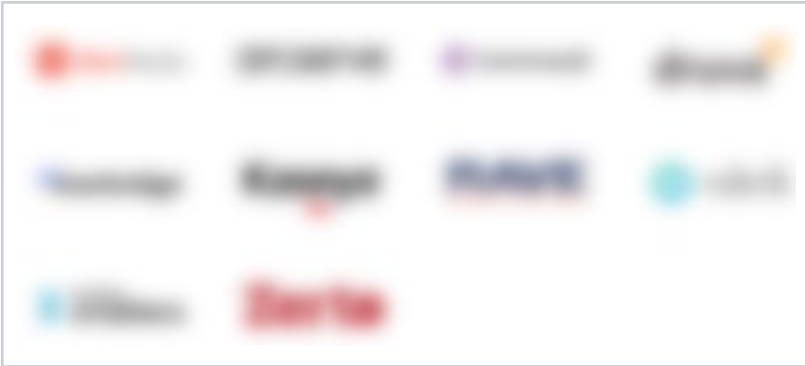
BROADER GRC AND BCM PLATFORMS



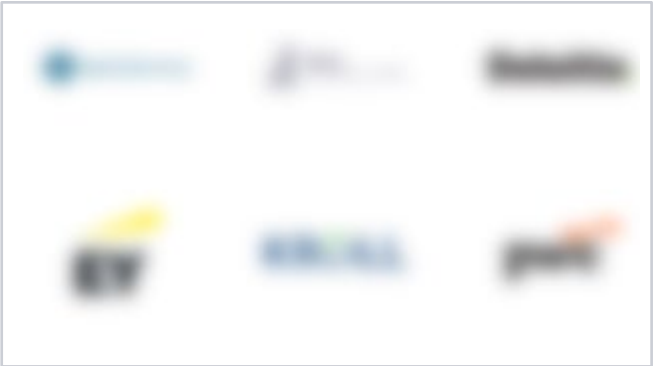
DISASTER RECOVERY, DATA PROTECTION, AND BACKUP



EMERGENCY NOTIFICATION AND CRISIS MANAGEMENT



CONSULTING AND ADVISORY SERVICES



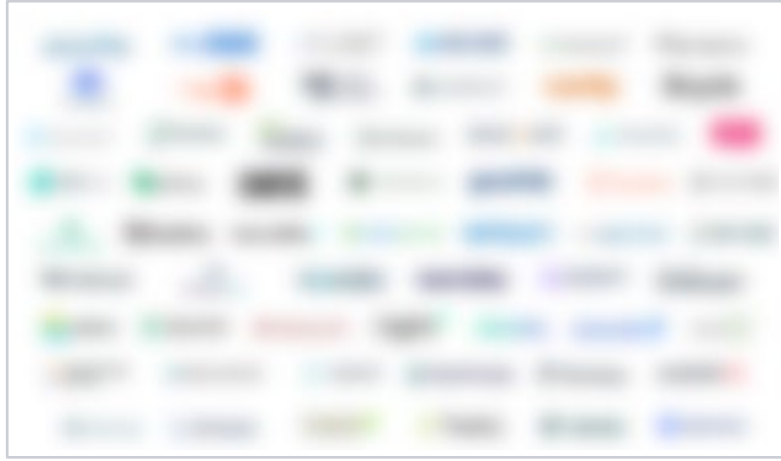
To view the full market map, please contact Andrew.Atherton@HL.com.



GRC: ESG

Selected GRC technology companies (public, investor-backed, and privately held).

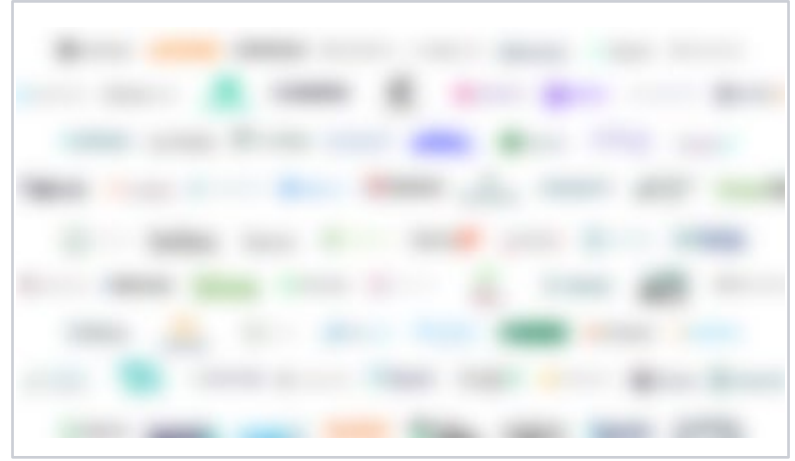
ESG REPORTING AND MONITORING



GHG ACCOUNTING AND OFFSETTING



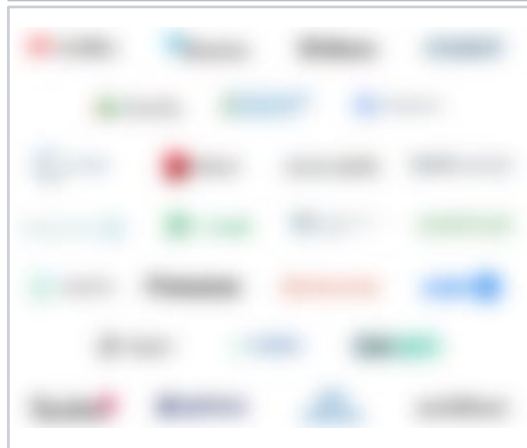
SUSTAINABLE FINANCE AND INSURANCE



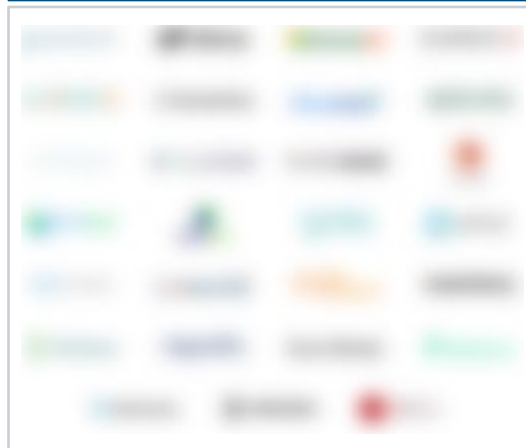
DATA AND ANALYTICS



SUSTAINABLE SUPPLY CHAINS



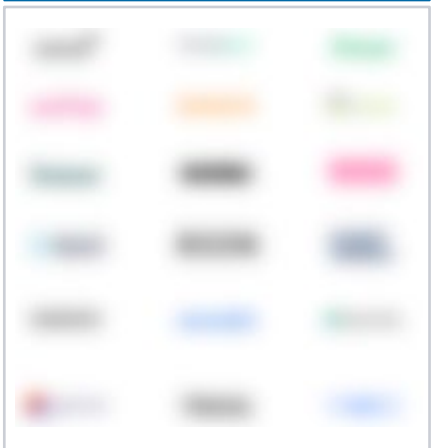
ESG MACRO RISK MANAGEMENT



CLEAN AND RENEWABLE ENERGY



RESOURCE EFFICIENCY AND CIRCULARITY



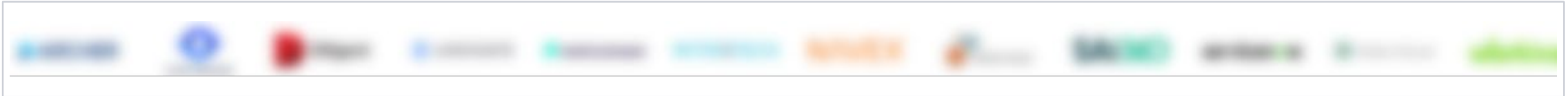
To view the full market map, please contact Andrew.Atherton@HL.com.



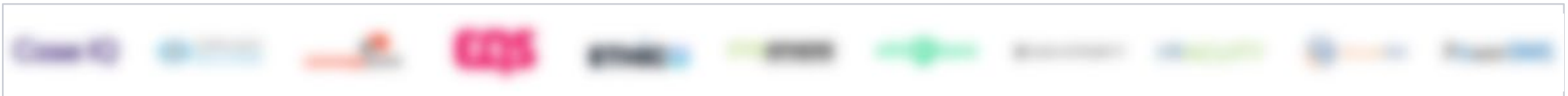
GRC: Compliance and Ethics Management

Selected GRC technology companies (public, investor-backed, and privately held).

