Hype Cycle for Legal and Compliance Technologies, 2023

Published 12 July 2023 - ID G00789644 - 110 min read

By Analyst(s): Lauren Kornutick, Ron Friedmann, Kerrie McDonald

Initiatives: Legal and Compliance Technology Planning and Strategy

Tech innovations grow increasingly important for corporate legal and compliance leaders facing significant workload demands and looming economic and regulatory headwinds. Leaders must close foundational tech gaps and carefully pursue innovation to deliver outcomes effectively for their business.

Strategic Planning Assumptions

- By 2024, legal departments will have automated 50% of legal work related to major corporate transactions.
- By 2025, legal departments will triple their spend on technology.
- By 2025, at least 25% of spending on corporate legal applications will go to nonspecialist technology providers.

Analysis

What You Need to Know

Over the past year, legal's workload has increased in both volume and complexity. Thinly stretched legal departments can leverage technology to build data foundations, increase their teams' efficiency and scalability, optimize spend, analyze bottlenecks and trends, enable more proactive legal service delivery and demonstrate legal's impact on broader business goals.

Legal departments falsely assume what innovation means. For example, technology is cost-prohibitive, one technology will suit all of their use cases and unproven, emerging technology will have an immediate impact. Legal takes a misguided approach to adopting innovation as a simple shopping exercise. Improvement requires shifting from assuming innovation is a quick fix to adopting a long-term strategy that includes both process improvement and innovation to better enable their team's capabilities.

To succeed, legal should focus on the operational capabilities and long-term business outcomes that innovation addresses — instead of short-term and one-off purchases.

The Hype Cycle

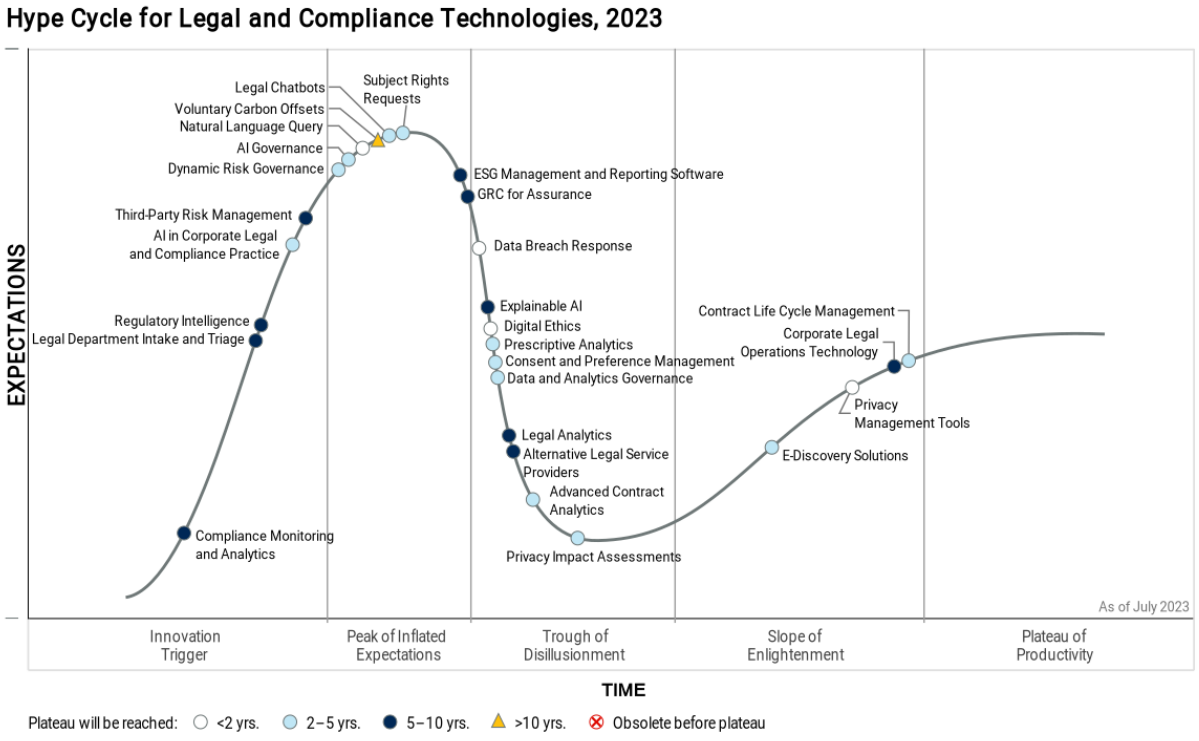
The most significant emerging technologies of 2023 are artificial intelligence (AI), machine learning (ML) and large language models (LLMs). These are expected to disrupt how legislators govern and industries work. Corporate legal and compliance leaders are intrigued by the potential to automate their high-volume, low-value tasks and are prematurely expecting the technology to perform.

Added regulatory complexity and mandates to demonstrate compliant and risk-aware organizations have enabled legal and compliance departments to pursue innovation. Legal and compliance leaders are investing in technology to support compliance monitoring and analytics; enterprise environmental, social and governance (ESG) reporting and management solutions; and governance, risk and compliance (GRC) for assurance.

In response to demand for new solutions to improve efficiency, vendors in dynamic markets aggressively promote new solutions, and early adopters uncover limitations in still emerging innovations. These midstage innovations also show the greatest movement in the Hype Cycle as organizations quickly find limitations (e.g., natural language query) or sour on overly ambitious claims (e.g., GRC for assurance leaders).

More mature innovations (e.g., corporate legal operations technology, contract life cycle management, privacy management tools) have seen more moderate movement. This movement reflects continued refinements in these platform offerings and their intended use cases, even while legal and compliance leaders struggle to effectively use these solutions.

Figure 1: Hype Cycle for Legal and Compliance Technologies, 2023



The Priority Matrix

The Priority Matrix shows the likely impact of innovations for legal and compliance leaders, comparing the potential benefit on the vertical axis to the timeline until mainstream adoption on the horizontal axis. Leaders should use this information as they consider potential impacts on their own organization and prioritize their investments.

AI, ML and LLM are expected to dramatically reduce the need for high-touch service models typical of most teams. Use cases for legal teams include improving productivity by reducing time spent on transactional legal work (e.g., contracts), litigation (e.g., legal research, e-discovery) and compliance (e.g., risk assessment, policy management). These technologies also promise to help legal teams quickly match internal customers to the right resources (e.g., chatbots).

Some market observers argue that these advancements will be transformative. However, we take a more conservative view, acknowledging the risks of these new advancements and their impact on legal teams to manage these risks. We estimate they will have a high benefit rating, foreseeable in a two- to five-year timeline. The early-stage innovation we see in 2023 will require refinement and iteration in solutions' design, accompanying processes and human factors to fully deliver its potential.

Table 1: Priority Matrix for Legal and Compliance Technologies, 2023

(Enlarged table in Appendix)

Benefit	*Years to Mainstream Adoption*			
↓	*Less Than 2 Years* ↓	*2 - 5 Years* ↓	*5 - 10 Years* ↓	*More Than 10 Years* ↓
Transformational		Dynamic Risk Governance	Legal Department Intake and Triage	
High	Data Breach Response Digital Ethics Natural Language Query Privacy Management Tools	AI Governance AI in Corporate Legal and Compliance Practice Contract Life Cycle Management Data and Analytics Governance E-Discovery Solutions Legal Chatbots Prescriptive Analytics Privacy Impact Assessments Subject Rights Requests	Alternative Legal Service Providers Compliance Monitoring and Analytics Corporate Legal Operations Technology ESG Management and Reporting Software Explainable AI Legal Analytics Regulatory Intelligence Third-Party Risk Management	
Moderate		Advanced Contract Analytics Consent and Preference Management	GRC for Assurance	Voluntary Carbon Offsets
Low				

Source: Gartner (July 2023)

On the Rise

Compliance Monitoring and Analytics

Analysis By: Lauren Kornutick

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

Compliance monitoring and analytics refers to a series of technology tools and an established risk management methodology that drive positive risk outcomes. Together, these resources quantify risk, mitigate risk in real time and monitor exposure to risk in real time.

Why This Is Important

Regulators are increasingly setting expectations that chief compliance and ethics officers (CCEOs) remediate a risk as soon as they identify them. Meanwhile, compliance functions face both a reduction in misconduct reporting and heightened expectations from regulators to develop systems for ongoing compliance control monitoring. To address these challenges, compliance leaders seek to leverage existing tools, processes and methodologies used by their peers in audit and risk.

Business Impact

Compliance monitoring and analytics tools enable the following:

- Management actions — Extend root cause analysis of incidents.
- Real-time reporting — Analyze data across systems.
- GRC for assurance — Automate risk governance and coordination.
- Process mining — Detect payment anomalies.
- Predictive modeling — Analyze patterns in datasets that can predict risk outcomes.
- Risk quantification — Prioritize risks by the magnitude of potential loss.

- Simulations — Simulate consequences for compliance violations to enable training retention.

Drivers

- The pace of regulatory change and increased regulation complexity is growing. CCEOs increasingly look for ways to track and integrate changes into the risk management process to make data-driven, risk-based decisions, and use data to drive a more informed risk-response strategy.
- Recent activity by global regulators signals a potential focus on executive risk oversight and monitoring. This puts pressure on internal and external reporting systems and leaves CCEOs looking for technology solutions to improve their governance oversight.
- The U.S. Department of Justice (DOJ) has also issued its Corporate Voluntary Self-Disclosure Policy. This policy provides CCEOs with incentives to disclose misconduct as soon as they are aware. The DOJ requires CCEOs to build mechanisms to monitor their most significant risks and remedy issues in near real time.
- CCEOs increasingly look for ways to measure the effectiveness of their programs and organization's policies. They aim to move toward metrics that demonstrate compliance gaps or show the measured impact of compliance program elements.
- CCEOs are looking to advance their use of technology to support this clear regulatory mandate from the DOJ and other regulators. Due to continued digital transformations in many organizations, modern compliance programs have access to more data than ever before, providing CCEOs with more opportunities to gain insight into compliance risk. The supply of new sources of data (e.g., in real time data lakes) make new modes of monitoring possible.
- Continued digitalization is giving compliance leaders unprecedented access to data and greater insight into compliance risk. New sources of data (e.g., in real-time data lakes) is enabling new, improved modes of monitoring.

Obstacles

- CCEOs may not know how to contextualize risk management processes used across assurance functions to their own risk assessment process

- Other barriers to success include technical and cultural obstacles to accessing the tools, low data quality, gaps in the skills required to analyze data and chief data and analytics officer (CDAO) prioritization of other functions.
- A more mature future vendor marketplace should help compliance leaders urgently address risk in real time to meet regulators' requirements.
- Buyers should be also wary of underperforming technology that promises all-in-one solutions.
- CCEOs should be aware that investment in multiple solutions may be prohibitively costly.
- The current methods CCEOs use for incident investigation do not align with the systemic approach to risk management required by regulators. To answer regulators' requirements, CCEOs must develop a continuous improvement mindset to consult, interpret and act on data.

User Recommendations

- CCEOs must move away from relying solely on discussions with management, whistleblower reporting and point-in-time audits to detecting misconduct in their highest risk areas in near real time.
- They should clearly document their risk assessment process and focus on prioritizing resources to the risk areas where they will have the most impact. CCEOs should also look for outliers in compliance metrics to identify hot spots.
- CCEOs should leverage existing risk management methodology from their assurance partners to understand their unknown risks.
- CCEOs should look to bring the risk management process to life by using technology that quantifies risk, monitors risk in real time and monitors exposure to risk in real time.
- CCEOs should prioritize multiple solutions, paired with a layer of data analytics, where appropriate. This will enable them to benefit from the technology market's breadth and from tools that integrate with each other and with relevant data.

Sample Vendors

Datricks; IBM; KonaAI; LogicGate; MetricStream; Microsoft; Tableau Software

Gartner Recommended Reading

2023 U.S. DOJ Update for Corporate Compliance Programs: Key Questions and Recommendations

Oversight, Disclosure and Risk Management: Compliance Program Implications of Recent DOJ and SEC Actions

Business Case for Implementing Process Mining

Market Guide for Third-Party Risk Management Solutions

Quick Answer: Use an Enterprise Data Strategy to Meet Risk Monitoring Goals

Legal Department Intake and Triage

Analysis By: Kerrie McDonald

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Intake and triage is a core component of any legal operating model. Intake and triage is the means by which corporate legal teams receive, assign, execute and manage legal work. It enforces work strategy and service delivery models, allowing legal departments to control what work they do and how it gets done. To drive business outcomes, legal departments must have intake and triage for internal and external work management.

Why This Is Important

Many legal teams have well-established intake and triage of external work (i.e., work handled by law firms or ALSPs); however, most legal departments lack systematic intake and triage for internal work (i.e., work handled by in-house legal professionals). Full visibility into internal and external work through systematic intake and triage allows more efficient operation, improved strategic planning and better talent management.

Business Impact

Intake and triage improves a department's ability to proactively manage legal work to drive business outcomes. By developing an effective intake and triage system, legal departments can:

- Improve turnaround times.
- Reduce administrative burden.
- Streamline communication with legal team members and business partners about work status.
- Prioritize work aligned to business goals.
- Align lawyer expertise to high-value work.
- Anticipate business partner needs based on identified sources of demand.

Drivers

- Current legal workloads are unmanageable, and lawyers are exhausted. Demand for legal services continues to expand, and workloads are rising in both volume and complexity — a trend that is expected to continue in coming years. Intake and triage helps address these pressures by allowing legal teams to control what work they do and how they do it and to develop more radical productivity-improving solutions at scale (e.g., automation of tasks and work types).
- Amid economic uncertainty, legal leaders are under increasing pressure to validate current resourcing and show the value they bring to the business. Without the data systematic intake and triage offers, legal leaders struggle to manage resources efficiently, identify continuous improvement opportunities and tell their value story aligned to business goals.
- Technology vendors that have historically focused on external matter management are expanding system functionality to account for internal work management needs. This enhanced functionality allows legal teams to manage work in purpose-built ways not previously possible without significant custom development investment. New legal workflow vendors are also emerging in this space to meet internal work management needs.
- Legal departments that have relied on systems cobbled together using email, forms, trackers and other collaboration tools are realizing these solutions do not hold the same automation potential as specialized legal workflow tools. While these cobbled together systems are good starter solutions, they require a high degree of administrative effort and are not scalable for the business's long-term needs.
- The advent of large language models (LLMs) holds promise to simplify intake and make it more accessible for legal and business teams, as an add-on to existing products or potentially as stand-alone, new products. Despite market excitement and pronouncements of immediate change, it likely will take two to five years for LLM to make a significant impact on intake.

Obstacles

- Legal departments have limited budgets, resources and time and believe they need to make a large investment in new technology before they can begin to standardize intake and triage.
- The business case for intake and triage solutions is not obvious and is often viewed as “soft.” Legal leaders need help articulating the broader business benefits of intake and triage to secure buy-in and encourage adoption.
- Moving from the traditional, free-for-all model for intake and triage of internal work to something more systematic is daunting for most legal teams. Most do not adequately address change management challenges such as resistance to providing structured metadata for internal work requests.
- Myths about intake and triage are pervasive throughout legal and business teams and are preventing progress that would drive better business outcomes. These myths include the belief that intake and triage will create more legal drag and ruin relationships between legal and the business.

