Market Guide for Corporate Compliance and Oversight Solutions

Published: 11 August 2017 **ID:** G00305296

Analyst(s): Elizabeth Kim, Jeffrey Wheatman

CCO solutions help standardize and automate compliance activities to increase efficiency and effectiveness of compliance management programs. This research will help security and risk management leaders supporting compliance programs to identify key selection criteria for a CCO solution.

Key Findings

- One of the biggest challenges for compliance leaders is the speed of change. Compliance management is largely composed of myriad workflows and processes with dynamic interdependencies.
- CCO solutions enable a common cross-enterprise approach to compliance activities that most affect the regulatory oversight of corporate governance through support of the five major requirements for managing a compliance program: policy development, regulatory aggregation, normalization and mapping, control monitoring, workflow management, and case management.
- The corporate compliance and oversight solutions market is mature in its primary feature set, but differentiation lies in areas such as user-friendliness, quick and easy implementation, integration with other integrated risk management (IRM) solutions, and good visualization and reporting capability.

Recommendations

Security and risk management leaders supporting compliance programs and audit management in choosing corporate compliance and oversight (CCO) solutions should:

- Select vendors based on alignment with current and future IRM initiatives and investments.
- Evaluate compliance-focused vendors, especially if compliance is a significant business driver. For some organizations, it may be advisable to focus on the narrower needs of your industry, rather than investing in larger, broader, more expensive IRM solutions.

- Shortlist vendors based on alignment with prioritized requirements such as pricing, geographical alignment and support availability, industry alignment, regulatory content availability, and integration capability.
- Assess deployment options and identify short- and long-term appetite for SaaS, hosted or on-premises deployment models.

Market Definition

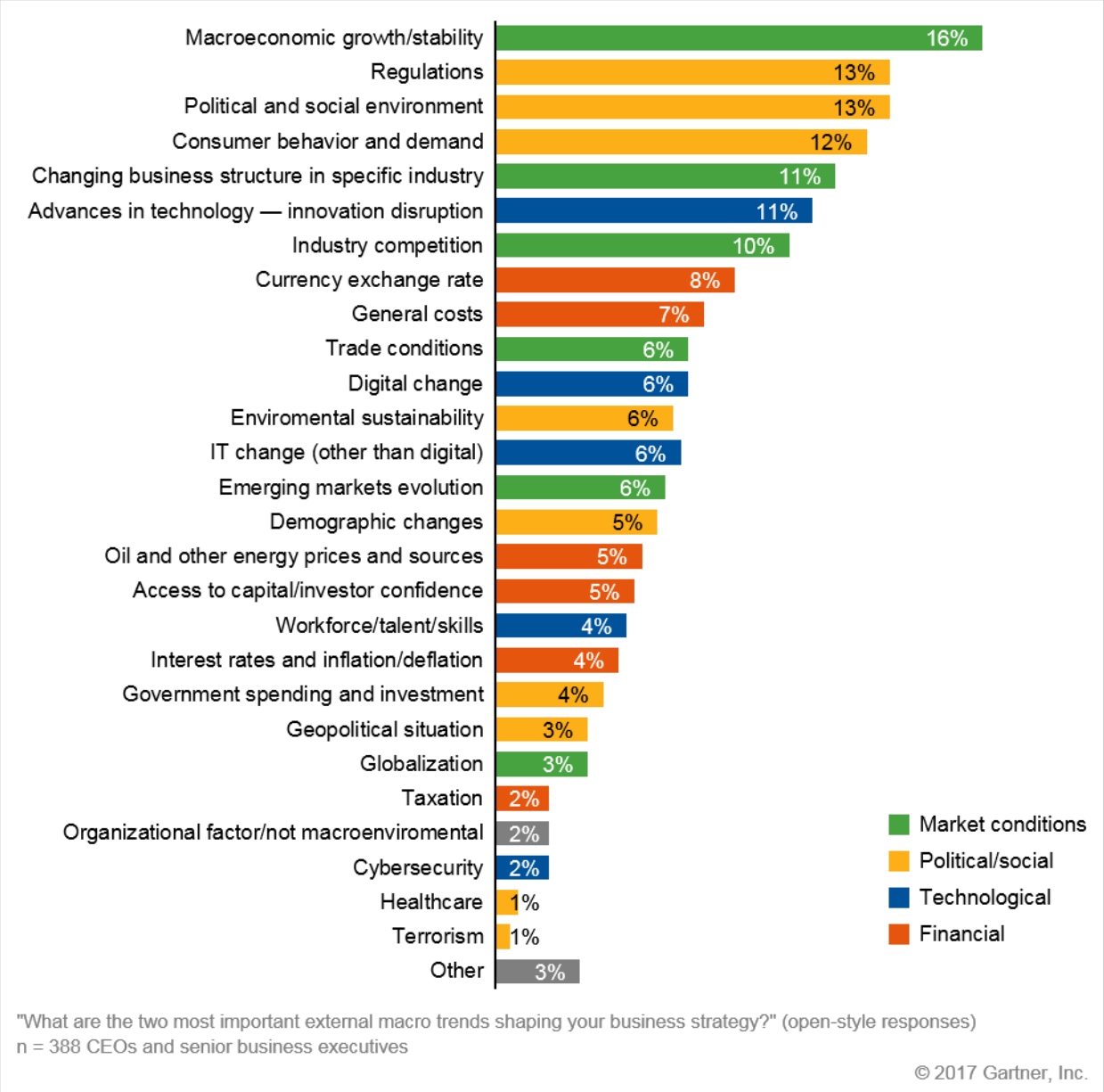
CCO tools provide the framework and support for standardization of compliance activities and automation to increase efficiency and effectiveness of compliance management programs. CCO enables a common cross-enterprise approach to IT compliance activities that most affect the regulatory oversight of corporate governance. This is done through support of the five major requirements for managing a compliance program: policy development, aggregation and normalization, control monitoring, workflow management, and case management.