GRC PLATFORMS



COMPLIANCE AND ETHICS MANAGEMENT PLATFORMS

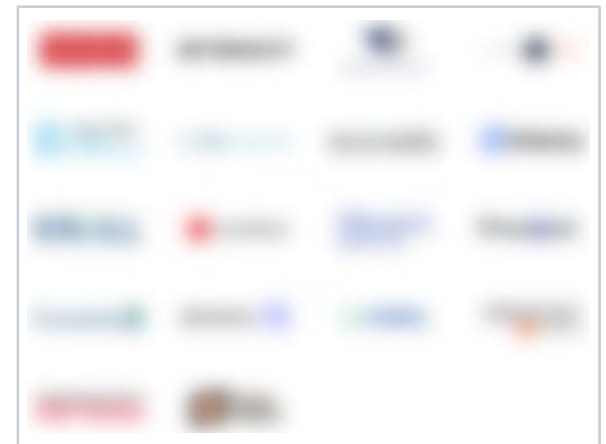
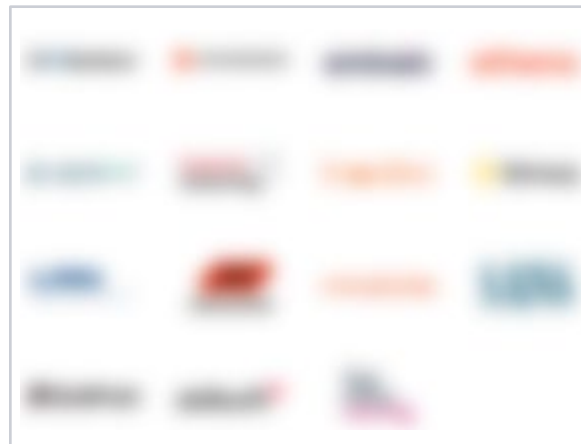
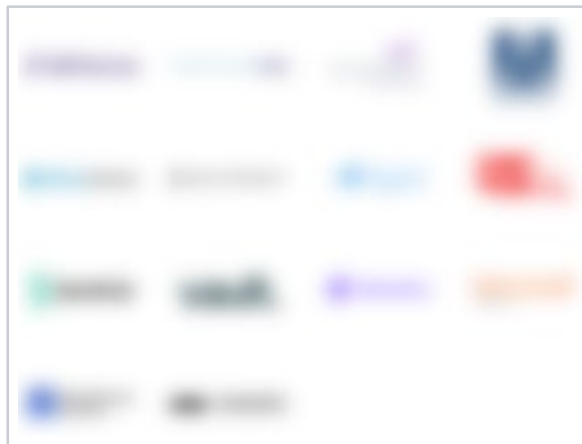
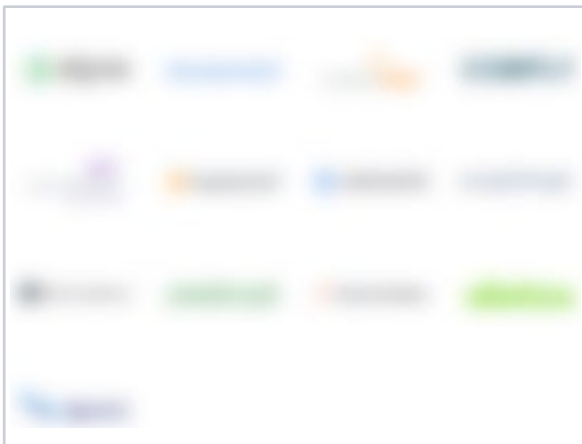


POLICY MANAGEMENT AND CODE OF CONDUCT

WHISTLEBLOWER AND INCIDENTS

TRAINING AND AWARENESS

THIRD-PARTY ETHICS AND INTEGRITY



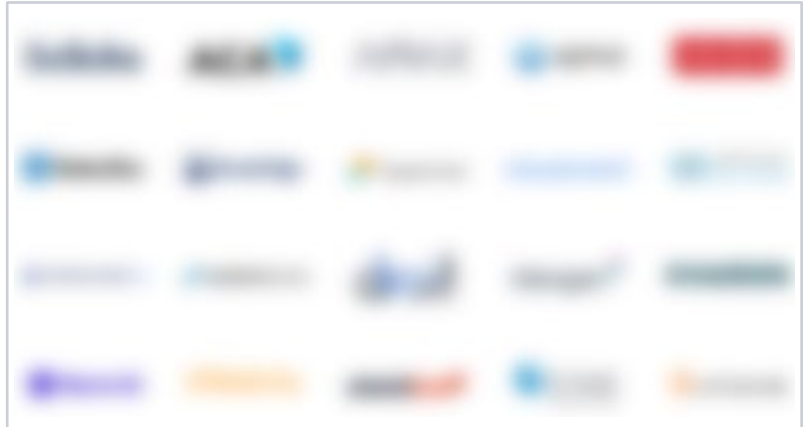
To view the full market map, please contact Andrew.Atherton@HL.com.



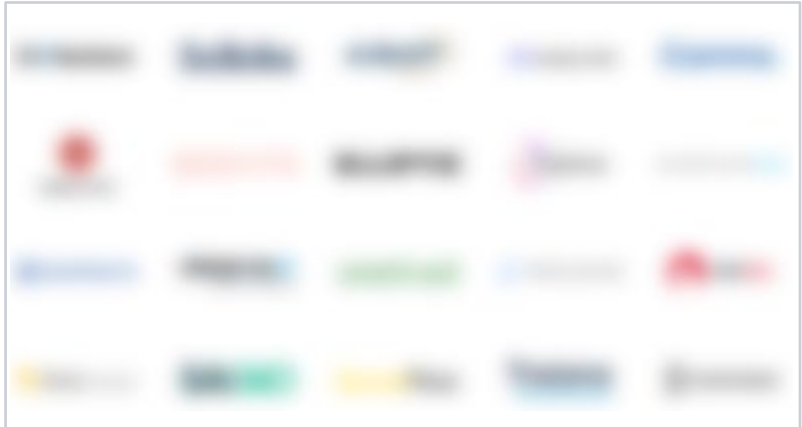
GRC: Financial Crime and Financial Risk Management

Selected GRC technology companies (public, investor-backed, and privately held).

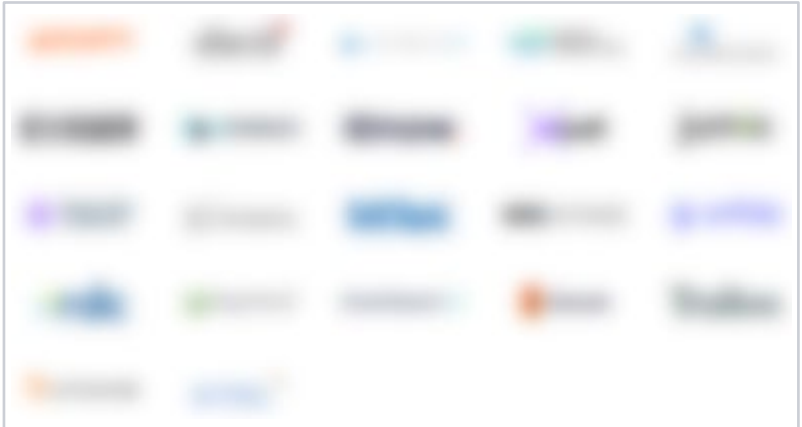
FINANCIAL SERVICES COMPLIANCE



FINANCIAL SERVICES RISK MANAGEMENT



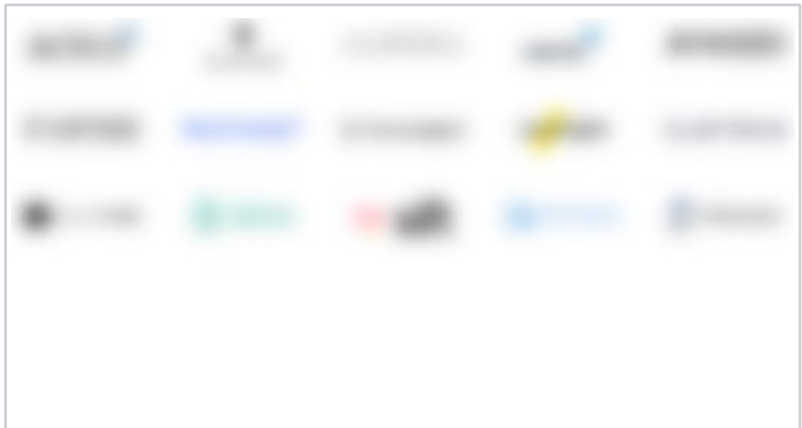
IDENTITY VERIFICATION AND KYC



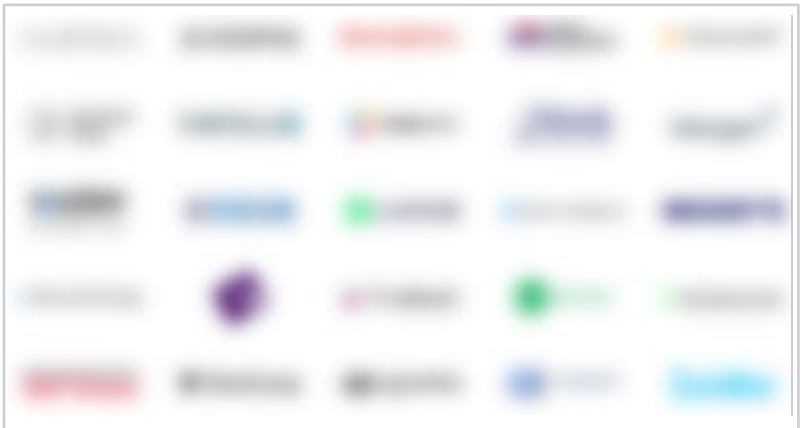
TRANSACTION MONITORING



FINANCIAL CRIME AND FRAUD PREVENTION



REGULATORY REPORTING



To view the full market map, please contact Andrew.Atherton@HL.com.



GRC: EHS

Selected GRC technology companies (public, investor-backed, and privately held).