User Recommendations

- Design new intake and triage processes collaboratively with the business. Involve others in requirements gathering, testing and development of new solutions. Along the way, invest resources to understand what myths and fears exist about moving to a standardized approach for intake and triage and proactively address them in the design, communication and training of new methods.
- Start small and build the business case for increased investment. Prior to deploying purpose-built technology, legal departments can use no- or low-cost starter solutions such as creating a central email box; funneling all requests through a single collaboration platform channel; or using Google Forms, Microsoft Excel or equivalent. These starter solutions address very real pain points while legal departments work toward increased automation through purpose-built technology platforms.
- Select metrics that will measure the effectiveness of the new intake and triage method. Proactively and consistently report on them.

Sample Vendors

Brightflag; BRYTER; Checkbox; Josef; LawVu; Mitratech; Onit; ServiceNow; Xakia

Gartner Recommended Reading

5 Myths About Legal Department Intake and Triage

Drive Strategic Success Through Business-Driven Legal Intake and Triage

Innovation Insight: Using Legal Department Intake and Triage to Transform Service Delivery

Tool: Guidance on Designing an Effective Legal Intake and Triage Process

5 Must-Ask Questions for an Effective Legal Intake Form

Regulatory Intelligence

Analysis By: Lauren Kornutick

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

Regulatory intelligence reflects the portfolio of solutions ranging from in-house staff teams and law firms to the marketplace for such solutions, including regulatory tracking, change management, and governance, risk and compliance (GRC) software. The market for regulatory intelligence software solutions is designed to support legal and compliance leaders in identifying new and emerging regulations and operationalizing changes brought on by regulatory change throughout their organizations.

Why This Is Important

Increasing regulatory oversight, geopolitical tensions and the COVID-19 pandemic have led to unprecedented regulatory change. Legal and compliance leaders have historically resourced their regulatory intelligence needs by tracking regulations manually within their departments or leaning on law firms for reactive support. Leading teams are reassessing their portfolio of regulatory intelligence resources, with many seeking alternatives from within the regulatory intelligence marketplace.

Business Impact

Business impacts include:

- Reactively resourcing regulatory needs with law firms and in-house resourcing has led many legal and compliance leaders to rethink cost and productivity inefficiencies, with no signs of a slowdown in the pace of change.
- Leading teams reassess their portfolio of regulatory intelligence resources for alternative legal service providers (ALSPs) and regulatory intelligence solutions (such as tracking and change management software) to improve cost efficiencies and find a long-term solution to resource their needs.

Drivers

- In addition to tracking routine regulatory obligations, such as Securities and Exchange Commission (SEC) rules, Department of Justice (DOJ) guidance, and export/import obligations, legal leaders are increasingly tasked with monitoring emerging legislation such as ESG commitments. All 10 of the world's largest economies have announced, or implemented, disclosure rules since 2021.
- Other global factors include disruptions caused by the ongoing Russian invasion of Ukraine putting pressure on the supply chain. Ongoing lockdowns have exacerbated the situation and have required legal and compliance leaders to navigate an increasingly complex system of requirements to consider.
- According to the 2023 Gartner Legal Budget and Efficiency Survey, nearly 40% of in-house specialist attorneys support regulatory compliance. This suggests that in-house legal teams have, in many cases, in-sourced their support to be better positioned to respond to regulatory change and reduce outside counsel spend.
- When surveyed on what has had the most impact on their work, legal leaders ranked legal and regulatory changes as second, just after increase in remote work throughout the organization. The increasing workload has contributed to employee burden and exhaustion, putting departments at risk of increased attrition and seeking out strategies for better managing increasing workloads brought on by volatility in regulatory regimes.
- Given increasing in-house burnout and the high costs of law firms in identifying and managing regulatory changes, many in-house teams are rebalancing their portfolio of regulatory intelligence services, looking toward ALSPs, and regulatory intelligence vendors. We have observed that legal departments use a mix of ALSPs, regulatory intelligence, and in-house and outside counsel to support keeping pace with change.
- According to a MarketsandMarkets report, the global regulatory reporting solutions market size will reach USD 1.6427 billion in 2030, growing at a compound annual growth rate (CAGR) of 18.8% over the analysis period.

Obstacles

- The regulatory intelligence solutions market is evolving. The market remains highly fragmented by available capabilities and covered terrains. We observe an unprecedented number of regulatory intelligence solutions available, including new solutions targeting industry verticals like financial services. There are three primary categories of software that can facilitate regulatory change — regulatory tracking, regulatory change management and GRC tools that integrate multiple systems.
- There is no single solution that can encompass tracking for all risk areas. Legal leaders face challenges ensuring regulatory tracking tools are tracking the right obligations and note that it is difficult to track global requirements with a singular tool.
- The regulatory intelligence market has been replete with merger and acquisition (M&A) activity in recent years, leading to many familiar vendors absorbing new capabilities. Yet, transparency into the risk terrains supported and the capabilities available remains clouded.

User Recommendations

- Reassess the portfolio of resources currently used to track and manage regulatory change and determine how human capital resources (law firms, in-house teams) can be best supported by regulatory intelligence solutions.
- Conduct a workload analysis to determine the amount of time and resources in-house staff is devoting to regulatory intelligence work. Identify how to best filter the changes through the organization by leveraging a regulatory intake process.
- Evaluate technology options for regulatory intelligence and horizon scanning tools based on terrain support and differentiating capabilities, including products packaged specifically for highly regulated industries such as financial services, healthcare and pharmaceutical, or specialized risk areas like ESG. Capabilities within regulatory change management software provide organizations the ability to track and implement regulatory changes.
- Regulatory tracking software can be integrated into a GRC tool to provide a similar workflow management as is available in the regulatory change management point solutions.

Sample Vendors

Assent; Clausematch; CUBE; IQVIA; LexisNexis; LogicManager; PerformLine; Propylon; SAI Global; Thomson Reuters

Gartner Recommended Reading

4 Paths to Staying Ahead of Regulatory Change

Market Guide for Regulatory Change Management Solutions

AI in Corporate Legal and Compliance Practice

Analysis By: Lauren Kornutick, Ron Friedmann

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

AI in corporate legal practice is focused on applying core AI technologies to legal practice, such as large language models (LLMs), natural language processing, text analytics, data science and machine learning. The most relevant areas are contract management, e-discovery, litigation management, legal research, drafting memos and briefs, compliance, and legal risk management.

Why This Is Important

Legal departments often lag behind other corporate functions in utilizing technology to control costs and improve outcomes. AI-based solutions, especially LLM models, are seen as a shortcut compared to conventional solutions without AI. But the relevance and readiness of the approaches in emerging solutions vary greatly. Buyers show increasing interest in the potential of AI-based solutions to automate manual tasks, discover new insights, increase operational efficiency and manage risk.

Business Impact

Use cases for AI that can improve legal department efficiency and efficacy include:

- **Intradepartment:** Contract management life cycle, legal spend, legal self-service (e.g., Q&A and automation).

- **Litigation:** Research, briefs, memos, insights, e-discovery search and analysis.
- **Intellectual property:** Filings, analysis and management.
- **Risk/compliance:** Regulatory tracking, control monitoring, reporting, analysis and policy management.
- **Privacy:** Data mapping and exfiltration.

Drivers

- **New use of LLM models:** The use of ChatGPT and similar LLM models has become a trending topic. OpenAI announced they will now allow third-party apps to build on their platform. With their new subscription-based model, it is likely additional vendors will use the technology to bring products to market.
- **Demonstrable law practice benefits:** Contract management and e-discovery have long been fertile grounds for AI. The advent of LLM promises benefits across multiple legal practices and tasks.
- **Growing number of specialist legal vendors:** Even before the advent of widely available LLM, many vendors offered products powered in part by AI. Numerous providers have already announced LLM-powered new or enhanced products.
- **Generative AI built-in to core productivity solutions:** Most enterprises use either Microsoft or Google productivity suites. With Microsoft Copilot and Google Cloud Duet AI releasing soon beyond beta customers, most legal departments will have access to LLM in their word processor, spreadsheet, and presentation applications.
- **Pent-up customer demand:** Advances in technology, including the use of AI, offer legal functions the opportunity to invest in new applications and emerging technologies to manage workloads more effectively and efficiently. However, few legal and compliance departments have invested in even foundational legal technologies.

Obstacles

- **Balance risk with benefits technology:** LLM models provide promise for organizations to improve efficiency. However, legal needs to balance risk with reward.
- **Unpredictability of outcomes:** AI-based solutions for legal practices that contain prepackaged “intelligence” may work well only in a narrow context. AI solutions can provide false information and raise privacy issues.
- **Successful deployments depend on more than technology:** Even where solutions work as intended, effective use also depends on the ability of the organization to make necessary changes. Few legal departments have the resources to do so.
- **AI-based legal technology may not be a complete solution:** Each legal practice area involves a range of activities where AI may have little or no role to play. This problem is compounded by poor understanding of the limitations of AI solutions, which leads to pursuing either unrealistic use cases or realistic use cases under unrealistic conditions.

User Recommendations

- **Build understanding:** Investigate the effectiveness and business impact of AI technologies in each area of legal practice, considering your specific use cases and context. Potential benefits include cutting costs, improving timeliness and quality, or managing risks.
- **Prioritize legal practice areas amenable to AI-based analysis:** Prioritize AI-based solutions in legal practice areas with high business impact and technical feasibility, such as contract management, e-discovery, and compliance. To increase the likelihood of a positive payback, vendor claims need to be tested in realistic situations.
- **Consider sourcing options beyond specialist AI vendors:** Include all sourcing options, including established legal technology vendors and law firms, as well as existing legal applications.
- **Align legal AI solutions with digital transformation plans:** Plan AI use within broader digital transformation plans, in order to leverage commonalities and secure executive support.

Sample Vendors

Apperio; Brightflag; Casetext; Compliance.ai; Litera; Luminance Technologies; Neota Logic

Gartner Recommended Reading

Legal Automation Use Cases

Building a Digital Future: Emergent AI Trends

Board Briefing: Understanding ChatGPT, Other Large Language Models and Their Risks

Get Ready for AI Regulation: 4 Critical Areas for the GC to Address

What Legal and Compliance Leaders Need to Know About Large Language Model Risks

Third-Party Risk Management

Analysis By: Lauren Kornutick

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

The third-party risk management (TPRM) market consists of vendors offering technologies to identify, assess, manage, monitor and report on risks associated with vendors, suppliers, distributors, agents, partners or other parties external to your organization. This market includes vendors, distributors, agents, partners or other parties whose products support a range of management workflows, across multiple risk terrains, including legal and compliance, privacy, IT and supply chain risks.

Why This Is Important

With the addition of new and sometimes high-risk third parties and the subsequent heightened oversight on TPRM from the board, stakeholders and regulators, many organizations are refining their TPRM efforts to improve risk management outcomes.

Business Impact

Observations include:

- **Limited end-to-end support across third-party life cycle:** Platforms that manage risks can provide competitive advantage and agility, but many vendors offer limited support for due diligence and monitoring.
- **Limited support across risk terrains:** Synthesizing risk metrics for multiple functional leaders remains out of scope for some.
- **Limited support for a primary functional leader of TPRM:** Solutions provide discrete support, restricting the primary owner's access to critical third-party risk information.

Drivers

- Forty-two percent of organizations believe third parties are more critical for their organization's profitability than they were just three years ago, according to our 2023 Gartner Cross-Functional Third-Party Risk Management Benchmarking Survey.
- Over half of respondents (51%) observed an increase in oversight on critical vendors in the last three years, a six percentage point increase over 2019 projections. In addition, more than 50% observed an increase in senior leader oversight of the network, while 46% indicated an increase in board oversight. Furthermore, there is no consensus on what to report to the board, an issue that is partly driven by a lack of reliable metrics.
- An intensified third-party regulatory environment endures as many national and state-level laws are beginning to be enforced in 2023. A recent focus from the U.S. Department of Justice on sanctions evasion legislation in the U.S. and EU (e.g., DORA, Critical Infrastructure Act) places pressure on clients to document their TPRM programs.
- Heightened scrutiny of third parties is being driven by a growing network of third, fourth and "nth" parties, and the business-critical role the network increasingly plays for the organization. This shift is driving corporate investment in TPRM systems to reduce the effort required to manage TPRM activities.
- The push for improved environmental, social and governance (ESG) initiatives has created a renewed focus on TPRM activities and application investments. This focus is pressuring organizations to rethink their due diligence requirements to encompass ESG-related criteria and perform greater scrutiny of third-party practices and nth parties. In response, over 29% of TPRM vendors are offering support for ESG-related third-party risks, and others are looking to enhance their solutions to provide ESG support, given the rapid growth of related regulations.

Obstacles

- The market for TPRM solutions remains highly fragmented, leaving companies to make compromises in their search for a best-fit solution. Organizations typically use a collection of solutions and risk domain insight that is leveraged by diverse teams throughout the enterprise.
- Because TPRM solutions offer discrete datasets, buyers may nest solutions alongside others across business functions and rely on a layer of data analytics in business intelligence or governance, risk and compliance software.
- An increased pressure on compliance functions from IT functions — which typically have a larger role in purchasing software — to lean on systems that are easier to integrate within existing technology systems, regardless of compliance requirements.
- TPRM offerings are climbing the Innovation Trigger and face many challenges ahead. Vendors must expand their solution offering to support the end-to-end risk management process.

User Recommendations

- Acknowledge that technology is a foundational part of the TPRM program to control potential gaps in risk terrain and risk processes. No technologies are all-in-one solutions that meet the needs of dynamic risk terrains and processes throughout the organization.
- Match the technology to the types of risk being managed and their priority. Many types of vendors address risk, but not all of them address the same types of risk. Additionally, there are functional differences between technologies that support front-end due diligence versus regular, ongoing monitoring of vendors and source validation.
- Layer TPRM into the existing enterprise technology ecosystem. Leaders should seek out foundational systems that satisfy the need for risk evaluation for primary risk owners and can scale TPRM processes in existing enterprise tools. They should also complement that foundation with solutions that support analytics, security rating services and other specialized services.

Gartner Recommended Reading

Third-Party Risk Management Benchmarking Report 2023

Research Index for Third-Party Risk Management Governance and Technology Solutions

Market Guide for Third-Party Risk Management Solutions

Prepare to Be a Better Buyer of Third-Party Risk Management Solutions for Compliance

Third-Party Risk Management Governance and Technology Investments: A Gartner Trend Insight Report

At the Peak

AI Governance

Analysis By: Svetlana Sicular

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

AI governance is the process of creating policies, assigning decision rights, and ensuring organizational accountability for risks and investment decisions for the application and use of artificial intelligence techniques. AI governance is part of adaptive data and analytics governance, addressing the predictive and generative nature of AI.

Why This Is Important

With AI now delivering value in the enterprise, data and analytics leaders observe that scaling AI without governance is ineffective and dangerous. Generative AI and applications, like OpenAI's ChatGPT, make AI governance a necessity, as using pretrained AI models billions of times sharpens risk concerns. The leaders want to balance AI's business value and the need for appropriate oversight. AI draws the attention of legislators worldwide, who mandate actions by clarifying AI governance priorities.

Business Impact

AI governance, as part of the organizational governance structure, enacts responsible AI, and provides common implementation and adherence mechanisms across the business ecosystem when it comes to:

- Ethics, fairness, and safety to protect the business and its reputation,
- Trust and transparency to support AI adoption via explainability, bias mitigation, model governance, operationalization, and collaboration norms and capabilities.
- Diversity to ensure the right technology and roles for each AI project.

Drivers

- AI governance is in the peak area of the Hype Cycle. Enterprise practitioners are taking steps toward establishing AI governance. Leading organizations in various industries establish AI governance by addressing standards for AI development and operations, providing best practices, guidelines for model management and monitoring, data labeling and interpretation, explainability, fairness, bias mitigation, security, and legal.