Market Direction

Compliance leaders have seen their roles become more visible, more challenging and more important within their organizations over the past 10 years, as the global legal and regulatory landscape continues to become more complex. They are facing increased demands from customers, partners, boards of directors, and regulatory bodies to ensure that all applicable compliance obligations are met consistently and the organization stays up-to-date in predicting and planning for risk of noncompliance (which compliance teams should do by consulting legal counsel).

Increased focus on the policy implications of the regulatory environment, regulatory change management, controls automation, and case and incident management is now at the forefront of organizations' IRM strategies. In Gartner's 2017 CEO survey, CEOs cited regulations as one of the top external macrotrends shaping their business strategy. This indicates an increased level of focus around regulations and its business impact on all levels of organizations (see Figure 1).

Figure 1. Gartner 2017 CEO Survey External Macrotrend Rankings: Ranked by Mentions Within Top Two



Source: Gartner (August 2017)

CCO solutions can improve an organization's compliance management program through capabilities that align to and support areas of policy development, aggregation and normalization, control monitoring, workflow management, and case management.

Policy Development and Management

Policies and policy statements are among the most critical strategic controls for asserting management perspective and requirements. Policies shape behavior and create a roadmap of compliance for the organization. Features within this capability include:

- Mapping policies and controls to compliance requirements
- Integration of commercial and partner compliance requirements
- Integration of organization requirements such as ethics and behavior
- Policy authoring, change management and version control
- Development and approval workflow

Aggregation and Normalization

The huge number of global legal, regulatory and administrative requirements and the variety of standards, guidelines and frameworks require compliance managers to merge and normalize mapping of requirements to controls and other compliance activities. Add to this the growing requirements for compliance within the scope required by business relationships and internally generated mandates, and one can see how the role of the compliance leader has become increasingly challenging.

Requirements come from multiple sources, often conflicting entirely or in part. This means the challenge of aggregating, normalizing and designing controls has grown beyond the ability of manual effort, even when supported by basic technology such as spreadsheets.

The ability to take inputs from a wide range of sources and create a policy set that is easy to understand, support and manage is the foundation for measuring and reporting compliance across regulatory, commercial and organizational frameworks. Features within this capability include out-of-the-box content that is variable and diverse. Features within this capability include:

- Corporate compliance requirements, such as the Foreign Corrupt Practices Act (FCPA), the Gramm-Leach-Bliley Act (GLBA) and the Sarbanes-Oxley Act (SOX)
- Industry-specific regulatory guidelines, such as those from the Food and Drug Administration (FDA), the Federal Energy Regulatory Commission (FERC), the Federal Aviation Administration (FAA), Basel III, Hazard Analysis Critical Control Point (HACCP), anti-money-laundering (AML) controls, the Federal Acquisition Regulation (FAR) and the New York State Department of Financial Services (DFS)
- Information security and privacy regulations and other similar mandates, such as those from the Health Insurance Portability and Accountability Act (HIPAA), the International Organization for Standardization (ISO) 27001, the National Institute of Standards and Technology (NIST) 800-53, the Payment Card Industry (PCI), the EU General Data Protection Regulation (GDPR) and the Chinese Cybersecurity Law

- Risk frameworks such as COBIT, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and ITIL
- Business compliance management (BCM) frameworks, such as the Federal Financial Institutions Examination Council (FFIEC) Business Continuity Planning, ISO 22301:2012 and 22313, National Fire Protection Association (NFPA) 1600, and Department of Homeland Security/Federal Emergency Management Agency (DHS/FEMA) National Incident Management System/Incident Command System (NIMS/ICS)
- Fraud management and other business-aligned risk areas
- Access to additional data feeds to supplement out-of-the-box content
- The ability to support custom compliance requirements
- The ability to address conflicts between various requirements in a defensible manner

Control Assessments and Monitoring

This functional area supports the process of assessing compliance risks and controls, reporting on violations or variances, and attesting to controls and compliance. These functions help organizations automate the workflows, analysis and data repository requirements associated with control assessment. Features within this capability include:

- Control assessment and attestation workflow
- Survey functions to support data gathering
- Control catalog and reporting
- Employee training and certification
- Interface with other IRM solution initiatives
- Compliance metrics/reporting

Workflow and Business Process Management

One of the most difficult challenges for compliance leaders is the speed of change. Compliance management is largely composed of myriad workflows and processes with dynamic interdependencies. Successful compliance leaders are able to deploy, manage, maintain and report on process workflows in near real time.