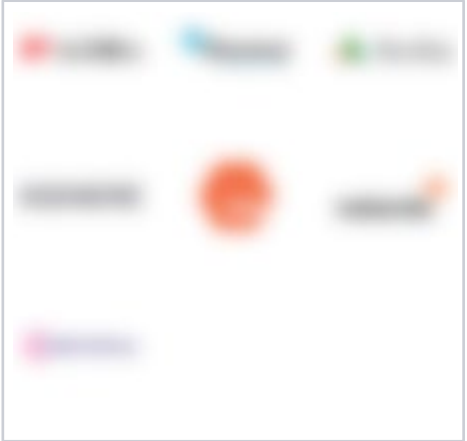
EHS PLATFORMS



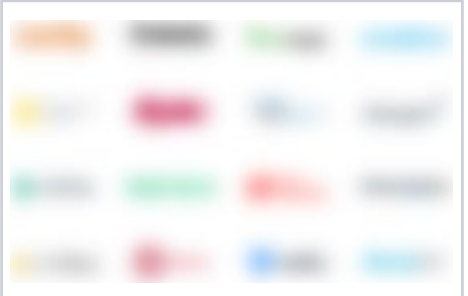
ENVIRONMENTAL COMPLIANCE



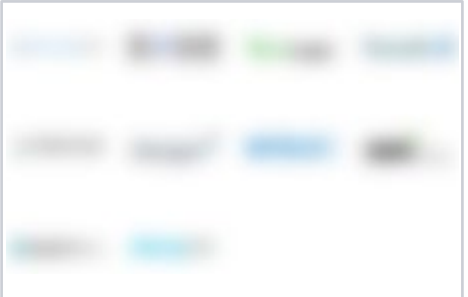
CONTRACTOR MANAGEMENT



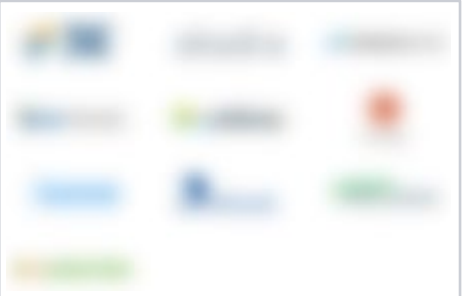
OCCUPATIONAL HEALTH AND SAFETY



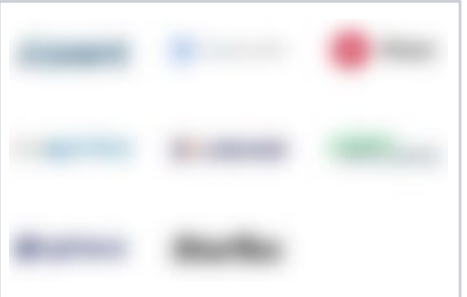
INSPECTION AND AUDIT MANAGEMENT



DATA/INFORMATION SERVICES



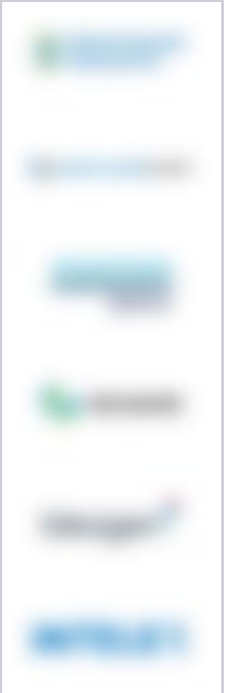
PRODUCT COMPLIANCE



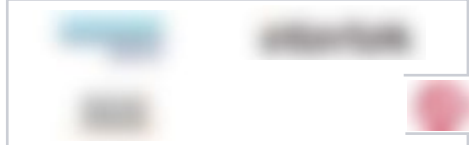
ESG



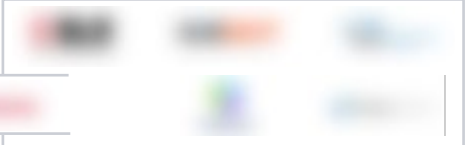
QUALITY MANAGEMENT



AUDIT AND INSPECTION



TRAINING





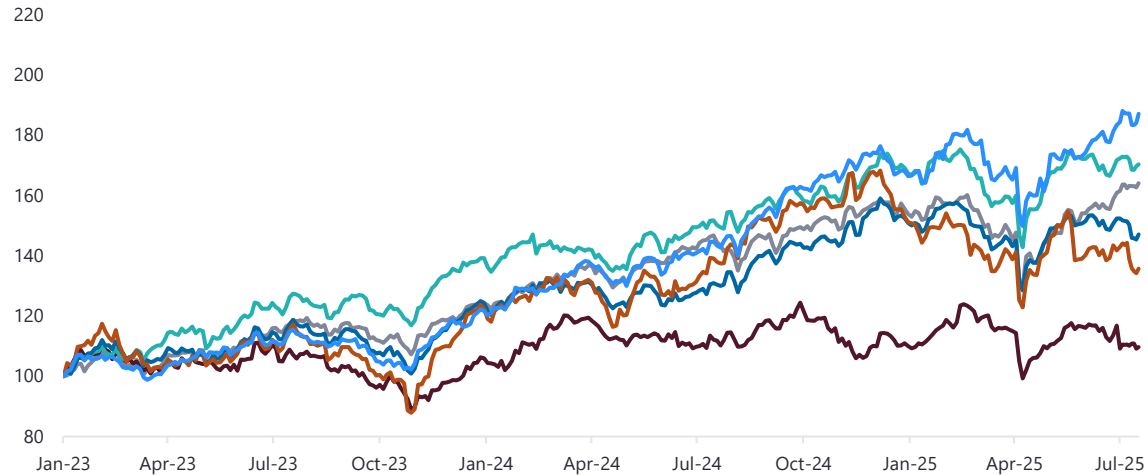
Public Market Performance
and Valuation Update

04

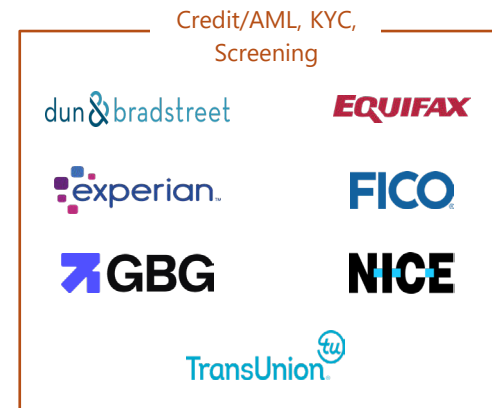
Index Performance: GRC Vs. Broader Market

Considerable variability of performance by the GRC subsector.

Indexed Share Price Performance Since January 2023



Index	Since Jan. '23	Since Jan. '24	YTD '25
S&P 500	64%	33%	7%
GRC Index ⁽¹⁾	47%	21%	(2%)
GRC	70%	25%	2%
EHS	10%	5%	0%
Credit/AML, KYC, Screening	36%	14%	(10%)
Diversified With GRC	87%	56%	12%

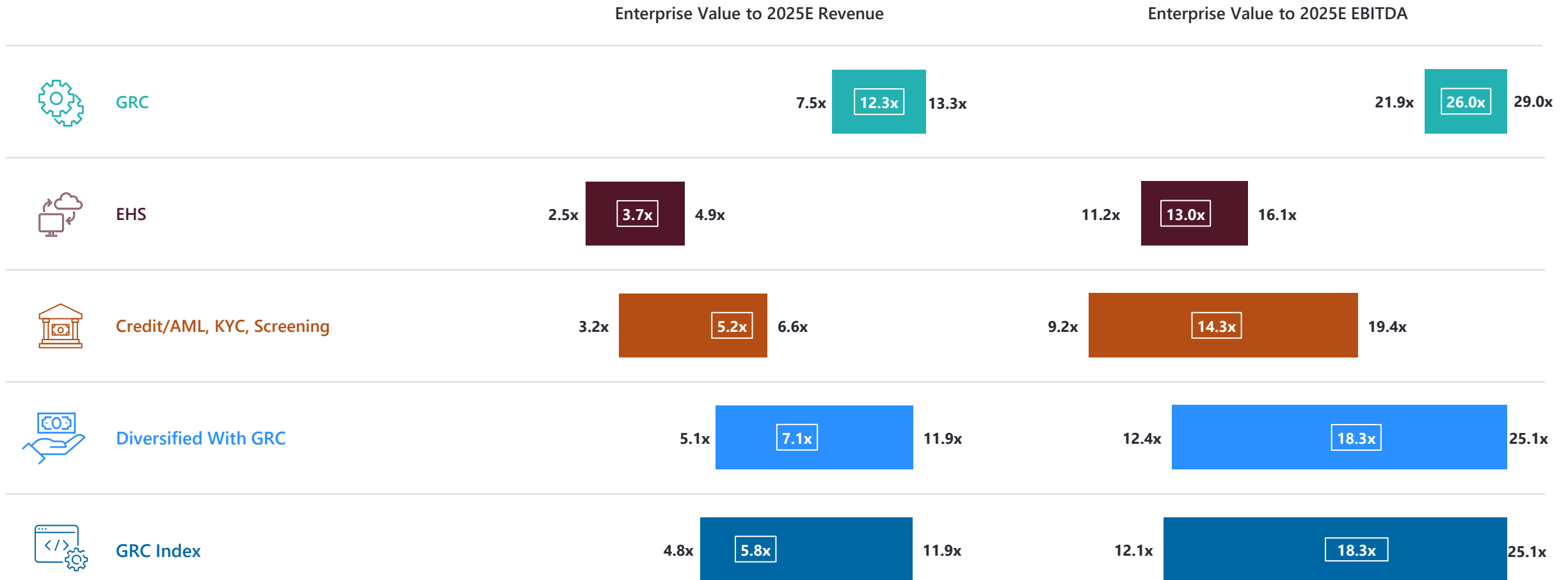


Notes: Indices shown are equal-weighted with all share prices rebased to 100. Data derived from S&P Capital IQ as of July 17, 2025. Companies listed within each subsector are not solely dedicated to that category—they address these areas as part of a more comprehensive solution set.