- Regulations around the globe target AI directly and affect AI practices indirectly, making AI governance goals more concrete. The U.S. Blueprint for an AI Bill of Rights provides governance pathways, from principles to practice. The objective of the EU AI Act is to "enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems." The Algorithmic Impact Assessment is a mandatory risk assessment tool intended to support the Treasury Board of Canada. Singapore's Model AI Governance Framework guides organizations in developing appropriate governance structures and mechanisms.

- Trust and transparency of AI solutions are crucial for AI adoption. The probabilistic and opaque nature of AI is new to audiences familiar with deterministic outcomes. AI governance can minimize misinterpretations of AI results by scrutinizing trust in data sources and the explainability of AI decisions. It provides specific testing and validation guidelines, differentiating "life-critical AI."

- AI governance is necessary to establish AI accountability. It is difficult to achieve because use cases differ in terms of their data, solution and outcome requirements. It outlines reactive responsibilities, actions and procedures in the case of unanticipated and unintended consequences. It ensures that ethics are considered for each use case.

Obstacles

- Often, AI governance is stand-alone from mainstream governance initiatives, which stalls its progress. The best method is to extend existing governance mechanisms to take advantage of recognizable policies and methods, such as in data governance. AI governance benefits from a conversation with the security, legal and customer experience functions.

- Many governance initiatives assume command and control. Instead, adaptive governance supports freedom and creativity in AI teams but also protects the organization from reputational and regulatory risks. Little or no governance in AI teams to facilitate freedom and creativity is an acceptable approach if this is a conscious governance decision.
- AI value assurance and model risk management are new in AI. While methods exist — for example, in the financial industry — they are largely unknown to others, and every governance organization is inventing its own.
- Technologies to support AI governance are fragmented and are often designed for a single industry.

User Recommendations

- Extend to AI your existing governance mechanisms, such as risk management or data and analytics governance.
- Establish and refine processes for handling AI-related business decisions. Blend processes, people and technology to succeed.
- Aim to align your AI governance framework with the laws and regulations in your jurisdiction(s) to directionally assure your efforts amid evolving AI-specific considerations. Gain agreement on AI risk guidelines that are driven by the business risk appetite and regulations.
- Decide on the organizational structure and accountability for propagating responsible AI — for example, what to centralize and what to do locally.
- Implement tools for AI review and validation. For each AI use case, require an independent AI model validator, a data scientist whose job is to assure model explainability and robustness. Have all parties in the process defend their decisions in front of their peers and validators.
- Ensure that humans are in the loop to mitigate AI deficiencies.

Sample Vendors

Arthur; Chatterbox Labs; Credo AI; DarwinAI; FICO; Google; IBM; Prodago; SAS; Weights & Biases

Gartner Recommended Reading

Applying AI — Governance and Risk Management

4 AI Governance Actions to Make a Swift Business Impact

Artificial Intelligence Primer for 2023

Dynamic Risk Governance

Analysis By: Malcolm Murray

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

Dynamic risk governance (DRG) is a new approach to risk governance, which is the critical task of defining the roles and responsibilities for risk management. As opposed to traditional risk governance models, such as the three lines of defense (3LOD), DRG makes risk management more tightly connected to strategy and more meaningful for the business. By customizing risk governance appropriately to each risk, organizations can better manage risks and lower their cost of assurance.

Why This Is Important

The world in which organizations are operating is getting more complex and uncertain, making strategic risk management more important than ever. However, it is also more difficult than ever. Risks are more interconnected and volatile, and can no longer be managed through antiquated risk governance frameworks. DRG offers an approach to rethink the organization's risk management, and manage risk as a strategic asset and liability.

Business Impact

DRG is quantitatively proven to lead to better risk management than traditional risk governance, such as 3LOD. It benefits risk and assurance functions (such as information security and compliance) by improving their collaboration, and benefits the business by reducing the "assurance fatigue" it often experiences from disconnected assurance efforts. DRG makes it easier for the organization to make risk aligned with strategy by applying risk appetite and tolerance to risk governance decisions.

Drivers

- While the risk landscape has evolved dramatically in the last few years, risk governance models have not. While risks have become dynamic and digital, risk management remains too inflexible and uniform. This makes DRG necessary to make risk management more meaningful for the business.

- As organizations have become more complex, risks have become more interconnected. Today's top organizational risks, such as supply chain, cybersecurity and third-party risk, all cut across large parts of the organization.

- The increased digitalization of organizations has led to the creation of new, fully digital risks such as ransomware, as well as an increase in the speed and volatility of other risks such as third-party risks. Risks now change in their nature more often and quickly.

- The rapid adoption of generative AI looks likely to lead to rapid changes in organizations, thereby adding increased uncertainty to many of the key risks in an organization. This includes cybersecurity risk, fraud risk and competitor risk.

Obstacles

- The lack of shared technology platforms and tools, where risk information and analytics are shared between all relevant functions, is an obstacle to DRG implementation. These platforms, such as GRC (governance, risk and compliance) and IRM (integrated risk management) systems are evolving, but there is still a lack of adoption and full implementation.

- A lack of maturity in terms of the collaboration between risk and assurance functions also obstructs the adoption of DRG. Due to organizational history, artificial lines of separation and regulatory pressure, the level of alignment of assurance efforts is still limited and has remained static over the last few years. Adopting DRG aids collaboration, but a higher initial level of risk management agility in the collaboration between functions would be helpful.

User Recommendations

- Apply differing levels of risk governance intensity to different risks, depending on the organization's strategic needs and tolerance for the specific risk.
- Assign accountable parties for risk management activities, based on their actual suitability for the task and not their theoretical function in the organization (e.g., first-, second- or third-line). Use risk-responsible, accountable, consulted and informed (RACI) charts to map this, in order to limit risk management activities to only the essential ones.
- Put digital risk management considerations first when designing and refining risk governance models to streamline risk governance with automation, and more centralized and coordinated data analytics usage.
- Make the board and senior management more involved in risk discussions by framing risk governance discussions around risk tolerance and risk appetite.

Gartner Recommended Reading

The "Risk Balance Sheet" — What It Is and Why You Need One

Use Dynamic Risk Governance to Align Risk Management to Strategy

Dynamic Risk Governance Is the New Risk Mandate

Ignition Guide to Piloting Dynamic Risk Governance

Achieving More Dynamic Risk Governance in Financial Services While Maintaining 3LOD Independence

Natural Language Query

Analysis By: David Pidsley, Rita Sallam

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

Natural language query (NLQ) allows business users to query information using business terms typed into a search box or chatbot, or via voice. Vendors' techniques differ in analytical complexity of queries, data volumes and types supported. These keyword searches translate terms into natural language questions using natural language processing technologies and LLM like ChatGPT. Some support querying structured data, and others enable semantic search of multistructured information.

Why This Is Important

- Business users need to make faster data-driven decisions and get context-enriched analysis that includes reasoning about location and time-sensitive situations.
- Despite significant advances in the usability of the point-and-click visual-based analytics, business intelligence (ABI) platforms and other knowledge bases, traditional access paradigms are still too hard for most business users.
- Flattening the learning curve for ABI platform users enables adoption by the remaining two-thirds of employees in organizations that do not use them.

Business Impact

NLQ drives adoption by nontechnical users, offering the ability to ask questions to gain insights, overcoming resistance to visual-based self-service analytics interfaces. NLQ is an increasingly important interface for analytic content development and consumption in data-driven decision making accessible to those unfamiliar with SQL. For data pipelines to enable multistructured analytics across a spectrum of structured data and unstructured content, NLQ can unify a multiexperience user interface.

Drivers

- Foundation models like BERT, large language models (LLMs) and ChatGPT see NLQ repositioned at the Peak of Inflated Expectations and a high benefit rating with less than 2 year time to plateau.
- Generative AI hype is accelerating NLQ capabilities with advanced text analytics and deep learning as catalysts of natural language technologies, including natural language generation (NLG) and NLQ. They enable two-way communication between the human questioner and the machine-generated answer based on the data.
- Demand for generative D&A is substantial with the substantial increase in entrants in 2023. Established ABI platform vendors responded to ChatGPT by improving support for and innovations in NLQ, which is a well-established critical capability of the platforms. Adoption continues to grow as NLQ awareness, availability and solution capabilities improve.
- Orchestration of the entire analytics workflow will increasingly become NLQ-driven and used to manage the analytics and application development activities.
- Augmented analytics capabilities make the analytics consumer of tomorrow a power user by today's standards. Most analytics consumers enter the data story workflow when viewing content that has been created from prepared components and existing data visualizations. Their interaction is typically followed by NLQ or conversational analytics.
- NLQ is becoming central to personalized, consumer-oriented user experiences that combine augmented analytics or automated insights into automated data stories, scenario analysis and conversational analytics. Analytics collaboration enables NLQ engines to learn from team-usage preferences.
- Increasingly mobile workforces using handheld devices and voice interfaces need NLQ to interpret geospatial questions and immediately deliver location-based answers and business insights as a best-fit map visualization. Geospatial analytics and algorithm advances enable NLQ to deliver geospatial reasoning of distance, route calculations and analytics about entities near, farther than or within a certain proximity or boundary, based on business-defined regions or geocoded reference data.

Obstacles

- Limitations in real-time type ahead search-bar suggestions can frustrate users, reduce usefulness and hinder adoption. Some users may not understand the implicit structure of underlying data, rendering queries uninterpretable by the NLQ parser.
- Unindexed datasets often hinder bringing search into an ABI platform. The effort/costs to map/model wide data are high, although generative AI is enabling NLQ of unstructured data to expand the scope and enable multistructured analytics.
- A substantial variety exists in the analytical complexity of queries, NLQ reasoning, support for suggestions for the next questions to ask, NLG to explain findings and support for large data volumes, structured and formats.
- Poor support of spoken languages beyond English, limited domain and industry ontologies, difficulty in configuration, and the need to be predefined in advance means optimizing NLQ implementations often requires customizing the platform and curating synonyms.
- Consistency is lacking for where users can ask questions across platforms and where implementations embed NLQ into the decision making or business process.

User Recommendations

- Help users adopt NLQ for decision making and orchestrating workflows.
- Promote NLQ-specific data literacy training for augmented consumers, business analysts and analytics developers.
- Assess the NLQ roadmaps of vendors and augmented analytics startups.
- Prioritize vendors based on how and what a platform learns (from activate metadata for personalization) via a proof of concept with real data and users.
- Evaluate how NLQ fits into analytics solution architectures. Involve IT in evaluation, data preparation and deployment of ABI platforms.
- Support multiple use cases with multiexperience UIs including evaluating enterprise conversational AI platforms.
- Invest in design thinking on dialogue flows and in competencies to connect conversational analytics to the ecosystem of APIs; for example, ABI platforms and insight engines that enable semantic search and analyzing results sets of wide data with multistructured analytics.

Sample Vendors

ConverSight; iGenius; Pyramid Analytics; Qlik; Tellius; ThoughtSpot

Gartner Recommended Reading

Magic Quadrant for Analytics and Business Intelligence Platforms

Is Your Business Intelligence Enabling Intelligent Business?

Quick Answer: What Are the Short-Term and Midterm Implications of ChatGPT for Data and Analytics?

Magic Quadrant for Insight Engines

Magic Quadrant for Enterprise Conversational AI Platforms

Legal Chatbots

Analysis By: Ron Friedmann

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Emerging

Definition:

Chatbots are domain-specific or task-specific conversational interfaces that use an app, messaging platform, social network or chat solution for conversations. Chatbots range in use-case sophistication from simple, decision-tree-based solutions, to implementations built on feature-rich enterprise conversational AI platforms. Unlike virtual assistants, chatbots are always narrow in scope. A chatbot can be text-based, voice-based (commonly referred to as a voice bot) or a combination of both.

Why This Is Important

Legal departments struggle to answer the ever-growing volume of questions from internal business clients. Their lawyers and staff cannot scale to answer more questions, but technology can. Consequently, chatbots, which can automate answering legal questions, hold much allure as a way to offload routine questions. While web and mobile interfaces are also options to automate legal advice, many people prefer the chat interface.

Business Impact

Legal chatbots' greatest potential impact is in improving client service while freeing legal professionals to focus on higher-value work. Even where chatbots cannot directly answer questions, they make it easier to ask the legal department questions and streamline the intake process by collecting relevant information. Furthermore, moving questions to chatbots supports more systematic tracking of demand — an area of weakness for many legal departments.

Drivers

Both demand- and supply-side factors are driving interest in, and eventual uptake of, chatbots. Demand-side factors include:

- The advent of widespread mainstream media discussion of ChatGPT and large language models (LLMs) starting in late 2022 has increased user interest in and expectations for "intelligent" chat.
- More regulations and periodic disruptions continue to drive a growing volume of client questions.
- Widespread use of Microsoft Teams, Slack and other collaboration products favor chat interfaces over email and voice. Adding a chatbot as a new channel in collaboration software makes it easier to ask legal questions than several existing channels. As chatbots reduce the barrier to ask questions, clients likely will ask more of them.
- As chat becomes a favored channel by consumers, behavior outside of work will carry over to the business world.

Supply-side factors include:

- The advent of multiple LLM will make developing chatbots easier and less expensive. Several legal tech vendors have already announced LLM capabilities. Historically, no-code platforms were the go-to solution for legal chatbots. In this period of rapid LLM evolution, the platform of choice remains uncertain.
- Legal departments face continued pressure to limit budget and headcount increases, especially given current economic uncertainty. This creates pressure to automate and standardize the lower end of work, which encourages building more chatbots.

- A trend to collect more data about the work the legal department does will be aided by the data generated from chatbots; legal departments will have better visibility into the most common questions asked. This will provide better direction on what additional chatbots to build.

Obstacles

- Widespread LLM availability is new and promising, but the ease of producing ones tailored to legal, with the requisite accuracy, remains uncertain.
- Even if LLM with “legal guardrails” become widely available and cost-effective, legal doesn’t know how valuable an out-of-the-box LLM will be versus one customized to the enterprise. Many legal departments would struggle to custom-train models because of data and resource limits.
- With some 2,000 chatbot-building options available (in the market at large, not necessarily targeted to legal) prior to numerous LLM coming to market, technology selection is difficult.
- With LLM likely becoming pervasive across functions in the medium term, the resources required to deploy them likely will first flow to corporate functions with higher-value use cases, such as sales or creative teams, than the legal department.

User Recommendations

- Track the vendor landscape for both general-purpose and legal-market specific LLM and the ability to tune models to specific domains or enterprises.
- Target any chatbot building efforts to high volume questions, such as employment law and nondisclosure agreements.
- Develop a strategy to organize internal content that could help train a LLM. For example, take steps to save documents in a central location or start to collect data about the work legal does in-house by moving toward a more centralized intake approach.
- Monitor the use of secure LLM elsewhere in the organization and, where license terms and resources permit, experiment with legal use cases.
- Ensure a plan is in place to keep the chatbots current, both technically and substantively.
- If lawyers or staff have the skill and want to build a chatbot to serve their clients or for their own development, free them up to do so.

Sample Vendors

BRYTER; Casetext (CoCounsel); Cognigy; Harvey; Josef; OpenAI; Rasa

Gartner Recommended Reading

Selecting Conversational AI Solutions for Chatbot and Virtual Assistant Initiatives

Magic Quadrant for Enterprise Conversational AI Platforms

Hype Cycle for Artificial Intelligence, 2022

Subject Rights Requests

Analysis By: Nader Henein

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Definition:

Subject rights requests (SRRs) are a set of legal rights that enable individuals to make demands and, in some instances, changes for clarity regarding the uses of their data. Organizations handling data must address SRRs in a defined time frame. These rights come in three categories — informative, corrective and restrictive. Their execution implicitly requires multiple capabilities of a modern privacy management program, such as personal data discovery, automation and mapping.

Why This Is Important

The percentage of the world's population with access to fundamental privacy rights will soon exceed that with access to clean drinking water. For security and risk management (SRM) leaders in digital enterprises, subject rights management is a standard requirement and a prerequisite for building trust. Vendors in the SRR market provide capabilities that serve organizations in many areas to deliver partial- or full-process automation from initial capture request to response.

Business Impact

The impact of poor or delayed response to SRR is threefold:

- Fines are levied by regulators for failure to comply. These rulings also mandate executing requests without delay.
- Trust between the organization and its customers is eroded. The loss of trust may also prompt requests such as deletion or limitations on processing.
- Long waits for a response negatively impact customer experience (CX) and sentiment.

Drivers

- Organizations must securely and effectively handle their customers' personal data to garner loyalty and avoid fines and litigation.
- Similar to "organic" or "cruelty-free" standards, privacy has become a conviction-based motivator, as individuals are making buying decisions based on how an organization handles their personal data.
- Large multinationals have adopted conviction-based motivators across their core products and supply chain.
- Fear of regulatory fines is the least of some organizations' concerns. Rapid mobilization through social media, followed by a violation of trust, has seen a mass consumer exodus far in advance of regulatory action.

Obstacles

- A sense within the leadership that the organization will not receive enough requests to justify upfront investment in resourcing.
- A degree of automation is needed to address SRRs at scale. It is important to maintain the capacity to respond in a time frame that complies with regulatory mandates and matches customers' expectations.

User Recommendations

- Ensure request fulfillment follows a repeatable and scalable process for compliance and efficiency.
- Nurture customer loyalty and support regulatory compliance by delivering a transparent, user-centric experience for SRR fulfillment.
- Establish the foundational metrics around SRRs. This should include the amount of time it takes to respond to a single request, the cost of a request — often calculated based on the person-hour rate of the team processing SRRs and any other resources involved — and the scale denoting the number of requests an organization can fulfill (given available resources) in the requisite time frame defined by applicable laws. Examples of time frames include 30 to 90 days under the General Data Protection Regulation (GDPR) and 45 to 90 days under the California Consumer Privacy Act (CCPA).
- Propose a level of automation in SRR fulfillment in line with the projected outlay. Identify areas within the response chain that would benefit from improvement.

Sample Vendors

DataGrail; Fair&Smart; IntraEdge; Mine; OneTrust; Osano; Securiti; WireWheel

Gartner Recommended Reading

Market Guide for Subject Rights Request Automation

State of Privacy — Regional Overview Across North America

State of Privacy — The European Union

State of Privacy — China

Voluntary Carbon Offsets

Analysis By: Chet Geschickter, Lauren Wheatley, Aapo Markkanen

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Voluntary carbon offsets are credits for capturing or eliminating a ton of carbon dioxide equivalent (CO2e) to fund carbon sequestering or reduction projects or processes. Offsets provide organizations a mechanism to achieve sustainability goals by funding projects that have a positive contribution to the environment and, therefore, balance out their GHG emissions. Carbon offsets do not include carbon credits from cap-and-trade markets, such as the EU Emissions Trading System.

Why This Is Important

Voluntary carbon offsets provide ownership of quantities of CO2e that are physically removed from the atmosphere by specific projects, assets or activities. Alongside direct emissions reductions by an enterprise, carbon offsets represent a very important tool to move the world economy to net zero by 2050. Large quantities of high-quality carbon offsets are needed to fund new carbon sequestration technology development and scale up proven approaches.

Business Impact

Enterprises can purchase and use carbon offsets within decarbonization pathways to net zero. Originators that sell carbon offsets can use funds to develop and scale projects that sequester carbon. Examples include protecting forest land, changing agricultural practices (for example, no-till farming) or distributing high-efficiency cooking stoves in low-income markets.

Drivers

- Corporate interest growth continues in carbon offsets as a component of decarbonization roadmaps that contribute to a low-carbon economy.
- Climate entrepreneurs, developers of new carbon removal technologies and parties with carbon sequestering resources are driving offset creation.
- Standards: (1) Article 6 of the Paris Agreement provides a framework to transfer carbon credits from one nation to another and a framework for international carbon markets. (2) Carbon registries establish criteria for qualifying projects and enable carbon offset purchase and sale. (3) Evolving best practices continue to address challenges associated with long-term sequestration — for instance, establishing a buffer or reserve for negative events such as forest fires that release carbon from tracts of sequestered land.
- Investment: (1) Corporate and private investor funding is increasing for development of carbon capture technologies and industrial projects. (2) Traditional energy companies are pursuing energy transition strategies. Some oil and gas companies are developing strategies to apply industrial engineering capabilities, geological expertise and underground storage assets for industrial carbon removal. (3) There is ongoing research and development of emerging industrial technologies, such as direct air capture, and nature-based solutions, such as cultivating kelp and agricultural practices like no-till farming and cover crops.
- Technology (emerging digital capabilities): (1) Blockchain can enable reliable and transparent issuance, distribution and pricing of tokenized carbon credits. (2) Remote sensing facilitates the monitoring of offset schemes for their real-life impact. (3) Offset marketplaces provide access to specific offset generating projects, activities and investments. Some vendors are also directly marketing offsets to individuals and organizations and facilitating their purchase.

Obstacles

- Methodologies to measure and verify the performance of offsetting schemes are immature.
- There is a shortage of verifiable and high-quality offsets and risks of double counting.
- Enterprises that rely on offsets before pursuing available renewable energy and energy efficiency options risk greenwashing.
- Industrial solutions such as direct air carbon capture or effluent capture are expensive, with limited availability.
- Viable underground storage options are geographically constrained.
- Protecting a forest does not increase sequestration, resulting in validity concerns.
- Longevity of carbon sequestration — e.g., shift in land usage can release carbon; deforestation occurs to increase agriculture resources.
- Speed of regenerating carbon offsets — e.g., newly planted trees can take 100 years or more to reach peak sequestration.

User Recommendations

- Appoint an executive to create an enterprise offset strategy and to establish board-level oversight.
- Use carbon offsets as an adjunct to, but not a replacement for, energy efficiency and renewable energy investments.
- Conduct due diligence and vet carbon offsets before purchase; ensure methodology, assurance and project controls are adequate.
- Assess longevity as only long-term carbon offsets have true value. Hence, think decades and centuries, not years.
- Set realistic expectations. Experimental technologies might not generate adequate volume at expected costs.
- Focus on offsets that are validated by reputable sources, such as longstanding carbon offset marketplaces with quality controls and verification programs.
- Differentiate between direct investment in new projects and storage capacities that increase carbon removals versus trading offsets in secondary markets that do not.
- Take early action to invest in long-term carbon offset projects as costs may increase over time.

Sample Vendors

Gold Standard; IncubEx; Pachama; Plan Vivo Foundation; Puro.earth; SOCIALCARBON; Supercritical; Sylvera; United Nations Carbon Offset Platform; Xpansiv

Gartner Recommended Reading

Building a Low-Carbon Energy Strategy

3 Practical Actions to Address Uncertainties in Pathways for Reducing GHG Emissions

Ignition Guide to Building a Net-Zero Greenhouse Gas (GHG) Emissions Roadmap

ESG Management and Reporting Software

Analysis By: Lillian Oyen-Ustad, Chet Geschickter, Aapo Markkanen, Simon Mingay

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

ESG management and reporting software is used to manage, measure and improve enterprise sustainability performance and provide a consolidated data collection method to report to ESG reporting standards and regulatory reporting obligations. Capabilities include support for data collection from diverse sources, analytics and decision support, KPI dashboards and visualizations, and identification of actions that advance ESG performance and ESG program management.

Why This Is Important

Enterprises are prioritizing transparency in response to stakeholder pressure — notably, regulators, investors and customers. Now that many enterprises measure and report ESG data, and have made public sustainability commitments, they need to make decisions and take actions to drive ESG performance. As such, executive leaders are looking toward systems that meet internal ESG program needs and external reporting requirements, and ensure verifiable, traceable data.

Business Impact

Fully featured and well-implemented enterprise ESG software can:

- Streamline ESG data collection and management.
- Improve ESG program management and visibility.
- Enable tracking and managing progress toward sustainability ambitions.
- Provide forecasting and decision-modeling tools for decision support.
- Streamline ESG reporting, enabling more focus on engagement and improvement activities.

Drivers

Market demand for enterprise ESG software is on the rise. Drivers include:

- Increased scrutiny and demands for transparency from external stakeholders, including the expectation of regulators to provide third-party verified data.

- A fragmented, complex and evolving regulatory environment, including regional variations in a regulatory approach.
- Investor pressure for data to inform ESG portfolio construction.
- Evolving sustainability ambitions and strategies among executive leadership, boards of directors and investors.

Corporate ESG programs are also growing in complexity and scope. Drivers include:

- Identification and inclusion of wide-ranging material ESG issues in program design.
- Challenges in identifying and collecting necessary data from diverse internal systems and external partners, especially up and down the supply chain.
- Challenges in balancing financial and economic considerations with ESG progress.
- Social commitments from an increasing number of corporations addressing diversity, equity and inclusion concerns.

Obstacles

- Responsibilities for ESG management are often spread across a range of functions and roles, making it difficult to collaborate, as well as identify material issues and data requirements.
- Diverse and distributed data often resides in a variety of systems and functions and across the value chain, complicating solution implementation.
- Shifting and uncertain regulatory requirements and fragmented standards complicate the process of establishing clear requirements.
- Executives often think they just need a solution for historical reporting to produce reports structured around specific standards. In reality, they need much better tools to provide operational insight and planning and modeling tools.
- The solution landscape is very dynamic and fragmented, with adjacent vendors expanding into ESG and pure-play vendors entering the market, making selecting the “right” vendor difficult.

User Recommendations

- Work with ESG stakeholders to identify material issues and data requirements as a basis to specify solution requirements. Consider how to instill a process that engages the organization to look for opportunities to improve ESG reporting and embed ESG into operational decision making.
- Review current reports that your organization produces, including corporate social responsibility reports, mandated regulatory filings and information for ESG rating services, and look for opportunities to integrate these and consolidate effort.
- Review standards, and identify relevant frameworks for your industry, such as the U.N. SDGs, CSRD, ISSB, TCFD, GRI and CDP.
- Assess needed data, source systems, and people and datasets that you will need to rely on to provide estimates and answers to questions about processes and practices.
- Improve the vendor selection process by focusing on vendors with experience in your industry, roadmaps and capabilities that align with relevant, evolving regulatory requirements.

Sample Vendors

Cority; Figbytes; IBM; Nasdaq; Sphera; Workiva

Gartner Recommended Reading

Market Guide for ESG Management and Reporting Software

Key Competitive Scenarios Product Managers Must Prepare for in Sustainability and ESG Software

Emerging Tech: Sustainability and ESG Software Will Underpin the New ESG Era

GRC for Assurance

Analysis By: Lauren Kornutick, Zachary Ginsburg

Benefit Rating: Moderate

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

The governance, risk and compliance (GRC) market for assurance leaders provides technologies that facilitate key areas of the risk management process associated with the diverse enterprise and compliance risks, and for which assurance leaders have oversight. These tools enable assurance leaders to gather insight from stakeholders panenterprise to facilitate the timely prevention, detection and remediation of risks.

Why This Is Important

Postpandemic risk landscape, shift to hybrid work, budgetary pressures, digitalization and the pace of regulatory change has complicated how assurance leaders manage risk. There has been increased scrutiny from regulators on management's duty of oversight for the risk management process. Additionally, nearly every framework and standard calls for a risk-based approach to managing risks. This drives complexity and pushes assurance leaders to lean on technology to support these initiatives.

Business Impact

GRC impacts the business as:

- The speed of regulatory change and scrutiny on management's duty of oversight requires assurance leaders to ensure new risks are identified, prioritized and mitigated in a timely manner.
- Assurance leaders are tasked with expanding responsibilities for oversight of risk domains managed by other teams and benefit from automating the coordination of assurance activities.
- GRC tools offer the prospect of expanding risk analysis capabilities and creating efficiencies in assurance workflows.

Drivers

- The need for assurance teams to handle an increase in data, information and risk management activities is driving them to increased automation and tracking in their workflows.
- Assurance leaders increasingly look to technology to help them integrate complex and rapid regulatory change into risk management processes.
- Financial services regulators increasingly scrutinize oversight of operational risk and resilience, cyber- and third-party risk management. This has left global financial institutions and their value chain turning to technology to meet new obligations, such as the EU's Digital Operational Resilience Act (DORA) and similar regulations in other locales.
- U.S. regulators have recently signaled potential focus on executive risk oversight and monitoring, putting pressure on internal and external reporting systems that could leave assurance leaders looking for technology solutions to improve governance oversight.
- Assurance leaders are under increased pressure from regulators, executives and boards to make data-driven, risk-based decisions and use data to drive a more informed risk response strategy. Thus, leaders are looking for ways to advance their technology use to support this clear mandate. In fact, 49% of assurance leaders plan to increase spend on risk and compliance technology, with 30% reporting an increase of over 10% in the coming year.
- Aligned assurance models that build connective tissue between compliance, risk and audit are becoming more common. Technology is needed to support these models to reduce silos of information. This provides a holistic view into risk management and can improve risk coordination and response outcomes.
- Assurance leaders desire to make use of data and analytics to assess probable risk impacts, analyze risk scenarios and continuously monitor risk exposure. GRC tools can support such analyses or enable them to be actioned in other tools.

Obstacles

- Despite the GRC market's growth to USD 39.4 billion in 2022, and expected growth to USD 76.4 billion by 2028 exhibiting a compound annual growth rate (CAGR) of 11.6% during 2023-2028, the market is highly homogeneous. There is little differentiation between products regarding core, functional capabilities (e.g., on risk coordination or workflow tracking). But, there is some differentiation among vendors in their ability to support continuous monitoring, probabilistic risk analysis and the use of emerging technology, such as AI, to support risk analysis.
- Vendors often market their tools to make them seem highly differentiated from competitors, but there is typically no differentiation in terms of core functionality. While differences do exist between offerings in terms of nonfunctional attributes (e.g., APIs), and niche domains and workflows, vendors often repackage the same tools for different buyer personas, confusing buyers.
- Buyers note that barriers to implementing GRC include cost, integrating technology and data, user adoption, and staff skills.

User Recommendations

- Given the breadth of the risk technology market, and the increasing readiness for tools to integrate with each other and relevant data, assurance leaders may find it more common that suites of solutions meet their needs better than single solutions. When scoping GRC technology, assurance leaders should remain focused on broad risk coordination and assessment capabilities (e.g., risk quantification, interdependency), and the ability to automatically consolidate controls across frameworks rather than leading with niche use cases.
- Buyers should beware of marketed specialized capabilities in modules (i.e., privacy, business continuity management [BCM], cyber), as these may not function as well as stand-alone solutions. They should consider whether GRC tools that have multiple prepackaged APIs for integrating other risk technologies would better suit their needs.
- Assurance leaders should evaluate vendors in this marketplace based on risk management methodology, ease of use, deployment models and integration with other applications, and data in the enterprise technology stack.