(1) Total GRC Index includes all companies depicted across all segments of GRC technology, as shown at the bottom of this page.

Key Valuation Metrics by Subsector

Metrics reflect first quartile, median, and upper quartile, respectively.



GRC Public Companies:

Valuation Multiple and Operating Metric Detail

All \$ USD in Millions

Company Name	Capitalization		Stock Performance		Valuation Metrics				Calendar Year 2025E Operating Metrics					Calendar Year 2026E Operating Metrics				
	Market Cap (\$M)	Enterprise Value (\$M)	YTD Return	% of 52 Week High	EV/Revenue		EV/EBITDA		Revenue Growth	Gross Margin	EBITDA Margin	FCF Margin	Rule of 40	Revenue Growth	Gross Margin	EBITDA Margin	FCF Margin	Rule of 40
					CY 2025E	CY 2026E	CY 2025E	CY 2026E										
GRC																		
ServiceNow	\$198,977	\$198,007	(10%)	80%	15.2x	12.8x	43.4x	35.5x	19%	81%	35%	28%	46%	19%	81%	36%	29%	48%
S&P Global	\$161,119	\$176,029	5%	96%	11.8x	11.0x	23.5x	21.9x	6%	--	50%	49%	55%	7%	--	50%	49%	56%
RELX	\$97,925	\$105,997	18%	95%	8.1x	7.6x	20.3x	18.9x	10%	65%	40%	35%	45%	7%	65%	40%	35%	42%
Thomson Reuters	\$94,257	\$95,972	30%	96%	12.8x	11.9x	32.9x	29.9x	3%	73%	39%	31%	34%	8%	75%	40%	32%	40%
Moody's	\$90,406	\$95,693	6%	94%	12.8x	11.9x	26.0x	23.6x	5%	--	49%	45%	49%	8%	--	51%	46%	54%
Verisk	\$42,329	\$45,153	10%	94%	14.7x	13.7x	26.5x	24.5x	7%	70%	55%	47%	54%	7%	70%	56%	48%	55%
Wolters Kluwer	\$37,688	\$40,935	(2%)	78%	5.7x	5.4x	17.4x	16.5x	16%	72%	33%	27%	44%	5%	72%	33%	27%	33%
Workiva	\$3,705	\$4,257	(39%)	57%	4.9x	4.2x	n.a.	39.6x	18%	80%	6%	6%	24%	16%	81%	11%	10%	27%
Median					12.3x	11.4x	26.0x	24.0x	8%	71%	39%	33%	46%	8%	71%	40%	33%	45%
Average					10.7x	9.8x	27.1x	26.3x	10%	55%	38%	33%	44%	10%	56%	39%	35%	44%
EHS																		
Hexagon	\$28,180	\$31,988	10%	78%	5.1x	4.8x	13.9x	12.8x	14%	67%	36%	25%	39%	5%	68%	37%	27%	32%
SGS	\$20,084	\$23,119	3%	84%	2.7x	2.5x	12.1x	11.3x	16%	44%	22%	18%	34%	5%	44%	22%	18%	24%
Fortive	\$17,426	\$20,570	(32%)	62%	5.0x	4.8x	16.8x	16.1x	(34%)	65%	30%	27%	(6%)	4%	65%	30%	28%	31%
Bureau Veritas	\$14,429	\$16,223	6%	88%	2.1x	2.0x	10.7x	9.9x	18%	72%	20%	18%	35%	6%	72%	20%	18%	24%
UL Solutions	\$14,049	\$14,639	40%	95%	4.8x	4.6x	19.8x	18.1x	6%	49%	24%	17%	23%	6%	49%	25%	18%	24%
Intertek	\$10,277	\$11,331	11%	88%	2.4x	2.3x	10.9x	10.3x	9%	39%	22%	18%	27%	5%	39%	23%	19%	23%
Median					3.7x	3.5x	13.0x	12.0x	11%	57%	23%	18%	30%	5%	57%	24%	18%	24%
Average					3.7x	3.5x	14.0x	13.1x	5%	56%	26%	20%	25%	5%	56%	26%	21%	26%

GRC Public Companies: Valuation Multiple and Operating Metric Detail (cont.)

All \$ USD in Millions

Company Name	Capitalization		Stock Performance		Valuation Metrics				Calendar Year 2025E Operating Metrics					Calendar Year 2026E Operating Metrics				
	Market	Enterprise	YTD	% of 52	EV/Revenue		EV/EBITDA		Revenue	Gross	EBITDA	FCF	Rule	Revenue	Gross	EBITDA	FCF	Rule
	Cap (\$M)	Value (\$M)	Return	Week High	CY 2025E	CY 2026E	CY 2025E	CY 2026E	Growth	Margin	Margin	Margin	of 40	Growth	Margin	Margin	Margin	of 40
Credit/AML, KYC, Screening																		
Experian	\$49,772	\$54,557	26%	100%	6.9x	6.4x	19.7x	17.7x	8%	--	35%	26%	34%	9%	--	36%	28%	36%
FICO	\$37,128	\$39,530	(23%)	63%	19.3x	16.7x	34.2x	28.1x	14%	--	56%	55%	69%	16%	--	59%	58%	74%
Equifax	\$32,468	\$37,368	3%	84%	6.2x	5.6x	19.0x	16.6x	6%	56%	33%	25%	30%	11%	57%	34%	27%	38%
TransUnion	\$18,136	\$22,830	0%	82%	5.2x	4.7x	14.3x	12.8x	6%	60%	36%	28%	34%	9%	60%	37%	31%	40%
NICE Systems	\$9,686	\$9,755	(10%)	65%	3.3x	3.1x	9.6x	8.9x	7%	71%	35%	34%	41%	7%	71%	35%	34%	41%
Dun and Bradstreet	\$4,067	\$7,417	(27%)	70%	3.0x	2.9x	7.6x	7.2x	3%	63%	39%	32%	34%	5%	64%	40%	33%	37%
Global Benefits	\$772	\$835	(27%)	60%	2.2x	2.1x	8.9x	8.5x	7%	--	25%	24%	31%	5%	--	25%	24%	29%
Median					5.2x	4.7x	14.3x	12.8x	7%	56%	35%	28%	34%	9%	57%	36%	31%	38%
Average					6.6x	5.9x	16.2x	14.3x	7%	36%	37%	32%	39%	9%	36%	38%	33%	42%
Diversified With GRC																		
Oracle	\$698,697	\$797,381	49%	99%	13.0x	10.9x	25.1x	20.4x	11%	--	52%	9%	21%	19%	--	53%	15%	34%
SAP	\$359,346	\$358,411	(0%)	88%	8.3x	7.4x	26.7x	22.9x	23%	74%	31%	29%	52%	12%	74%	32%	30%	42%
IBM	\$262,090	\$317,962	28%	95%	4.8x	4.6x	18.3x	17.0x	6%	59%	26%	24%	29%	4%	59%	27%	25%	29%
ServiceNow	\$198,977	\$198,007	(10%)	80%	15.2x	12.8x	43.4x	35.5x	19%	81%	35%	28%	46%	19%	81%	36%	29%	48%
Fiserv	\$92,785	\$120,660	(19%)	70%	5.8x	5.3x	11.8x	10.8x	8%	62%	49%	42%	50%	8%	63%	50%	42%	51%
LSEG	\$76,629	\$87,529	16%	99%	7.1x	6.7x	14.7x	13.6x	13%	88%	48%	38%	51%	6%	88%	49%	39%	46%
NASDAQ	\$51,642	\$60,735	16%	99%	11.9x	11.1x	20.8x	19.2x	9%	--	57%	53%	62%	7%	--	58%	54%	61%
FIS	\$42,269	\$53,555	(0%)	88%	5.1x	4.9x	12.4x	11.7x	3%	38%	41%	32%	35%	4%	38%	42%	33%	38%
GlobalData	\$1,388	\$1,431	(23%)	59%	3.2x	3.1x	8.3x	7.5x	24%	--	39%	37%	60%	6%	--	41%	38%	44%
Median					7.1x	6.7x	18.3x	17.0x	11%	59%	41%	32%	50%	7%	59%	42%	33%	44%
Average					8.3x	7.4x	20.2x	17.6x	13%	45%	42%	32%	45%	10%	45%	43%	34%	44%
Global Median					5.8x	5.4x	18.3x	16.8x	9%	61%	36%	28%	37%	7%	62%	37%	29%	39%
Global Average					7.6x	6.9x	19.6x	18.3x	9%	48%	37%	30%	39%	8%	48%	38%	31%	40%



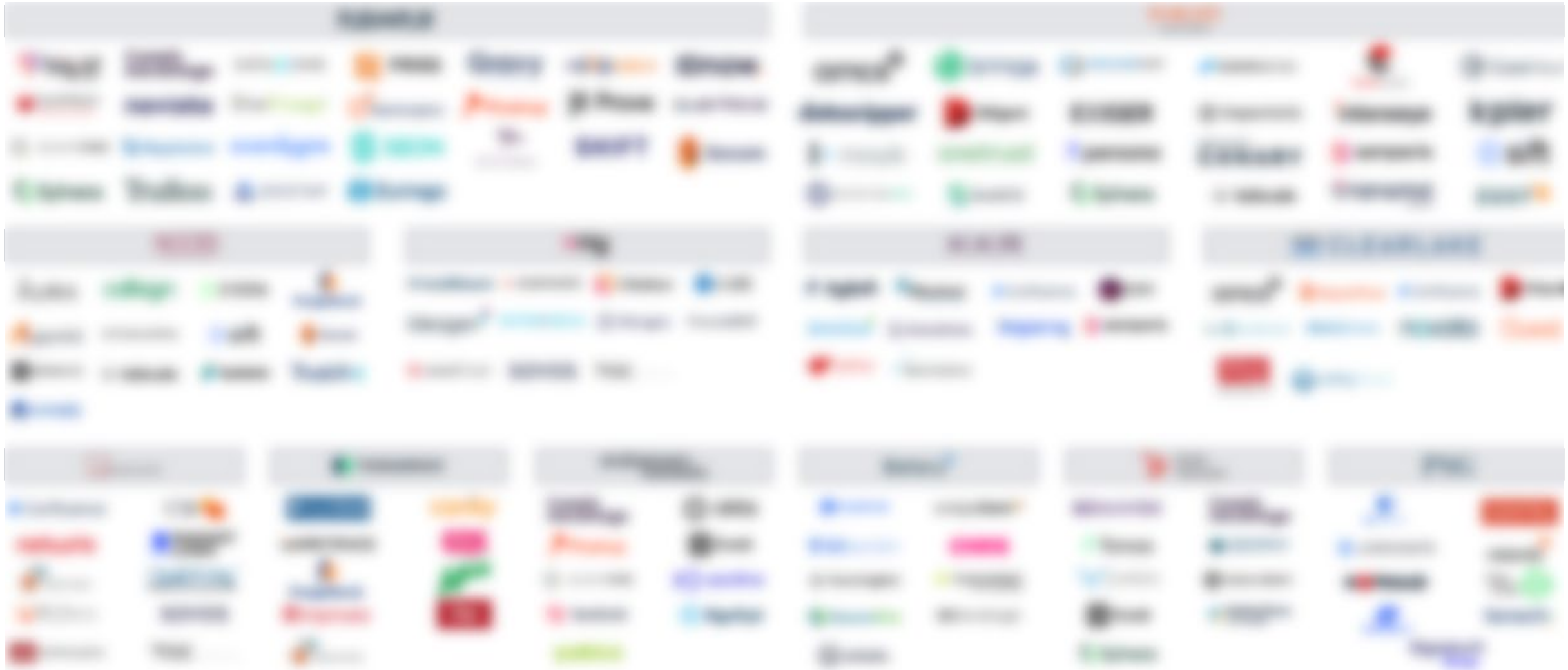
GRC Notable Deal Activity:
Investors, Acquirers, and
Transactions

05

To view the full sponsorscape, please contact Andrew.Atherton@HL.com.

GRC Sponsorscape

The investor field is broad and diversified.



To view the full sponsorscape, please contact Andrew.Atherton@HL.com.

GRC Sponsorscape (cont.)

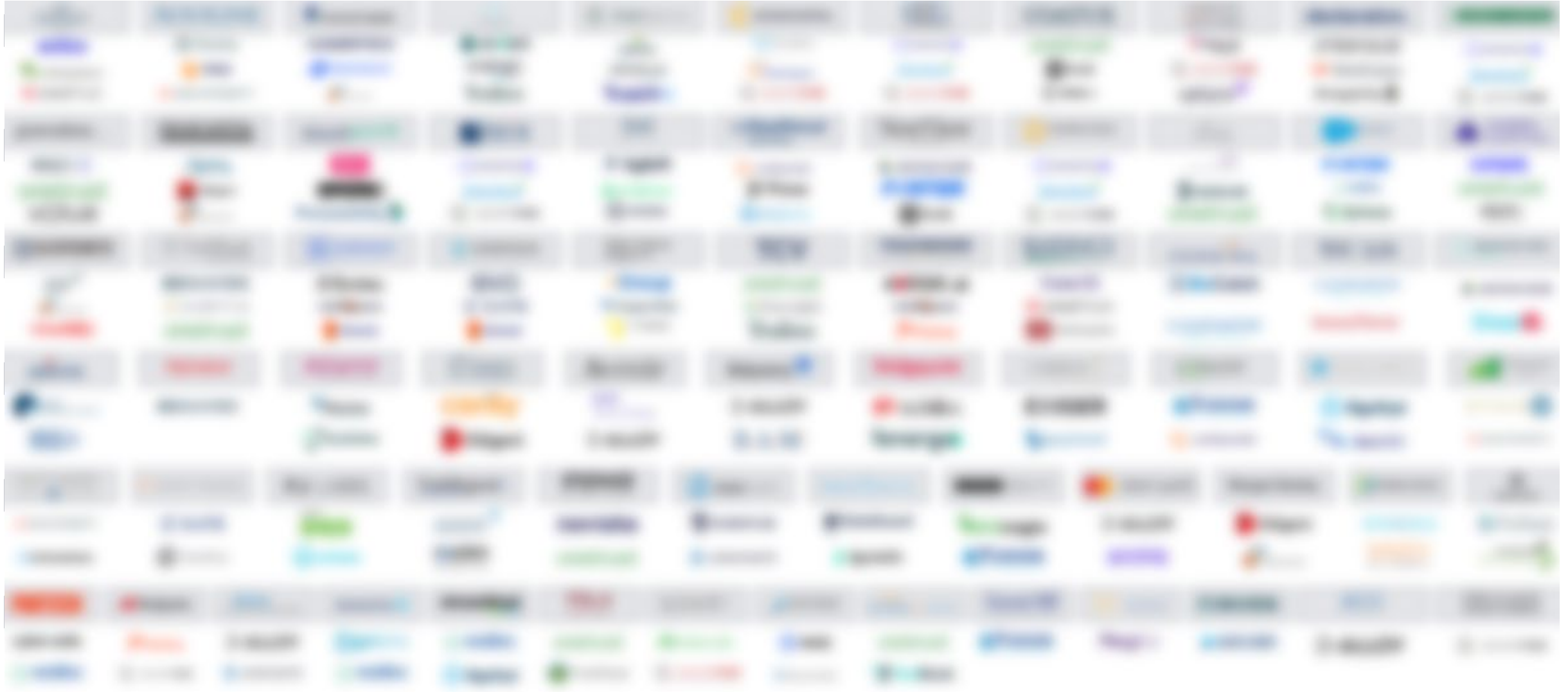
The investor field is broad and diversified.



To view the full sponsorscape, please contact Andrew.Atherton@HL.com.

GRC Sponsorscape (cont.)

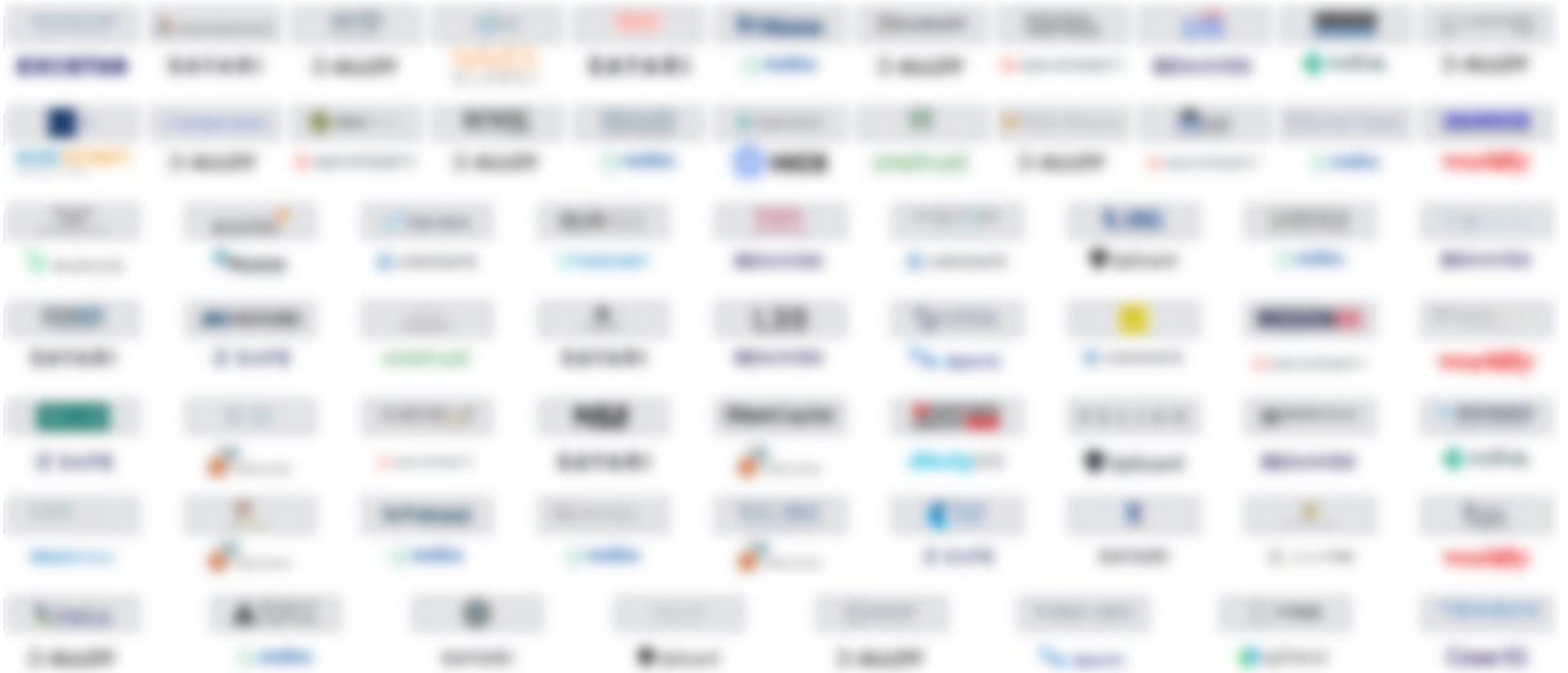
The investor field is broad and diversified.