Sample Vendors

Archer; Diligent; MetricStream; NAVEX; OneTrust; SAI360; ServiceNow

Gartner Recommended Reading

Oversight, Disclosure and Risk Management: Compliance Program Implications of Recent DOJ and SEC Actions

Quick Answer: Use an Enterprise Data Strategy to Meet Risk Monitoring Goals

GRC Tool Adoption in ERM, Part 1: Use Cases, Satisfaction and Challenges

GRC Tool Adoption in ERM, Part 2: Vendor Selection and Implementation

Sliding into the Trough

Data Breach Response

Analysis By: Nader Henein, Bernard Woo

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Early mainstream

Definition:

Data breach response, augmentation and the associated disclosure are the activities required to assess and notify regulatory authorities and, depending on the impact, the affected individuals when personal data is compromised. Disclosure is mandated by omnibus laws, such as the European Union's General Data Protection Regulation (GDPR), Australia's Notifiable Data Breaches (NDB) scheme, or subject- and region-specific laws, like the individual U.S. state breach notification legislation.

Why This Is Important

Appropriate management of a breach impacting personal data can substantially reduce fines and potentially strengthen ties with affected consumers. It demonstrates that the organization is proactively taking ownership of the situation. However, delayed response, limited transparency and overly legal communications often elicit regulatory investigations, resulting in reputational damage and customer loss.

Business Impact

Data breach response can have a critical impact on an organization's resilience. Breaches often create significant chaos as key executive team members pivot from preexisting priorities to address the reputational, regulatory and likely financial impacts of the breach. Further, newer legislation imposes statutory sentences on company directors for inadequate or negligent handling of personal data.

Drivers

- Modern privacy regulations have raised the bar for data breach notification. When personal data is impacted, disclosure to a supervisory authority within days of discovery is often required.

- In the U.S., all 50 states have breach notification laws in place and many states, such as New York and California, have amended their laws in the past two years. Amendments typically expand the data in the scope of the legislation and the responsibilities surrounding disclosure.
- Regulatory evolution illustrates the need for organizational commitment and resource allocation.
- Organizations must constantly align the technical and operational elements of incident response (IR) with new legal and regulatory requirements.
- Elevating the capacity to disclose a data breach to regulators and potentially affected individuals in an accelerated time frame is something many organizations still need to prepare for.
- Though many organizations are driven by fine avoidance, incidents are bound to happen, and a well-developed response program can pay back in dividends with fine reductions of over 50%.
- An emerging trend is rapid consumer mobilization following an incident. The impact of mass customer exodus, often led by social media, is expected to suppress regulatory fines. Also, it does not offer the organization the option of an appeal through the courts.

Obstacles

- Establishing and testing a data breach program is an expense without an immediate return. It will pay off only if something goes wrong. This often causes the program to be deprioritized in place of more pressing or revenue-generating tasks.
- Data breach service retainers are not commonly available because of the variability and uncertainty of the type of breach, the data involved and the number of records that makes each breach scenario unique.
- Even with a strong program, the time to discover an incident can range from months to years — although it is improving over time.
- Tensions between the general counsel and chief information security officers (CISOs) over limiting information may become available through discovery following an incident. This could negatively impact the organization's capacity to effectively handle a breach.

- Data breach response requires a combination of technical acumens, such as forensics analysis of how the breach occurred, the number and type of records involved, and appropriate remediation. Data breach response must be paired with coordinated organizational processes.

User Recommendations

- Assess whether an incident will trigger regulatory actions. Meet the threshold for a privacy violation.
- Record and maintain the details about incidents (not just violations), as some jurisdictions have stringent record-keeping requirements.
- View data breach response as a multidisciplinary process involving documented procedures and simulated drills, such as tabletop exercises. Doing so will ensure tasks are well-defined and responsibilities are clear. The process should also involve coordination and transparency between various teams and integration into the larger IR training to provide breach disclosure and rapid response requirements.
- Augment your organization's ability to address data breaches in an efficient and timely manner to fulfill regulatory and data-subject disclosure requirements.

Sample Vendors

BigID; BreachRx; Canopy; OneTrust; RadarFirst; Securiti

Gartner Recommended Reading

Toolkit: Cybersecurity Incident Response Plan

Toolkit: Security Incident Response Roundtable Scenario for Privacy

Explainable AI

Analysis By: Peter Krensky, Sumit Agarwal

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Explainable AI (XAI) is a set of capabilities that describes a model, highlights its strengths and weaknesses, predicts its likely behavior, and identifies any potential biases. It can clarify a model's functioning to a specific audience to enable accuracy, fairness, accountability, stability and transparency in algorithmic decision making.

Why This Is Important

XAI gives visibility into how a model arrived at a particular decision. This helps in building trust, confidence and understanding in AI systems. In highly regulated sectors such as insurance or banking, regulations directly or indirectly mandate the need for model explainability to properly manage model risk.

Business Impact

XAI is the responsibility of both vendors (data scientists and solution developers) and also of end-user organizations that consume them. Not supporting this capability puts businesses and decision making at risk. However, different levels of explainability are required for customers, the organization's IT and management, society, and regulators to direct AI governance.

Drivers

- The lack of model transparency or interpretability among model users, managers and consumers impacted by models' decisions severely limits an organization's ability to manage AI risk. Fairly or unfairly, consumers hold the originating organization responsible for the performance and behavior of AI.
- Not ensuring explainability invites model risk that can lead to financial loss, poor business and strategic decision making, or damage to organizational reputation.
- A lot of organizations are shifting to augmented decision-making capabilities with the use of AI models. As a result, they should be able to explain how an AI model arrived at a particular prediction or decision.
- XAI capabilities are prebuilt into both platforms and innovations in the open-source community to explain and interpret models are on the rise.
- Ethical and moral considerations need to be accounted for while relying on augmented decision making, often supported by thorough governance and auditing capabilities for these models.
- New regulations and legal interventions are taking place that mandate the use of explainable AI methodologies.
- Explainable models also help with attrition, so data scientists who quit the job do not leave black boxes behind them. Models that are interpretable help business audiences gain trust in AI.

Obstacles

- Explainability is often confused with ML interpretability. Although the latter serves data scientists, the former applies to different personas interacting with the AI life cycle.
- XAIs are often looked at as a task or a step required while creating AI projects toward the end of the AI life cycle, but they have to be continuous and tested throughout training, development and production phases.
- An inherent lack of trust exists in AI systems that keeps organizations from adoption, since they're simply not aware of XAI techniques or frameworks.
- Explainability tools are fragmented, and XAI is often consumed in an oversimplification such as showing feature importance to end users. Although that approach works in the beginning, XAI is much wider than that, and requires a deep understanding of the subject.
- Organizations that focus on the accuracy of the models rather than on the interpretability stall their decisions on creating a more explainable AI.

User Recommendations

- Define a range of actions that can be taken independently that identify unacceptable results and that flag those results for human intervention. Minimizing the number of incorrect results derived from AI is critical, because users will lose trust in a poorly performing system.
- Educate, train and foster ongoing conversations with key stakeholders, including line-of-business managers, legal and compliance, to understand the AI model's explainability requirements, challenges and opportunities.
- Strive for XAI for each model along the dimensions of business, data, algorithms, models and production.
- Accept deficiencies in explainability as a natural consequence of systems becoming increasingly complex. Document notable deficiencies or potential biases so that they can be used to make corrections in the future.
- Establish the role of AI model validator, a data scientist whose job is to ensure that models are explainable and robust, and meet all possible constraints.

Sample Vendors

Dataiku; EazyML; Fiddler AI; Google; H2O.ai; IBM; Microsoft; Modzy; Superwise; TruEra

Gartner Recommended Reading

Innovation Insight for Bias Detection/Mitigation, Explainable AI and Interpretable AI

Top 5 Priorities for Managing AI Risk Within Gartner's MOST Framework

Market Guide for AI Trust, Risk and Security Management

Incorporate Explainability and Fairness Within the AI Platform

Digital Ethics

Analysis By: Pieter den Hamer, Frank Buytendijk, Svetlana Sicular, Bart Willemsen

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Digital ethics comprises the systems of values and moral principles for the conduct of electronic interactions among people, organizations and things. It applies to areas such as AI, data and analytics, and social media.

Why This Is Important

Digital ethics, especially around topics like privacy, bias, polarization and veracity, is a concern to many. The voice of society is getting louder, with responsible AI coming into sharp focus for individuals, organizations and governments. People, increasingly aware that their data is valuable, are frustrated by lack of transparency, misuse and breaches. Organizations are acting to mitigate ethical risks around data, AI and other digital areas, while more governments are encouraging and regulating responsible use of these in digital society.

Business Impact

Digital ethics strengthens an organization's positive influence and reputation among customers, employees, partners and society. Areas of business impact include innovation, product development, customer engagement, corporate strategy and go-to-market. Intention is key. If ethics is simply a way to achieve business performance, it comes across as disingenuous. The goal to be an ethical organization serves all parties and society more broadly, and leads to better business trust and performance.

Drivers

- The media is frequently featuring high-profile stories about the impact of data, AI and other technology on business and society at large. Board members and other executives are increasingly sharing concerns about the unintended consequences of innovative technology use.
- For many technologies, ethics was often an afterthought. However, with the emergence of artificial intelligence, the ethical discussion is now taking place both before and during a technology's widespread implementation. AI ethics aims to establish responsible use of AI and to harness AI's growing powers.
- The current hype around generative AI, including ChatGPT and similar alternatives, is raising awareness about ethical and legal issues surrounding the veracity and (intellectual) ownership of data, including training data. In addition, the potential impact of inaccurate, misleading or insensitive output is fueling ethical concerns.
- Government commissions and industry consortia are actively developing guidelines for ethical use of AI. Examples include the EU's AI Act, the Netherlands' Fundamental Rights and Algorithm Impact Assessment (FRAIA), and the U.S.'s National AI Research Resource (NAIRR) Task Force and National Artificial Intelligence Initiative to advance trustworthy AI in the U.S.
- Over the past few years, a growing number of organizations declared their AI ethics principles, frameworks and guidelines. Many are in the process of going from declaration to execution.
- Universities across the globe have added digital ethics courses and have launched programs to address ethical, policy and legal challenges posed by new technologies.
- Digital ethics is expanding to address concerns about rising energy consumption. In the case of nonrenewable energy, it is focusing on the carbon footprint of digital technology (particularly, machine learning and blockchain).

Obstacles

- Because of the ambiguous, pluralist and contextual nature of digital ethics, organizations often struggle to operationalize it and expend significant effort to implement best practices.
- Organizations see digital ethics as a moving target because of confusion around society's expectations. An organization's position and beliefs may even steer digital ethics against the majority's opinion.
- Digital ethics is too often reactive, narrowly interpreted as compliance, reduced to a checklist, confined to technical support for privacy protection, and/or viewed only as explainable AI.
- AI ethics is currently the main focus of digital ethics. Supporting technology (e.g., to protect privacy or mitigate bias) needs to mature further and apply to the broader scope of ecosystems rather than singular technologies.
- Across people, regions and cultures, opinions differ on what constitutes "good" and "bad" and what doing the right thing means. Even in organizations that recognize ethics as an important issue, consensus between internal and external stakeholders (such as customers) is sometimes illusive.

User Recommendations

- Identify specific digital ethics issues and opportunities to turn awareness into action.
- Discuss ethical dilemmas from diverse points of moral reasoning. Anticipate and account for ethical consequences. Ensure that you are comfortable defending the use of a technology, including any unintended negative outcomes.
- Elevate the conversation by focusing on digital ethics as a source of societal and business value, rather than simply focusing on compliance and risk. Link digital ethics to concrete business performance metrics.
- Ensure that digital ethics is leading and not following the adoption of new, transformative technology such as AI. Address digital ethics upfront "by design" to create methods that identify and resolve ethical dilemmas as early as possible.
- Organize training in ethics, and run workshops to create ethical awareness within all AI initiatives. These should emphasize the importance of an ethical mindset and clear accountability in AI design and implementation.

Gartner Recommended Reading

Tool: Assess How You Are Doing With Your Digital Ethics

Tool: How to Build a Digital Ethics Curriculum

AI Ethics: Use 5 Common Guidelines as Your Starting Point

How to Manage Digital Ethical Dilemmas

How to Operationalize Digital Ethics in Your Organization

Prescriptive Analytics

Analysis By: Peter Krensky

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Prescriptive analytics is a set of capabilities that specify a preferred course of action and, at times, take automated actions to meet a predefined objective. The most common types of prescriptive analytics are optimization methods, a combination of predictive analytics and rules, heuristics, and decision analysis methods. Prescriptive analytics differs from descriptive, diagnostic and predictive analytics in that the technology explores multiple outcomes and provides a recommended action.

Why This Is Important

Prescriptive analytics capabilities either automate or augment decision making to improve business responsiveness and outcomes. From a “purist” perspective, the term “prescriptive analytics” is a broad category with little hype, encompassing components with varying positions across the Hype Cycle and various levels of maturity. Such components include optimization, rules combined with predictive techniques and decision intelligence. The increasing focus on composite AI is further propelling the importance of prescriptive analytics.

Business Impact

Prescriptive techniques support:

- Strategic, tactical and operational decisions to reduce risk, maximize profits, minimize costs, or more efficiently allocate scarce or competing resources
- Recommendations for a course of action that best manages the trade-offs among conflicting constraints and goals
- Exploration of multiple scenarios and comparison of recommended courses of action
- Strategic and tactical time horizons as well as real-time or near-real-time decision making

Drivers

- Prescriptive analytics benefits from maturing and expanding data science initiatives, better algorithms, more cost-effective cloud-based computing power, and a substantial increase in available data.
- With improvements in analytics solutions, data quality and user skills, prescriptive analytics will continue to advance.
- The increasing popularity of graph techniques provides a great substrate for prescriptive analytics. Graph techniques highlight early signals, causality links and paths forward, facilitating the implementation of decisions and actions.
- Demand is shifting away from traditional reactive reporting to actionable, proactive insight, placing greater focus on optimization, advanced techniques, composite AI and prescriptive analytics.
- AI platforms and decision management tools increasingly include prescriptive techniques, driving user acceptance and potential value to the organization.
- Prescriptive analytics continues to evolve, ranging from relatively straightforward rule processing to complex simulation and optimization systems. To respond to ever-greater complexity in business, organizations need more advanced prescriptive analytics and composite AI (e.g., combining rules/decision management with machine learning or optimization techniques).
- Organizations continue to improve, optimize and automate their decision making by applying decision intelligence and decision modeling. Prescriptive analytics is a key enabler of this approach.

Obstacles

- Expertise on how and where to apply prescriptive techniques is lacking.
- The industry lacks formal operationalization methods and best practices.
- Historically, organizations have required separate advanced analytics software specializing in prescriptive techniques. Such point solutions offer little cohesion across the analytics capability continuum from descriptive to diagnostic to predictive to prescriptive.
- Even established use cases can fall victim to common data science challenges, such as data quality issues, bias and talent shortages.
- Although it is a necessary competency, prescriptive analytics does not automatically result in better decision making.

User Recommendations

- Start with a business problem or decision involving complicated trade-offs, multiple considerations and multiple objectives.
- Explore the breadth of prescriptive analytics approaches and decision models available. Identify the ones that best cater to your specific business problems and skills.
- Analyze packaged applications to determine which provide specific vertical or functional solutions, and which service providers have the necessary skills.
- Make sure that the enterprise is willing to rely on analytics recommendations, by gaining buy-in from stakeholders — ranging from senior executives to frontline workers carrying out the recommended actions.
- Ensure that your organizational structure and governance program will enable the enterprise to implement and maintain functional, as well as cross-functional, prescriptive analytics recommendations.

Sample Vendors

AIMMS; Amazon Web Services; FICO; Frontline Systems; Google; Gurobi Optimization; IBM; Microsoft; River Logic; SAS

Gartner Recommended Reading

Combine Predictive and Prescriptive Analytics for Better Decision Making

Innovation Insight for Composite AI

How to Use Machine Learning, Business Rules and Optimization in Decision Management

Consent and Preference Management

Analysis By: Tia Smart

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Consent and preference management platforms consolidate end-user choices regarding how their personal data should be handled. Choices are synchronized across legacy, active and incoming repositories, both on-premises and in the cloud. The intent is to extend visibility and control to digital visitors, allowing them to determine and change how much of their data to expose, to whom and for what purpose. This also empowers marketers to respect customers' choices with a minimum of manual overhead.

Why This Is Important

Protections for personal data collected digitally continue to expand across the globe as more countries and U.S. states consider legislation similar to or stronger than GDPR, CCPA, CPRA and CPA. Technologies and organizations must quickly adapt to the global transformation. Consent and preference management platforms (CPMPs) empower organizations to comply with new laws, preserve and extend essential capabilities, and demonstrate to customers and stakeholders that they care about privacy.

Business Impact

- As new legislation is introduced worldwide, organizations must use CPMPs to demonstrate to consumers that they value their privacy and are in compliance to avoid costly violations and consumer mistrust.
- Protecting your organization from compliance violations while maintaining the ability to utilize customer data for business purposes can be technically and operationally challenging. CPMPs help to address these issues.

Drivers

- **New laws and variations in legislation.** With additional countries and regions seeking to implement their own consumer privacy laws, tracking laws in each country and region is a tedious but integral task to ensure compliance. CPMPs address specific requirements, such as auditing websites, enforcing consent choices and making data available for subject rights requests.
- **Reliance on first-party data.** The shift to an increased dependence on first-party data instead of third-party cookies forces organizations to reevaluate the enterprise's data structure. Managing consent and preference choices throughout the ever-convoluted enterprisewide structures takes time, and some CPMPs try to solve this. CPMPs' importance is ever more apparent in countries like the U.S., where implicit consent is still allowed in most states. Organizations need to take a state-by-state approach or risk messing up direct marketing opportunities available to them.
- **Societal norms and consumer expectations.** Consumers now expect to have control over their personal data as well as transparency from organizations on how it is used. However, consent flow banners and dialogues can significantly downgrade user experience, driving the need for better design solutions enabled by certain CPMPs.

Obstacles

- **Ever-changing global laws and best practices.** With regions and countries implementing their own data privacy legislations, organizations must adapt to each one to remain in compliance. CPMPs tend to oversell their ability to make managing consent options simple, often downplaying the complexity of managing an organization's internal and external databases.
- **Lack of UX design support.** Forcing too many privacy choices on consumers degrades UX and leads to high opt-out and abandonment rates. Yet, having too few choices limits the ability to tailor experiences. To strike the right balance requires cross-functional, collaborative activities across the organization.
- **Complex technology architectures.** Digital transformation acceleration efforts propelled organizations to rethink how technology solutions work together and how data flows throughout the ecosystem. Adopters need to factor in the number of connections — both native and customized (e.g., APIs, ETL) — that are needed to effectively use a CPMP.

User Recommendations

- Prioritize consent management policies and initiatives as a critical priority for all functions. Establish a cross-functional customer data and privacy council to review and update policies and processes for the enterprise to follow.
- Avoid “dark patterns” or deceptive language for consent dialogues that attempt to influence users’ choices (see the FTC’s Press Release).
- Use a “telescoping” approach to disclosures and preference dialogues that allow users to go as deep as they choose into specific details. Offer consistent, easy access to preference settings that can be viewed and changed on demand to ensure that you are undertaking a privacy-by-default approach.
- Compare and assess CPMP offerings against your organization’s highest-priority data privacy protection and integration requirements and internal costs.
- Develop a CPMP where the market cannot effectively connect and integrate with legacy internal tools.
- Take a modular approach to adoption and avoid excessively broad project scopes. Anticipate sufficient time to resolve unforeseen complications in these projects.

Sample Vendors

BigID; Didomi; Ketch; OneTrust; PossibleNOW; Syrenis; TrustArc

Gartner Recommended Reading

Market Guide for Consent and Preference Management

Market Guide for Consent and Preference Management for Marketers

Data and Analytics Governance

Analysis By: Saul Judah, Andrew White

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Data and analytics governance is the specification of decision rights and an accountability framework to ensure the appropriate behavior in the valuation, creation, consumption and control of data, analytics and AI. It includes the processes, roles, policies, standards and metrics that ensure the effective and efficient use of data and analytics in enabling an organization to achieve its goals.

Why This Is Important

Data and analytics governance allows organizations the oversight to drive better behaviors relating to information-related assets in the enterprise, enabling better business outcomes and mitigation of risk. Data and analytics leaders need good governance practices to enable key business outcomes, such as market growth, cost optimization, merger and acquisition scenarios, and compliance management.

Business Impact

Data and analytics leaders should anticipate the following impacts:

- Better governance oversight, accountability and understanding of decision rights relating to data and analytics across the enterprise and within business areas
- Increased levels of business collaboration, transparency, engagement and innovation to drive mission-critical priorities in the enterprise
- Increased levels of data literacy and cultural change enabled by better governance

Drivers

- Higher levels of risk appetite and growth expectations in organizations are based on digital as an implicit part of growth strategies. This requires data and analytics governance capabilities that enable flexibility, scale and resiliency. Data and analytics governance is hence recognized by CDAOs as among the top three critical enablers for successful data and analytics initiatives.
- Investment in data and analytics is widespread across enterprises, with business functions spending as much as central IT teams on these initiatives, causing proliferation of information silos. The need for effective governance capabilities has therefore become an increasing concern for data and analytics leaders as a framework for enabling the connected enterprise, while also addressing the local information needs of business functions.
- Organizations with higher information maturity increasingly recognize that taking a data and analytics governance approach — rather than one focusing on individual information asset types (e.g., data governance) — yields better business results. Elsewhere, we have seen organizations recognize the urgent need to establish governance "to get the ball rolling," even if it is for only data governance or analytics governance. This significant increase in effort and hype relating to data and analytics governance is being seen in all industries, geographies, organization types and maturity levels.
- Hype and interest are also growing in many areas related to data and analytics governance. These areas include AI model governance, analytics governance in data warehouses and data lakes, trust-based governance, IoT data governance, and ethics as a discrete governance policy type.

Obstacles

- Data and analytics governance is complex, organizationally challenging and politically sensitive. It is often difficult to get executive-level consensus for data and analytics governance programs, and as a result, they are led by IT, with a view to "bringing in the business later." Because these initiatives are not business-outcome-based, they typically result in failure.
- Despite the diversity and complexity of business scenarios, most organizations continue to take a one-size-fits-all, command-and-control approach to their data and analytics governance. Furthermore, most organizations have a poor understanding of executive leader accountability and decision rights for information. Establishing an effective governance for data and analytics is therefore difficult to achieve. As organizations' expectations of what can realistically be achieved through data and analytics governance decline, we see its position on the Hype Cycle descend into the Trough of Disillusionment.

User Recommendations

- Identify critical business outcomes that need good data and analytics to be successful. Focus your governance work there to maximize your investment, developing a business case if needed.
- Engage key business stakeholders and the CDAO in sponsoring and driving the initiative to enable information culture change.
- Focus on the least amount of data with the maximum business impact, while managing your risk to embed data and analytics governance in the full business context.
- Clearly define the scope of work related to data and analytics governance: policy evaluation and setting, policy interpretation and enforcement, and policy execution. The first two must be led by the business; the latter can be enabled by IT.
- Examine how data standards and metadata management can be used to implement data and analytics governance in the enterprise. Though business leaders may not fully understand their importance, an industrial governance capability needs enterprise-scale data and analytics capabilities.

Gartner Recommended Reading

7 Must-Have Foundations to Build a Modern Data and Analytics Governance Program

2022 Strategic Roadmap for Data and Analytics Governance

Quick Answer: How Can I Apply Composable Design Principles to Data and Analytics Governance Organization Capabilities?

Next Best Actions to Improve Your Data and Analytics Governance

5 Steps to Build a Business Case for Data and Analytics Governance That Even Humans Will Understand

Alternative Legal Service Providers

Analysis By: Ron Friedmann

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Alternative legal service providers (ALSPs) are non-law-firm providers that perform legal support work at a lower cost than law firms and corporate legal departments. Staffing ALSPs provide individual, highly skilled attorneys for limited-duration projects or teams of relatively junior lawyers for volume projects such as litigation document review. Managed-services ALSPs offer process-improved and tech-enabled support from lower-cost locations for high-volume work such as contract management.

Why This Is Important

Unlike legal departments and law firms, which use expensive lawyers for most work, managed-services ALSPs use lower-cost labor, enhanced by improved processes and automation, to deliver quality results cost-effectively. They typically cost less and price work per unit or per project for more predictable cost and turnaround time than other options. Lastly, they offer hard-to-hire multidisciplinary skills — for example, data science — to solve complex problems.

Business Impact

Legal services buyers benefit in four ways by using ALSPs:

- Reducing legal spend

- Improving outcomes
- Accelerating turnaround times
- Freeing up in-house lawyers for more strategic work

These benefits apply across multiple work types:

- Reviewing discovery documents
- Identifying risks in acquiring assets (due diligence)
- Generating and managing high-volume agreements, such as commercial contracts
- Filing for and managing patents, copyrights or trademarks
- Improving compliance
- Managing multiple corporate entities

Drivers

Macro trends drive growing demand for legal service as:

- A growing number of regulations and ongoing supply chain changes are generating more legal work.
- Organizations increasingly recognize that contracting often slows the time to revenue; therefore, they seek faster legal approval.

Legal departments continue to face cost and other pressures:

- Law firms' hourly rates continue to escalate.
- Keeping talent engaged remains difficult, and too much time spent on lower value tasks creates a risk that talent will exit.
- Legal departments continue to face C-suite pressure to modernize how they work and control their budgets.
- Solving legal problems today requires data analytics and technology expertise, which are lacking in most legal departments.

Improvements in supply-side factors make ALSPs a more attractive option:

- ALSPs have matured significantly in this century. Collectively, they have hundreds of years of experience on thousands of projects across document review, contract management, due diligence and other high-volume legal work.
- Most ALSPs, including large professional service firms, independents, tech providers and law firm captives continue to invest in expanding and improving their capabilities.
- ALSPs have successfully hired top talent across multiple disciplines, enabling them to solve more complex problems with legal operations consulting, solution design and data analytics.
- A growing number of legal professionals view ALSPs as desirable employers that offer a better set of work-life trade-offs than many large law firms.
- Moving work off-site has become less of a barrier with pervasive, hybrid working arrangements.

Obstacles

- Not every organization has enough high-volume work suitable for managed-services ALSPs.
- Many legal departments are uncertain about when to use ALSPs and lack the data to identify what work to shift to ALSPs.
- Legal departments favor established relationships; they select a provider — typically a well-known law firm — based on convenience, familiarity and perceived low risk, not on cost or data-informed factors that favor ALSPs.
- Enforcing the use of ALSPs top-down is a challenge because in-house lawyers have substantial autonomy in choosing providers.
- Though buyers are comfortable navigating a fragmented law firm market, they struggle to identify and select suitable ALSPs because of the multitude of options.
- Engaging a managed-services ALSP takes time and planning. Many in-house counsel face too many daily pressures to invest that time.
- The advent of generally available large language models may change both supply and demand factors in ways that are hard to predict.

User Recommendations

- Gain legal department management buy-in to use an ALSP by developing a return on investment analysis for one or more use cases.
- Identify appropriate matters or work types for an ALSP to handle by analyzing department workload and outside spend.
- Choose staffing ALSPs to substitute for absent in-house lawyers and to work on time-limited special projects.
- Choose managed-services ALSPs for higher-volume work of low to moderate complexity, such as contract management.
- Determine the requirements for performing work that is being shifted to an ALSP by interviewing department members. Then, have informal discussions with several ALSPs in advance of writing an RFI or RFP. Ask providers how they can improve and automate work and what their overall workflows are.
- Confirm provider suitability by starting with a pilot project with clearly defined endpoints and metrics.
- Once ready for contracting, negotiate an SLA that covers key metrics (e.g., volume, complexity, quality) and governance.

Sample Vendors

Clarivate; Deloitte; Elevate; Factor; Integreon; Morae; PwC; QuisLex; UnitedLex

Gartner Recommended Reading

Innovation Insight for Using ALSPs to Reduce Legal Spend

Getting Started With Using an ALSP

How General Counsel Should Select an Alternative Legal Service Provider

Why and How General Counsel Must Use an ALSP to Streamline Contract Management

Legal Analytics

Analysis By: Chris Audet

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Legal analytics reflect the use of descriptive, prescriptive and predictive analytics in the legal domain. Common desired outcomes include identifying ways to operate more efficiently, optimizing spend and communicating the legal department's value and impact on the broader business.

Why This Is Important

Amid an environment of economic uncertainty and persistent disruption, corporate legal teams face rising workloads, multifaceted risk exposures and increasing budget scrutiny. Data and analytics is a critical lever for legal leaders to increase their teams' efficiency and scalability, optimize spend, validate current resourcing and demonstrate legal's impact on the business.

Business Impact

Legal analytics can deliver value across various areas, such as:

- Decreasing costs (in-house versus external sourcing strategy, external spend management, active matter management, internal workload and resource management)
- Increasing speed and effectiveness (bottleneck/process failure identification, request and matter management, work strategy)
- Reducing risk (litigation management, risk management at the contract and portfolio level, risk tolerance alignment between legal and the business)

Drivers

- Growing Demands on Corporate Legal Leaders — Workloads continue to rise for already exhausted corporate legal teams, driven by expanding mandates, a volatile business environment and increasing regulatory and stakeholder scrutiny. These growing pressures coincide with greater budget scrutiny, precluding significant additional resource investments. Analytics address such pressures by enabling smarter strategic decisions, identifying opportunities for process improvement and automation, diagnosing inefficiencies and process failures, allowing legal to be more proactive in identifying business needs, and communicating legal's value in alignment to broader business goals.

- Rising Analytics Success Across the C-Suite — Many business leaders in other functions have delivered on the promise of analytics while corporate legal teams have lagged behind. Legal functions have long relied more on experience and judgment than data and analysis. As other functions continue to show progress, they set increasing expectations for the use of analytics in legal.

- Active Promotion by Vendors in Dynamic Technology Markets — Legal tech vendors have featured analytics heavily in their new offerings and product roadmaps, including AI-based use cases. This active promotion is capturing end users' attention and encouraging legal leaders to think about analytics applicability in their environments.

- Rising Legal Data Standards — The emergence of Standards Advancement for the Legal Industry (SALI) and other open-source standards to systematically characterize legal work holds the promise of easier data exchange across systems and more powerful analysis based on areas of law, jurisdiction and other key legal attributes, potentially overcoming limitations of previous efforts (e.g., UTBMS, ABA codes).

- Advent of Large Language Models (LLM) — While the prevalence of variable, unstructured, narrative data in corporate legal practice complicates matters, the advent of multiple LLMs will help unlock the potential of analytics for legal teams.