To view the full sponsorscape, please contact Andrew.Atherton@HL.com.

GRC Sponsorscape (cont.)

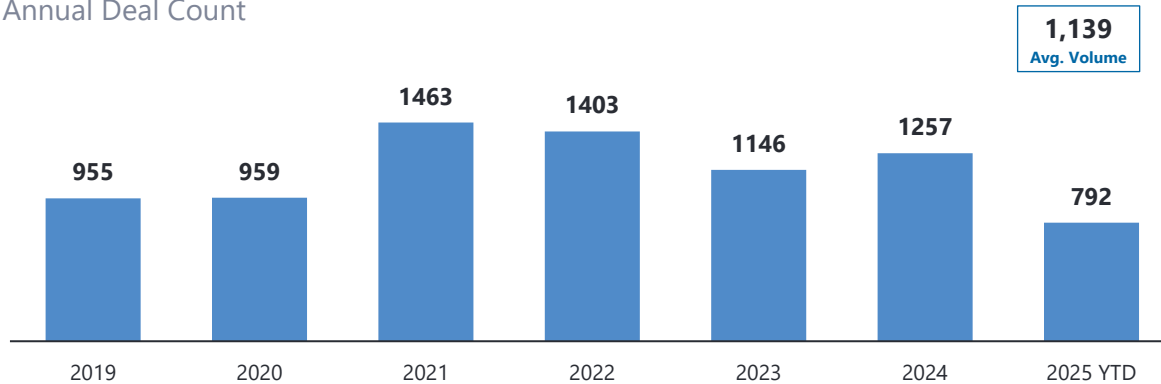
The investor field is broad and diversified.



Global GRC M&A and Capital Raise Transaction Volumes

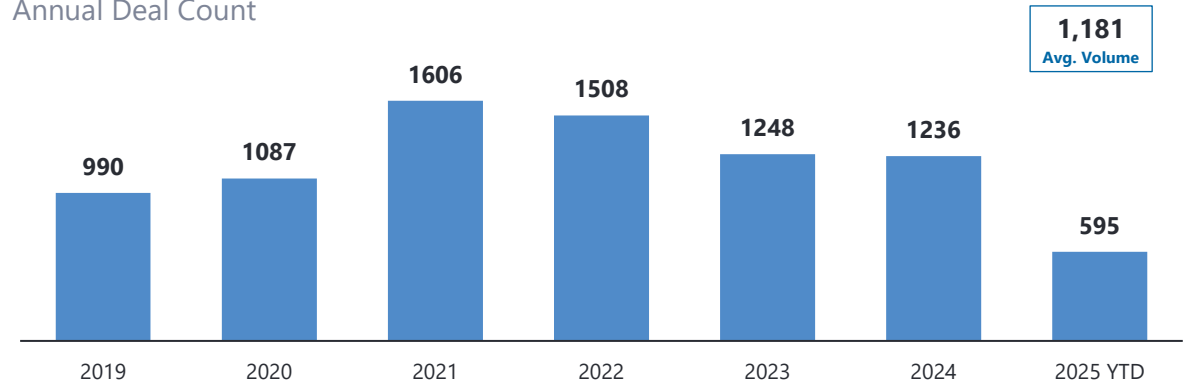
Mergers and Acquisitions

Annual Deal Count

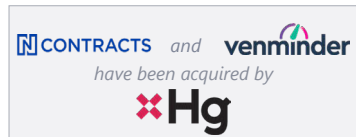


Growth and Venture Capital

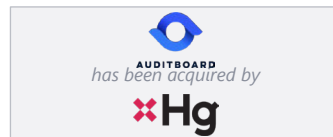
Annual Deal Count



Representative M&A Transactions (2024)



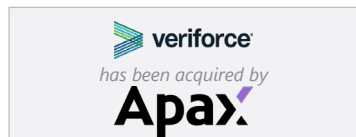
Risk and Compliance Management



Risk and Compliance Audit Automation



Supply Chain Risk Management



Supply Chain Risk Management and Compliance



Enterprise Risk and Performance Management



GRC Assets

Representative Growth and Venture Transactions (2024)



Regulatory, Risk, and Supervisory Reporting



Regulatory Advisory Solutions



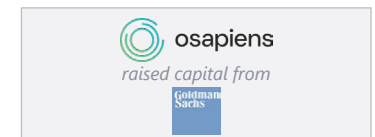
Regulatory Risk Management



Compliance and Security Automation



Cybersecurity and Data Compliance



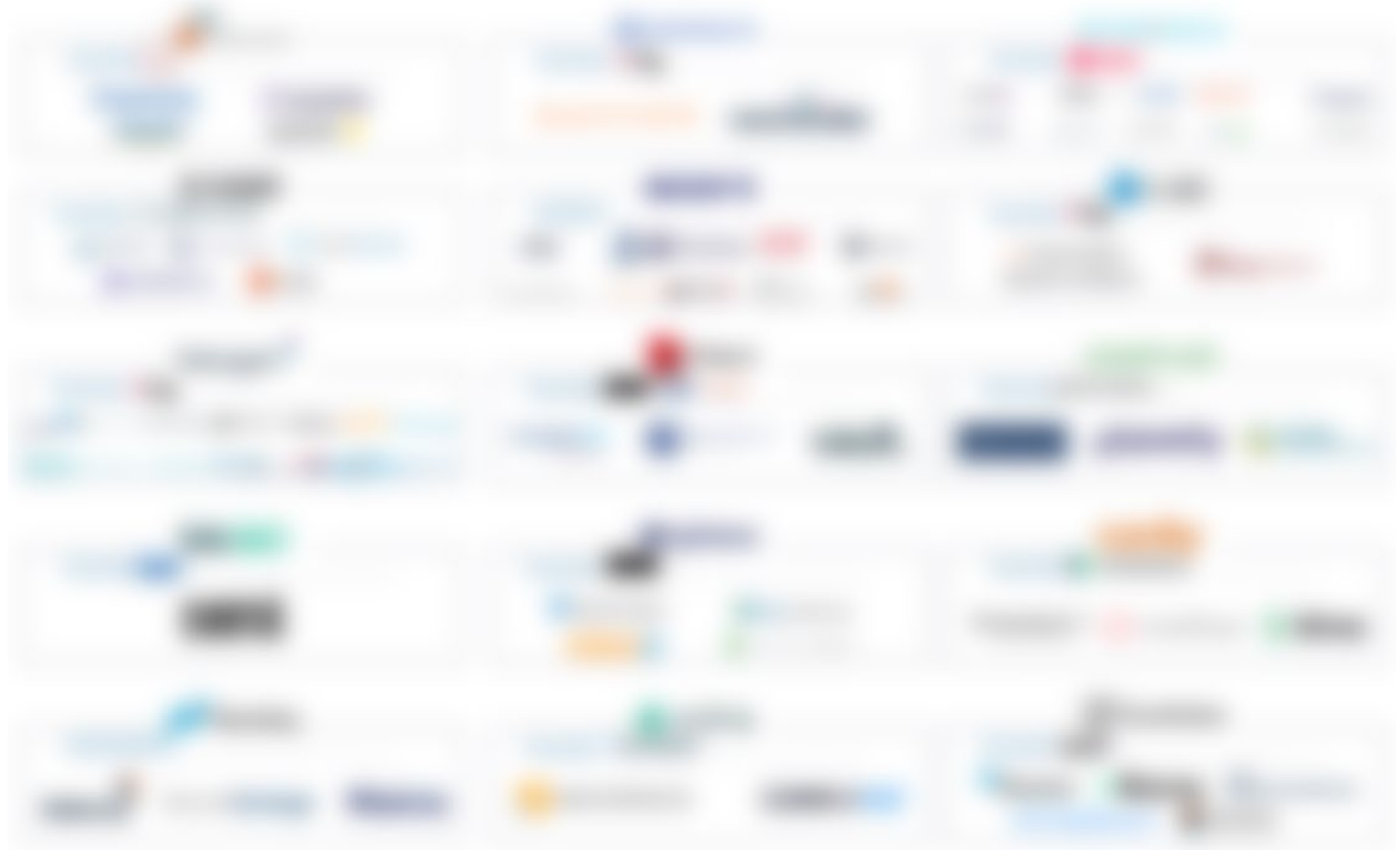
Operations Automation

Strategic Consolidation Remains Active

Major Platforms Bolster
Their Platforms
via M&A, and Emerging
Businesses Scale
Inorganically

To view the full consolidator map, please
contact Andrew.Atherton@HL.com.