Obstacles

- Difficulty Getting Started — Many legal teams remain in the early stages of implementing and adopting legal analytics. Legal teams struggle to make the business case for analytics, identify the right use cases for investment, navigate crowded technology landscapes and implement analytics programs that drive real value for legal and the business.
- Limited Experience and Investment — Analytics experience typically falls outside corporate legal leaders' traditional background, driving either an overacceptance of hype in the market or a pessimistic view of analytics' potential. Rising workloads, reactive postures and use of costly outside experts hamper teams' ability to invest in digital skills.
- No One-Size-Fits-All Approach — Vendors are challenged to deliver packaged, off-the-shelf solutions that support a broader data narrative because of the high variability across organizations in data availability, data quality, business processes, application environment and strategic priorities.

User Recommendations

- Evaluate analytics opportunities with discipline. Legal leaders should focus their pursuits on the business outcomes and related decisions that would benefit most from analytics. Then, weigh those opportunities against potentially available, relevant data to determine which opportunities are realistic.
- Harness existing or underused data sources (e.g., financial data, external/internal matter data, contract data). Many legal teams allow vast amounts of potentially valuable information to go uncaptured, rendering it unusable due to poor data management. Identify opportunities to change how teams curate data (including adopting data standards) to increase the volume and value of data to analyze.
- Build support and comfort for using analytics among the team by making the benefits clear and upskilling or hiring based on skills needed. Overcome hesitancy toward analytics by incentivizing team members to identify potential opportunities for legal analytics.

Sample Vendors

Apperio; Brightflag; LawVu; LexisNexis; Mitratech; SimpleLegal; Thomson Reuters; Wolters Kluwer

Gartner Recommended Reading

Ignition Guide to Building a Legal Analytics Program

Top 10 Analytics Skills for Legal and Compliance Teams

Market Guide for Corporate Legal Operations Technology

Advanced Contract Analytics

Analysis By: Kaitlynn Sommers

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Adolescent

Definition:

Advanced contract analytics solutions use natural language processing combined with artificial intelligence to uncover (and sometimes recommend) action in response to business performance insights. These insights are generated through the analysis of structured and unstructured data pertaining to contractual terms and conditions.

Why This Is Important

Advanced contract analytics solutions help organizations gain visibility into their signed contracts, drive efficiency in the contract review and risk assessment processes, and provide opportunities for continuous improvement. These solutions are positioned to improve contract processes across the legal, procurement and sales domains.

Business Impact

These solutions serve multiple use cases including contract visibility, contract review and risk analysis. They also support advanced reporting and continuous improvement. Many organizations have been successful in expediting their presignature contract process and improving postsignature, audit and regulatory compliance. Impact spans multiple departments involved in contracting processes within an organization and can support scalability efforts without adding additional headcount.

Drivers

- Legal departments wanting to scale their support services to the organizations without hiring additional resources can use these solutions to improve efficiency.
- The “new normal” of constant but changing business disruption has accelerated organizations’ urgency to understand what their contracts contain and their obligations to third parties and to better manage their contract risk going forward. As a result, solutions are seeing rapid innovation and becoming more applicable to a broader audience.
- Regulatory changes across industries, such as banking and finance, are increasing the need for organizations to document contract risk assessments. Organizations can also use this technology to quickly react to changes in regulations and make updates to affected contracts.
- Cross-functional use cases for contract analytics solutions are growing. Business stakeholders need quick access to contract documents and can benefit from risk analysis when managing third-party relationships. Joint ownership of these solutions increases ROI and the likelihood of business case approval.
- Leading contract life cycle management (CLM) vendors are rapidly investing in contract analytics as the next competitive field and organizations that are mature in their CLM processes are seeking this advanced capability.
- Generative AI will facilitate faster adoption of some use cases such as automated contract review and contract analysis by quickly delivering contract clause language and helping business users better understand contract terms.

Obstacles

- The cost for these solutions is generally high. Often, the pricing model scales with the number of documents needing review — meaning those that have the greatest need for the solution also incur the greatest cost. This limits the pace of marketwide adoption unless the use cases and ROI are very clear.
- While these solutions are maturing and have become more reliable, some use cases require a deep understanding of an organization's definition of risk, templates and term acceptance. This means time and manual intervention before the tools learn enough to act as a lawyer in your organization.
- The market is highly fragmented. Most solutions enter the market serving a single use case. This is also true for CLM vendors expanding into advanced contract analytics, focusing on one use case before others. Organizations may need more than one solution to address all of their requirements.

User Recommendations

- Define your requirements, use cases and desired business outcomes first.
- Survey the market for solutions suitable for addressing your use cases. The market is highly fragmented and terminology can be interchanged and confused, so be clear about the business outcomes you want to support and create a suitable shortlist of vendors based on these use cases.
- Allow that you may need more than one vendor to support multiple use cases. You may include your CLM vendor, but these vendors vary significantly in the use cases they support as well.
- Run pilots to assess the benefit and reliability of contract analytics to reduce contract review time, increase visibility and manage contract risk.
- Review new features and expanded use cases regularly to determine if your chosen solution can contribute further to enterprise goals. As these solutions mature, there may be opportunities for broader enterprise use.

Sample Vendors

BlackBoiler; Cognitiv+; DiliTrust; Knowable; Lawgeex; LegalSifter; LexCheck; Litera; Luminance Technologies; Pramata

Gartner Recommended Reading

3 Questions to Answer Before Shortlisting CLM Vendors

Market Guide for Advanced Contract Analytics

Privacy Impact Assessments

Analysis By: Bart Willemsen

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Privacy impact assessments (PIAs) enable organizations to identify and treat privacy risk. Typically conducted before implementing new processing activities and/or major changes, the PIA starts with a quick scan (looking at the process owner and description, types of data processed for specific purposes, and retention periods per purpose). A full PIA adds legal grounds, potential impact on data subjects, and mitigating measures to ensure a controlled personal data processing environment.

Why This Is Important

An ongoing shift in the regulatory privacy landscape mandates that organizations develop foundational insight into what personal data they process, why and how it is protected. Few organizations have the means to demonstrate insight in and control over personal data across the various repositories and silo types, let alone how they're used or intended to be used. This insight, however, is vital to proportionate and adequate deployment of privacy and security controls.

Business Impact

A PIA improves regulatory compliance, control over personal data throughout the data life cycle, and helps determine access management as well as data end of life following a deliberate intent toward purposefully processing people's data. Assisting in prevention of (internal) data breaches and personal data misuse, it helps security and risk management (SRM) leaders quantify risk to subjects and timely apply suitable mitigating controls. Conducting PIAs frequently and consistently provides a basis for responsible and transparent data management.

Drivers

- PIAs are one of the cornerstones of an effective privacy program. However, many organizations conduct PIAs manually, using spreadsheets and questionnaires. With increasing volumes and the need for repetition of PIAs, a manual approach becomes unmanageable.
- Overstandardization traps the skills needed to conduct PIAs with a few people rather than making them part of an organization's data-handling fabric.
- PIA automation tools allow for (API-driven) triggers to initiate the assessment process, collecting the needed information at every step and tracking it through a predefined workflow all the way until a case is closed or flagged for remediation.
- When done well, the PIA sits at the heart of connecting legal requirements and business process reengineering to practical operationalization in privacy by design and enablement of adequate security control application.
- The results of a PIA will help assess records of processing activities (RoPAs), and through intelligence of data fabric from data and analytics leaders, SRM leaders can further automate the intended personal data life cycle in terms of where it should and should not be available. In other words, the PIA outcome with purpose-based processing activities determines purpose-based access controls (PBAC). In addition, it facilitates automation of the determined data end-of-life moments.
- The entire PIA process eases data governance initiatives to a more controlled state, yet the current main drivers still primarily come from regulatory requirements. Additional frameworks do help, like the 2023 revamped ISO 29134.

Obstacles

- Often considered a tedious task because of poorly conceived manual workflows and a one-size-fits-all mentality, there is a certain PIA fatigue in organizations where this activity has been mandatory for a longer period of time.
- Business partners' view of a checkbox mentality does not help the quality of the PIA.
- Others simply underestimate its relevance and position and do not complete accurate PIAs or fail to frequently keep them updated, making the initial attempt an ultimately futile one.
- PIA automation tools are hard to tailor to an organization's needs in the absence of knowledgeable and trained staff. As a result, even an automated approach fails to fulfill the purpose for subsequent automation and alignment of the personal data life cycle governance or management activities that are ideally connected to the PIA.

User Recommendations

- Appoint and mandate business process owners with responsibility over their respective personal data processing activities, and actively involve them in optimizing the process for fluency and detail.
- Require PIAs to be conducted as a mandatory, frequently reiterated activity. Triage the necessity for PIAs in change processes and the introduction of new processing activities.
- Include the PIA's results — especially from large projects — in the corporate risk register for monitoring and follow-up. Depending on scope and focus, it may also help to integrate high-risk PIA activities to overarching business impact assessments.
- Extend the assessment's effectiveness to processing of personal data carried out by service providers by demanding that they complete and periodically revise a full PIA.
- Use a centrally provisioned tool for consistently conducting PIAs (for example, as an internal automated workflow process), or require the PIA to be conducted as a manual exercise when a less-mature procedure suffices.

Sample Vendors

DataGrail; OneTrust; PrivacyPerfect; RESPONSUM; Securiti; Smart Global Governance; TrustArc; WireWheel

Gartner Recommended Reading

Toolkit: Assess Your Personal Data Processing Activities

Use a Privacy Impact Assessment to Ensure Baseline Privacy Criteria

Ignition Guide to Implementing a Privacy Impact Assessment Process

Climbing the Slope

E-Discovery Solutions

Analysis By: Michael Hoeck

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

E-discovery solutions facilitate the identification, collection, preservation, processing, review, analysis and production of electronically stored information (ESI). ESI fulfills legal and compliance requirements for discovery that result from a variety of judicial and investigative scenarios. E-discovery solutions include software vendor offerings for a customer's own on-premises or cloud deployment, as well as hosted offerings provided by software vendors and services providers.

Why This Is Important

Data growth, new content sources, timely responses to data requests and demands to drive down legal operational costs have made e-discovery solutions essential for organizations. Use cases include litigation, employee and other internal investigations, public records requests, subject rights requests, regulatory demands, and post-data-breach investigations. Highly regulated and litigious industries must especially pay close attention to e-discovery requirements.

Business Impact

E-discovery solutions help by:

- Supporting multiple cases/investigations conducted by enterprises.
- Reducing the overhead associated with managing legal hold notifications and preserving related data.
- Integrating with new discoverable sources such as workstream collaboration and meeting solutions.
- Expanding use cases such as breach investigations and privacy regulation responses.

- Enabling insourcing of e-discovery for faster turnaround and lower cost than using service providers or law firms.

Drivers

- Growing volumes of litigation and internal, administrative and regulatory investigations.
- Accelerating data growth and complexity of data sources, combined with more use cases for e-discovery.
- Increasing emphasis to reduce the cost of legal operations.
- Integration of e-discovery solutions with cloud office solutions simplifies the abilities of legal and compliance teams to directly access, set legal holds and conduct general e-discovery processes.
- Responsibility of legal teams and related e-discovery efforts in response to data breach scenarios.
- Reduced reliance on IT and improved self-service capabilities for legal and compliance users.
- Public sector requirements to manage Freedom of Information Act (FOIA) and Public Records Act (PRA) requests.
- Expanding number of privacy regulations and the related requirement to conduct subject rights requests.

Obstacles

- Legal and IT need to learn to partner with one another for e-discovery technology selection, deployment and ongoing processes.
- Buyers and budgets for e-discovery solutions generally come from different departments in organizations.
- Pricing models for e-discovery solutions are inconsistent and can be complex, lacking the transparency required to properly budget cost.
- The large variety of e-discovery solutions from dedicated software manufacturers and service providers may complicate selection.

- E-discovery technology maturity of legal and compliance teams must be clearly defined before starting the selection process to help narrow the field of vendors to consider.
- The need to fully assess the types of investigations to be performed by in-house staff to properly scope requirements.
- Continued sprawl of discoverable data sources such as the expanded use of digital communication tools (e.g., mobile devices, workstream collaboration and meeting solutions).

User Recommendations

- Improve e-discovery processes by selecting solutions that integrate directly with the most commonly investigated ESI sources, apply in-place legal holds and provide rich review experiences of that data.
- Narrow solution options by aligning the vendor's available deployment architectures, such as on-premises, SaaS, infrastructure as a service (IaaS) or platform as a service (PaaS), and other certifications or authorizations, such as FedRAMP.
- Balance selection of solutions from e-discovery software manufactures and service providers by aligning the legal department skill set to the complexity of e-discovery efforts.
- Fully qualify e-discovery solution costs by engaging with each vendor to obtain a detailed, accurate breakdown of all costs.
- Eliminate multiple solution purchases by creating a cross-functional team of IT and legal personnel.
- Work together with the legal, compliance, IT and security operations teams, with shared responsibility for information governance, e-discovery, data privacy, and security tasks and responsibilities.

Sample Vendors

Consilio; DISCO; Epiq Systems; Everlaw; Exterro; IPRO (ZyLAB); Logikcull; Nuix; OpenText; Relativity

Gartner Recommended Reading

Market Guide for E-Discovery Solutions

Privacy Management Tools

Analysis By: Bart Willemsen

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Adolescent

Definition:

Privacy management tools help organizations facilitate compliance insights and check processing activities against regulatory requirements. They bring structure to privacy processes and workflows, enhance insight into data flows and governance maturity, and monitor and track the privacy program's maturity progression.

Why This Is Important

The increasing maturity of data protection legislation globally forces organizations to maintain awareness and control of personal data processing operations. Roughly two-thirds of jurisdictions worldwide have requirements similar to the EU's trendsetting GDPR in place. They range from U.S. state laws like the CCPA or the CPRA to national initiatives like Brazil's LGPD and China's PIPL. The differences in detail across requirements make managing compliance overviews manually almost impossible.

Business Impact

Privacy management tools give business leaders oversight and accountability about handling personal data, and enable transparency and control over those activities. They contain audit capabilities to demonstrate compliance especially across multiple jurisdictions. Point solutions are more and more integrated into suites to account for an increasingly automated enablement of a privacy UX, vendor risk management, records of processing activities (ROPAs), data intelligence inventories, and more.

Drivers

- In almost all cases, passed or proposed privacy laws have been heavily influenced by the GDPR. Therefore, they are introducing concepts such as subject rights, explicit consent and timely breach disclosure. Regulatory changes are likely to continue over the coming two to three years, establishing the fundamental basis for privacy at the legislative level.
- Individuals' awareness and demand for privacy continue to rise, often through confrontation with a widespread use of new technology. Amid these ongoing pressures, organizations must adapt their privacy programs to allow better scale and performance while staying within budgets that are still tight. They should do so without exposing the business to loss through fines or reputational damages.
- The privacy landscape is becoming increasingly complex. Gartner estimates that by 2025, 75% of the world's population will have its personal data covered under modern privacy regulations. Even further, we calculate that by that time over 80% of organizations worldwide will face modern privacy and data protection requirements. Fundamental capabilities carrying even an immature privacy program include those for ROPAs, privacy impact and compliance assessments, several elements of the privacy UX and incident or data breach management.
- To implement a consistent and holistic privacy program, organizations require two sets of capabilities — privacy management capabilities and data-centric control capabilities. Some organizations opt to tackle data issues first: discovery, classification, authorization and access controls, and operationalizing end of life.
- Finally, an in-control privacy-first posture as well as transparency and control over personal data processing activities are simply good for business. They enhance brand protection, customer trust and represent an ethical approach to data and the people behind that data.

Obstacles

- After time, a sense of “good enough” can lead to delays in adoption of privacy management tools, or worse, an absence of (automated) integration to reap the maximum benefit.
- On the other hand, some organizations already have point solutions for privacy UX components, data breach response or impact assessments in place. They might overlook opportunities for more mature complementary capabilities in an integrated suite. Attempts to integrate loose components from various vendors can often be disappointing, if only remaining manual workload is considered.
- Ongoing developments, including the “shift-left” movement where certain capabilities are automated at a code level, are often technical in nature. This hinders adoption even when they could ultimately increase immediate and long-term benefits.
- As the absence of immediate sanctions or investigations makes pressure seem to subside, some organizations continue to take a wait-and-see approach and rely on a set of unmanageable practices.

User Recommendations

- Incorporate the demands of a rapidly evolving privacy landscape into the organization’s data strategy by developing a common baseline driven by applicable regulatory guidelines and privacy frameworks available.
- Maintain a focus on overarching capabilities with relevance across the board, including privacy impact assessments (PIAs), ROPAs, consistent vendor risk management and a people-centric privacy UX.
- Accept, adapt and evolve with the new business challenges and needs to privacy by leading with a cost-optimized set of privacy capabilities.
- Assess the extent to which privacy management tools fit the organization’s criteria for standardization needs. For example, they can help in certification preparations against the EuroPriSe framework, ISO 27701, or aligning with others like the NIST Privacy Framework, cloud codes of conduct, etc.

Sample Vendors

DataGrail; Ketch; OneTrust; RESPONSUM; Securiti; TrustArc; WireWheel

Gartner Recommended Reading

State of Privacy — The European Union

State of Privacy — China

State of Privacy — Regional Overview Across North America

5 Privacy Imperatives for Executive Leaders

Contract Life Cycle Management

Analysis By: Lynne Phelan

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Contract life cycle management (CLM) solutions are used to proactively manage contracts from the initiation stage through the award, compliance and renewal stages. In this context, a contract is any agreement or contractual document containing rights and obligations that affect an organization now or in the future (e.g., a nondisclosure agreement).

Why This Is Important

It is critical to have visibility into legal documents and obligations with third parties. Interest in CLM remains high, as organizations seek to digitize their processes, manage compliance, minimize risk and eliminate inefficiencies related to contracting. Contract execution management has also become a high priority for organizations.

Business Impact

CLM appeals to companies of all sizes in all industries and geographies. Implementing it can lead to significant improvements in revenue management, cost savings and efficiency. Understanding and automating CLM can also reduce an organization's liability, risk and increase its compliance with legal requirements. Without a CLM solution in place, stakeholders commonly have to spend significant time extracting, managing, and reporting terms and pricing arrangements.

Drivers

- Implementing a CLM solution can lead to significant improvements in internal and external process efficiency, especially when contract clauses need to be reviewed by different departments within the organization.
- Digitizing and automating CLM can reduce an organization's liability and increase its compliance with legal requirements.
- CLM solutions provide a centralized repository and administrative alerts to avoid lost contracts, unexpected expirations and a lack of visibility. This can help legal teams and contract stakeholders manage third-party relationships more effectively.
- Digital workflows can provide increased governance over what is signed, when and by whom, and the protection of knowing that the correct contract terms are live. Such processes also provide deeper insights across all contractual agreements by analyzing content, conditions and risk.
- Innovative CLM solutions are offering AI-based capabilities that improve contract review, assessment and reporting to minimize contract risk.
- Standardized and custom reports allow CLM users to monitor aspects like cycle times, obligations, compliance and metadata management in a configurable dashboard.

Obstacles

- CLM adoption levels vary widely. The mixed adoption levels are often a result of lower-maturity contracting processes, rather than limitations of the technology itself.
- Mature CLM requires strong cross-functional collaboration between commonly siloed departments within an organization. Each department has its own priorities, and it can be difficult to meet the needs of all parties simultaneously to gain enterprise adoption.
- The prominent trend for CLM buyers is a single enterprise source of truth. However, this is a significant undertaking and cannot be underestimated. Additionally, most solutions that claim to support enterprisewide contracting requirements lack the breadth of partners and integrations to make this a reality.
- Emerging AI use cases in contracting further attract CLM buyers, but the capabilities are highly fragmented across the market, leading to lower realized value and uncertainty around whether the investment in AI is justified.

User Recommendations

- Evaluate CLM solutions from strategic sourcing suite vendors when seeking a buy-side contract management solution and look for CLM solutions that integrate with CRM or CPQ (configure, price and quote) suites when seeking a sell-side (customer) contract management tool.
- Evaluate CLM solutions that integrate with enterprise legal management suites when a solution for the legal department is a priority.
- Evaluate (often existing) content services platform (CSP) solutions when a solution to simplify organization contracts and track expirations is needed.
- Review vendors' coverage across both presignature and postsignature capabilities.
- Assess the potential use cases for AI as CLM vendors have a heavy focus on building out AI within their tools.
- Analyze CLM vendors' growth and financial viability. The market is crowded, and consolidation is inevitable. Contact Gartner if the CLM solution you are using or considering is acquired.

Sample Vendors

Agiloft; Conga; ContractPodAi; DocuSign; Evisort; Icertis; IntelAgree; Ironclad; Malbek; SirionLabs

Gartner Recommended Reading

Magic Quadrant for Contract Life Cycle Management

Critical Capabilities for Contract Life Cycle Management

3 Questions to Answer Before Shortlisting CLM Vendors

Toolkit: RFP for Contract Life Cycle Management

Corporate Legal Operations Technology

Analysis By: Chris Audet

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Early mainstream

Definition:

Corporate legal operations technology products are single solutions or integrated suites, often marketed as enterprise legal management (ELM) technologies, that enhance corporate legal department operations and workflows for in-house legal departments. The products typically provide solutions for e-billing and spend management; external matter management; intake, triage and service management; and workflow automation capabilities; among others.

Why This Is Important

Enterprises depend on their legal departments to manage risk and enable new business opportunities, whether by introducing new products, forging relationships in new ecosystems, managing strategic transactions or documenting new agreements. As a central hub for managing legal workflows, such as legal intake, e-billing and matter management, corporate legal operations technology also provides the organization with vital information on performance, cost and risk.

Business Impact

Corporate legal operation technologies' core capabilities include optimizing legal resource management and legal spend; facilitating attorney and staff collaboration on legal matters; supporting the intake and triage of legal matters; and digitizing and automating key legal workflows.

Drivers

Legal departments adopt corporate legal operations technology for a range of reasons, including to:

- Leverage automation for routine tasks and elevate legal's role in advancing business goals by enabling it to be more proactive, responsive and visible.
- Establish a single-source or single-platform solution for many legal applications and use cases, versus acquiring separate systems for matter management, e-billing, spend management and more.
- Establish a systematic and consistent data foundation to inform decisions and provide a range of analytics.

- Optimize costs by in-sourcing certain legal work, while applying more rigor to the management of spending on outside law firms and alternative legal service providers.
- Leverage innovation like artificial intelligence, advanced process management and analytics delivered in the context of ready-to-use legal applications.

Obstacles

- The success rate with corporate legal operations technologies has been meager, and the adoption rate is surprisingly slow for a well-established category in a needy space.
- Wildly differing internal operating environments and preferences across legal departments limit the opportunity for a standard, repeatable software solution.
- Organizations pursuing a single-vendor/single-platform approach have often come to the costly realization that addressing their corporate legal operations technology aspirations requires multiple products and vendors with more in-depth coverage.
- The rapid emergence of legal tech startups with point solutions that serve many of the same core capability sets (e.g., workflow and automation) as corporate legal operations technology runs counter to any hoped-for marketplace consolidation and creates fear of making the wrong selection.
- Application leaders in legal departments often struggle to resolve competing pressures to adopt corporatewide standard applications and legal-specific applications.

User Recommendations

- Evaluate opportunities for technology enablement by engaging stakeholders who perform the day-to-day work and gathering pain points. Map these pain points to required capabilities to identify technology needs.
- Prioritize technology needs by assessing potential impact to the department's current operations and future anticipated needs and the business, more broadly.
- Evaluate trade-offs of investing in a single solution or an integrated suite (e.g., ELM) by leveraging technology needs assessment. Integrated suite solutions provide broader, more holistic coverage across core capability sets whereas single/point solutions provide deeper coverage across a narrower set of capabilities.

Sample Vendors

Brightflag; doeLEGAL; LexisNexis; Mitratech; Onit; PracticeLeague; Thomson Reuters; Wolters Kluwer

Gartner Recommended Reading

Target Business Outcomes to Advance Your Legal Tech Strategy

Ignition Guide to Building a Legal Technology Roadmap

Market Guide for Corporate Legal Operations Technology

Vendor Identification Tool: Corporate Legal Operations Technology Vendor and Product Data

Predicts 2023: Increasing Corporate Legal and Compliance Technology Investments Amid Economic Volatility

Appendixes

See the previous Hype Cycle: Hype Cycle for Legal and Compliance Technologies, 2022

Hype Cycle Phases, Benefit Ratings and Maturity Levels

Table 2: Hype Cycle Phases

(Enlarged table in Appendix)

Phase	Definition
Innovation Trigger	A breakthrough, public demonstration, product launch or other event generates significant media and industry interest.
Peak of Inflated Expectations	During this phase of overenthusiasm and unrealistic projections, a flurry of well-publicized activity by technology leaders results in some successes, but more failures, as the innovation is pushed to its limits. The only enterprises making money are conference organizers and content publishers.
Trough of Disillusionment	Because the innovation does not live up to its overinflated expectations, it rapidly becomes unfashionable. Media interest wanes, except for a few cautionary tales.
Slope of Enlightenment	Focused experimentation and solid hard work by an increasingly diverse range of organizations lead to a true understanding of the innovation's applicability, risks and benefits. Commercial off-the-shelf methodologies and tools ease the development process.
Plateau of Productivity	The real-world benefits of the innovation are demonstrated and accepted. Tools and methodologies are increasingly stable as they enter their second and third generations. Growing numbers of organizations feel comfortable with the reduced level of risk; the rapid growth phase of adoption begins. Approximately 20% of the technology's target audience has adopted or is adopting the technology as it enters this phase.
Years to Mainstream Adoption	The time required for the innovation to reach the Plateau of Productivity.

Source: Gartner (July 2023)

Table 3: Benefit Ratings

Benefit Rating ↓	*Definition* ↓
Transformational	Enables new ways of doing business across industries that will result in major shifts in industry dynamics
High	Enables new ways of performing horizontal or vertical processes that will result in significantly increased revenue or cost savings for an enterprise
Moderate	Provides incremental improvements to established processes that will result in increased revenue or cost savings for an enterprise
Low	Slightly improves processes (for example, improved user experience) that will be difficult to translate into increased revenue or cost savings

Source: Gartner (July 2023)

Table 4: Maturity Levels

(Enlarged table in Appendix)

Maturity Levels	Status	Products/Vendors
Embryonic	In labs	None
Emerging	Commercialization by vendors Pilots and deployments by industry leaders	First generation High price Much customization
Adolescent	Maturing technology capabilities and process understanding Uptake beyond early adopters	Second generation Less customization
Early mainstream	Proven technology Vendors, technology and adoption rapidly evolving	Third generation More out-of-box methodologies
Mature mainstream	Robust technology Not much evolution in vendors or technology	Several dominant vendors
Legacy	Not appropriate for new developments Cost of migration constrains replacement	Maintenance revenue focus
Obsolete	Rarely used	Used/resale market only

Source: Gartner (July 2023)

Document Revision History

Hype Cycle for Legal and Compliance Technologies, 2022 - 1 August 2022

Hype Cycle for Legal and Compliance Technologies, 2021 - 19 July 2021

Hype Cycle for Legal and Compliance Technologies, 2020 - 20 July 2020

Hype Cycle for Legal and Compliance Technologies, 2019 - 11 November 2019

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Understanding Gartner's Hype Cycles

Tool: Create Your Own Hype Cycle With Gartner's Hype Cycle Builder

Use Gartner Hype Cycles to Guide Tech Adoption Strategies in Legal

Predicts 2023: Increasing Corporate Legal and Compliance Technology Investments Amid Economic Volatility

Table 1: Priority Matrix for Legal and Compliance Technologies, 2023

Benefit ↓	*Years to Mainstream Adoption*			
	Less Than 2 Years ↓	***2 - 5 Years*** ↓	***5 - 10 Years*** ↓	***More Than 10 Years*** ↓
Transformational		Dynamic Risk Governance	Legal Department Intake and Triage	
High	Data Breach Response Digital Ethics Natural Language Query Privacy Management Tools	AI Governance AI in Corporate Legal and Compliance Practice Contract Life Cycle Management Data and Analytics Governance E-Discovery Solutions Legal Chatbots Prescriptive Analytics Privacy Impact Assessments Subject Rights Requests	Alternative Legal Service Providers Compliance Monitoring and Analytics Corporate Legal Operations Technology ESG Management and Reporting Software Explainable AI Legal Analytics Regulatory Intelligence Third-Party Risk Management	
Moderate		Advanced Contract Analytics Consent and Preference Management	GRC for Assurance	Voluntary Carbon Offsets
Low				

Source: Gartner (July 2023)

Table 2: Hype Cycle Phases

Phase	*Definition*
Innovation Trigger	A breakthrough, public demonstration, product launch or other event generates significant media and industry interest.
Peak of Inflated Expectations	During this phase of overenthusiasm and unrealistic projections, a flurry of well-publicized activity by technology leaders results in some successes, but more failures, as the innovation is pushed to its limits. The only enterprises making money are conference organizers and content publishers.
Trough of Disillusionment	Because the innovation does not live up to its overinflated expectations, it rapidly becomes unfashionable. Media interest wanes, except for a few cautionary tales.
Slope of Enlightenment	Focused experimentation and solid hard work by an increasingly diverse range of organizations lead to a true understanding of the innovation's applicability, risks and benefits. Commercial off-the-shelf methodologies and tools ease the development process.
Plateau of Productivity	The real-world benefits of the innovation are demonstrated and accepted. Tools and methodologies are increasingly stable as they enter their second and third generations. Growing numbers of organizations feel comfortable with the reduced level of risk; the rapid growth phase of adoption begins. Approximately 20% of the technology's target audience has adopted or is adopting the technology as it enters this phase.
Years to Mainstream Adoption	The time required for the innovation to reach the Plateau of Productivity.

Phase	Definition

Source: Gartner (July 2023)

Table 3: Benefit Ratings

Benefit Rating	Definition
Transformational	Enables new ways of doing business across industries that will result in major shifts in industry dynamics
High	Enables new ways of performing horizontal or vertical processes that will result in significantly increased revenue or cost savings for an enterprise
Moderate	Provides incremental improvements to established processes that will result in increased revenue or cost savings for an enterprise
Low	Slightly improves processes (for example, improved user experience) that will be difficult to translate into increased revenue or cost savings

Source: Gartner (July 2023)

Table 4: Maturity Levels

Maturity Levels ↓	*Status* ↓	*Products/Vendors* ↓
Embryonic	In labs	None
Emerging	Commercialization by vendors Pilots and deployments by industry leaders	First generation High price Much customization
Adolescent	Maturing technology capabilities and process understanding Uptake beyond early adopters	Second generation Less customization
Early mainstream	Proven technology Vendors, technology and adoption rapidly evolving	Third generation More out-of-box methodologies
Mature mainstream	Robust technology Not much evolution in vendors or technology	Several dominant vendors
Legacy	Not appropriate for new developments Cost of migration constrains replacement	Maintenance revenue focus
Obsolete	Rarely used	Used/resale market only

Source: Gartner (July 2023)