Representative GRC Software and Data/Analytics Consolidators

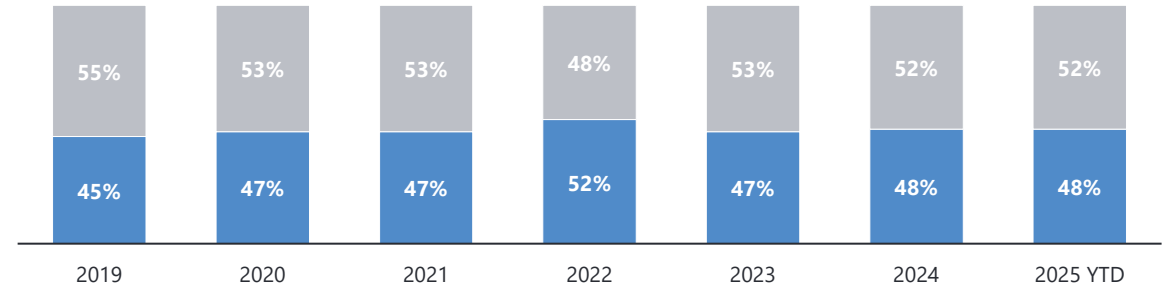
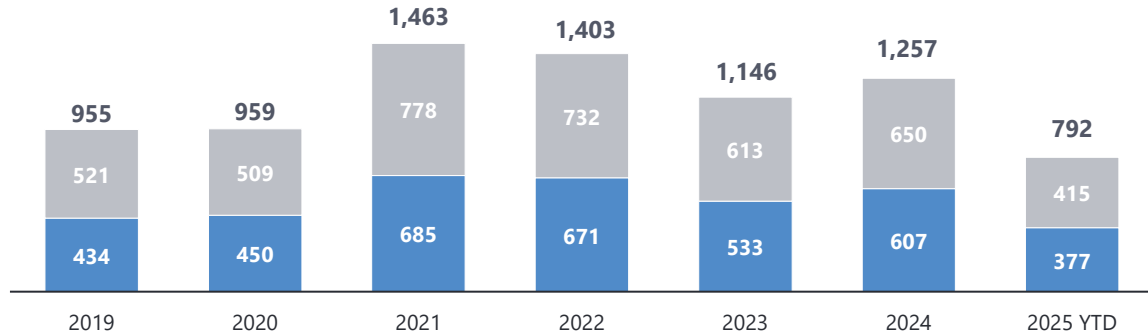


GRC Mergers and Acquisitions

Active, but stifled, consolidation.

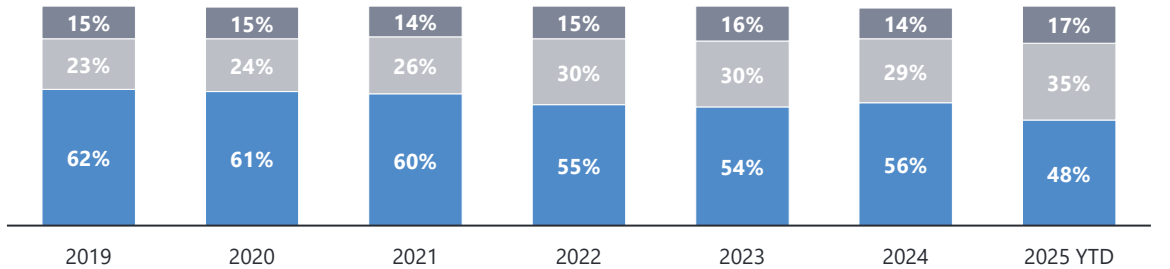
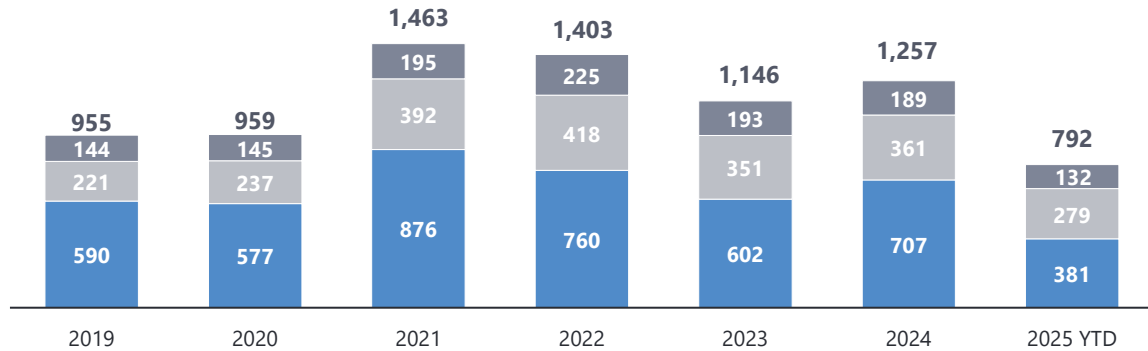
M&A Deal Count and Contribution by Type

■ PE Buyout and Bolt-Ons ■ Strategic Acquisition



M&A Deal Count and Contribution by Target Region⁽¹⁾

■ North America ■ EUR and U.K. ■ Rest of World



To view the full market map, please contact Andrew.Atherton@HL.com.

Featured Recent GRC M&A Activity (June 2025)

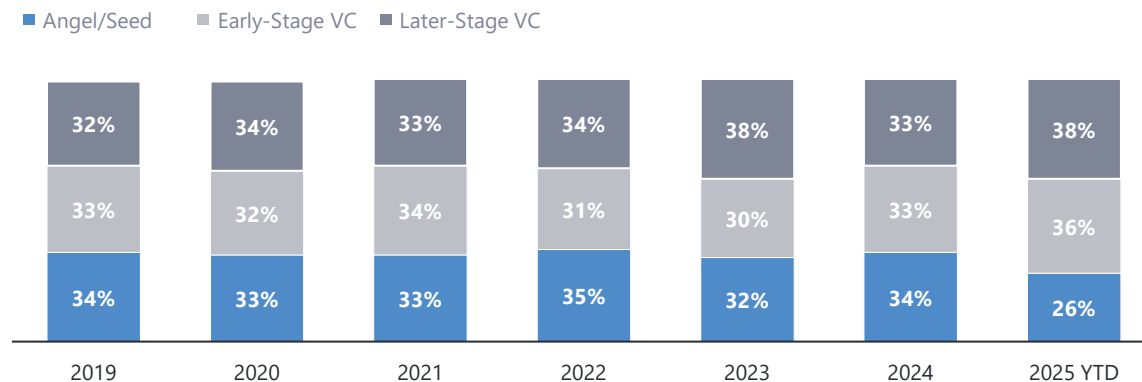
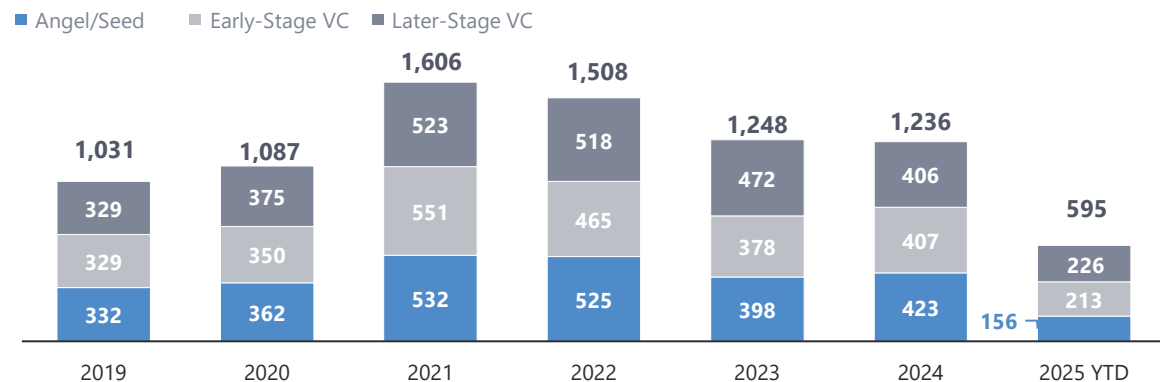
To view the full market map, please contact Andrew.Atherton@HL.com.

Featured Recent GRC M&A Activity (cont.) (June 2025)

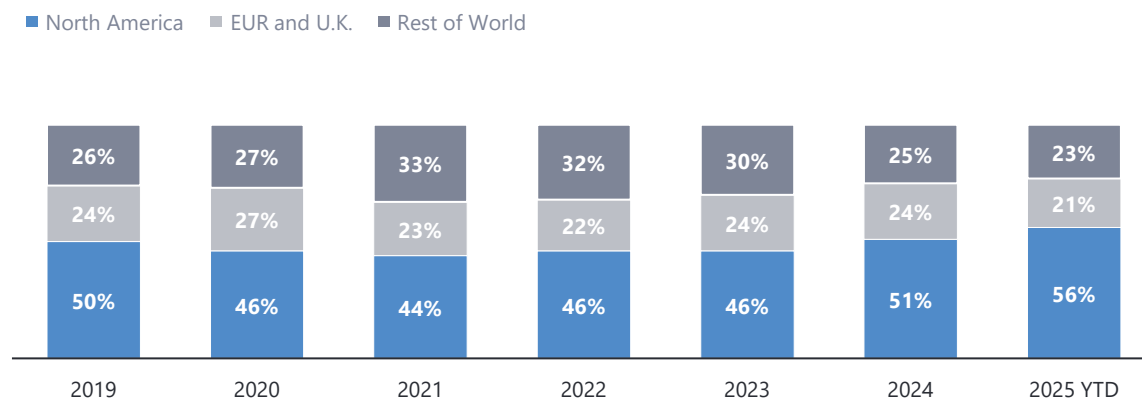
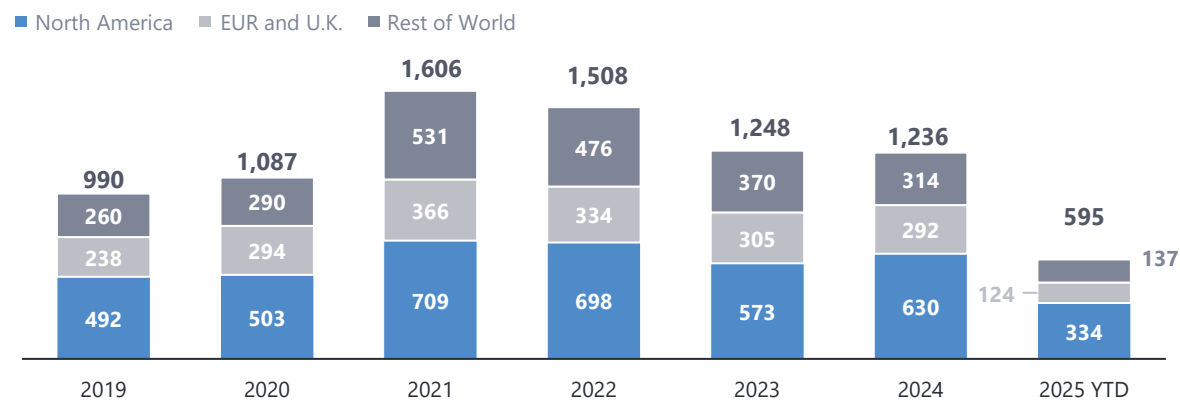
GRC Growth and Venture Capital

Funding continues but sinks below pre-COVID-19 deal volumes.

Growth and Venture Capital Deal Count and Contribution by Type



Growth and Venture Capital Deal Count and Contribution by Target Region



Featured Recent GRC Financing Activity

(June 2025)

To view the full market map, please contact Andrew.Atherton@HL.com.



Appendix: Houlihan Lokey
Platform Overview

06

Leading Independent, Global Advisory Firm

Houlihan Lokey is the trusted advisor to more top decision-makers than any other independent global investment bank.

2,677

Global
Employees

34

Locations
Worldwide

\$13.41B

Market
Cap⁽¹⁾

\$2.5B

Annual
Revenue⁽²⁾

~25%

Employee-
Owned

No

Debt



CORPORATE FINANCE

2024 M&A Advisory Rankings
All Global Transactions

	Advisor	Deals
1	Houlihan Lokey	415
2	Rothschild	406
3	Goldman Sachs	371
4	JP Morgan	342
5	Morgan Stanley	309

Source: LSEG (formerly Refinitiv).
Excludes accounting firms and brokers.

No. 1

Global M&A Advisor

Leading

Capital Solutions Group

FINANCIAL RESTRUCTURING

2024 Global Distressed Debt & Bankruptcy
Restructuring

	Advisor	Deals
1	Houlihan Lokey	88
2	PJT Partners	59
3	Rothschild	48
4	Lazard	44
5	Perella Weinberg	40

Source: LSEG (formerly Refinitiv).

No. 1

Global Restructuring Advisor

1,800+

Transactions Completed Valued at
More Than **\$3.8 Trillion** Collectively

FINANCIAL AND VALUATION ADVISORY

2000–2024 Global M&A Fairness Advisory
Rankings

	Advisor	Deals
1	Houlihan Lokey	1,243
2	Duff & Phelps, A Kroll Business	1,045
3	JP Morgan	1,020
4	UBS	792
5	Morgan Stanley	698

Source: LSEG (formerly Refinitiv).
Announced or completed transactions.

No. 1

Global M&A Fairness Opinion
Advisor Over the Past **25 Years**

2,000+

Annual Valuation Engagements

FINANCIAL SPONSORS COVERAGE

2024 Global Private Equity Financial
Advisors Rankings

	Advisor	Deals
1	Houlihan Lokey	232
2	Rothschild	189
3	Jefferies	175
4	William Blair	150
5	Morgan Stanley	147

Source: The Deal.

No. 1

Global Private Equity M&A
Advisor

1,900+

Sponsors Covered Globally

We Look Forward to Seeing You!

Recent and Upcoming GRC Events and Houlihan Lokey Conferences



ONE Houlihan Lokey Global Conference | New York

May 13–15, 2025
New York, New York



ISACA GRC Conference

August 18–20, 2025
New York, New York

[Click to Connect](#)



Enterprise Risk, Audit & Compliance Conference

September 8–9, 2025
Grapevine, Texas

[Click to Connect](#)



FinTech Week | London

October 6–10, 2025
London, U.K.

[Click to Connect](#)



Money20/20 | USA

October 26–29, 2025
Las Vegas, Nevada

[Click to Connect](#)



ONE Houlihan Lokey Global Conference | London

November 18–20, 2025
London, U.K.

[Click to Connect](#)

Additional Houlihan Lokey Coverage Reports

Q1 2025 FinTech Market Update

[View Report](#)



Capital Markets Technology Market Update

[View Report](#)



Q4 2024 Cybersecurity Quarterly Update

[View Report](#)



Office of the CFO Software Market Update

[View Report](#)



Disclaimer

© 2025 Houlihan Lokey. All rights reserved. This material may not be reproduced in any format by any means or redistributed without the prior written consent of Houlihan Lokey.

Houlihan Lokey is a trade name for Houlihan Lokey, Inc., and its subsidiaries and affiliates, which include the following licensed (or, in the case of Singapore, exempt) entities: in (i) the United States: Houlihan Lokey Capital, Inc., and Waller Helms Securities, LLC, each an SEC-registered broker-dealer and a member of FINRA (www.finra.org) and SIPC (www.sipc.org) (investment banking services); (ii) Europe: Houlihan Lokey UK Limited (FRN 792919), authorized and regulated by the U.K. Financial Conduct Authority; Houlihan Lokey (Europe) GmbH, authorized and regulated by the German Federal Financial Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht); Houlihan Lokey Private Funds Advisory S.A., a member of CNCEF Patrimoine and registered with the ORIAS (#14002730); (iii) the United Arab Emirates, Dubai International Financial Centre (Dubai): Houlihan Lokey (MEA Financial Advisory) Ltd., regulated by the Dubai Financial Services Authority; (iv) Singapore: Houlihan Lokey (Singapore) Private Limited an “exempt corporate finance adviser” able to provide exempt corporate finance advisory services to accredited investors only; (v) Hong Kong SAR: Houlihan Lokey (China) Limited, licensed in Hong Kong by the Securities and Futures Commission to conduct Type 1, 4, and 6 regulated activities to professional investors only; (vi) India: Houlihan Lokey Advisory (India) Private Limited, registered as an investment adviser with the Securities and Exchange Board of India (registration number INA000001217); and (vii) Australia: Houlihan Lokey (Australia) Pty Limited (ABN 74 601 825 227), a company incorporated in Australia and licensed by the Australian Securities and Investments Commission (AFSL number 474953) in respect of financial services provided to wholesale clients only. In the United Kingdom, European Economic Area (EEA), Dubai, Singapore, Hong Kong, India, and Australia, this communication is directed to intended recipients, including actual or potential professional clients (UK, EEA, and Dubai), accredited investors (Singapore), professional investors (Hong Kong), and wholesale clients (Australia), respectively. No entity affiliated with Houlihan Lokey, Inc., provides banking or securities brokerage services, nor is any such affiliate subject to FINMA supervision in Switzerland or similar regulatory authorities regarding such activities in other jurisdictions. Other persons, such as retail clients, are NOT the intended recipients of our communications or services and should not act upon this communication.

Houlihan Lokey gathers its data from sources it considers reliable; however, it does not guarantee the accuracy or completeness of the information provided within this presentation. The material presented reflects information known to the authors at the time this presentation was written, and this information is subject to change. Any forward-looking information and statements contained herein are subject to various risks and uncertainties, many of which are difficult to predict, that could cause actual results and developments to differ materially from those expressed in, or implied or projected by, the forward-looking information and statements. In addition, past performance should not be taken as an indication or guarantee of future performance, and information contained herein may be subject to variation as a result of currency fluctuations. Houlihan Lokey makes no representations or warranties, expressed or implied, regarding the accuracy of this material. The views expressed in this material accurately reflect the personal views of the authors regarding the subject securities and issuers and do not necessarily coincide with those of Houlihan Lokey. Officers, directors, and partners in the Houlihan Lokey group of companies may have positions in the securities of the companies discussed. This presentation does not constitute advice or a recommendation, offer, or solicitation with respect to the securities of any company discussed herein, is not intended to provide information upon which to base an investment decision, and should not be construed as such. Houlihan Lokey or its affiliates may from time to time provide financial or related services to these companies. Like all Houlihan Lokey employees, the authors of this presentation receive compensation that is affected by overall firm profitability.



Houlihan
Lokey

Corporate Finance
Financial Restructuring
Financial and Valuation Advisory

[HL.com](https://www.hl.com)