New compliance requirements are popping up all the time and must be integrated into existing workflows. New regulations and iterations of existing regulations present an ever-changing compliance landscape. Increasingly complex commercial relationships and shifting internal compliance needs make the process of managing the program more difficult.

Changing roles and responsibilities add another layer of complexity to process implementation and management.

CCO tools integrate new requirements, balance existing compliance requirements and regulations, and integrate the entirety into the compliance and control framework. Features within this capability include:

- Regulatory change management
- The ability to handle feeds from regulatory and oversight entities
- Mapping of new and modified requirements into existing frameworks
- Integration with compliance processes
- Support for granular roles and responsibilities within compliance processes
- Alignment with and support for an incident escalation process

Investigative Case Management

No matter how strong and mature processes are, there will invariably be violations and other incidents. The ability to input, track, escalate, manage and close cases related to active and passive compliance violations brings the system full circle. Case management supports tracking and reporting on compliance-related incidents. Features within this capability include:

- Compliance incident management/loss event capture and analysis (people, process and technological)
- Support for interdepartmental collaboration
- Incident (instances of noncompliance with an internal policy or external regulation) management workflow
- Whistleblower capabilities
- Tracking and escalation process

CCO technologies are some of the most mature in the risk management solution marketplace. Most commonly, they are used to comply with the Sarbanes-Oxley Act (SOX) and similar financial reporting rules. Capabilities to support anti-fraud or anti-bribery and ethics compliance are starting to be incorporated into CCO solutions. Gartner has seen some increased focus from clients on broader compliance efforts, but the growth has been slow. This is partly because it is difficult to align different compliance functions and their varying working methods. On the other hand, some compliance functions are simply unwilling to give up their established solutions that reasonably meet their own isolated needs.

Market Direction

The corporate compliance and oversight solutions market is mature in its primary feature set, but there are some variations in certain areas that are differentiators for organizations selecting a CCO solution provider.

Quick and Easy Implementation

Gartner hears varying experiences from organizations about their experience implementing a CCO solution. Implementation can be unsuccessful and long, especially if an organization fails to clearly define the scope of the workflow or process they are looking to automate. Some organizations even encounter high costs in deploying compliance management solutions, as their installation requires significant external consultancy. The need for external involvement in deployment makes solutions difficult to maintain in-house. Solutions that allow customers to take greater control of deployment from the beginning without significant implementation effort reduces consulting costs and ensures the internal support team understands the solution, making it easier to sustain. Organizations seek solutions that require no external consulting beyond initial training and on-site support during the initial design phase. As such we have seen some vendors have programs that allow quick time to implementation.

User-Friendly Interface

Compliance is one of the areas that touches all areas of organization and is increasingly involving more lines of business (LOBs) and departments. The ability of the solution to be user-friendly and intuitive enough for both end user and the administration to require minimal training, technical knowledge or skill is becoming more important. Where historically solutions were fit for "power users" with considerable experience and background in compliance management who perform compliance related tasks on a daily basis, vendors are increasingly looking to improve the usability of solutions so that users with little experience are also able to easily use the platform with minimal training. This aspect will become more important as organizations increasingly leverage these solutions for cross-departmental collaboration.

One of the areas where vendors are improving usability is around workflow engines. Some vendors have visual workflow capabilities that allow more mature organizations to implement complex workflows but also provide less-mature organizations with a simplified way to set review and approval workflows.

SaaS Deployment Model

There are three primary deployment options: cloud, hosted or on-premises. Most vendors provide a SaaS model of deployment, with the option of hosting the software at a customer's data center or their own facilities. The current deployment model leans more heavily toward on-premises, but we will continue to see a shift to a SaaS-based deployment model as more organizations look to benefit from short time to implement and a lower cost based on a per-user pricing model. As organizations increase their movement of workloads into the cloud, more vendors will look to provide solutions that are cloud-API-aware and become cloud-first providers.

Visualization Capability

Vendors have been improving visualizations capability as a broader range of users seek access to compliance data. Information must be presented in a way that allows users to easily extract data that is relevant to that user. Vendors have placed greater emphasis on visualization and the ability to

drill down to underlying information rather than providing static reports. Some CCO solutions have the ability to integrate with other visualization and reporting platforms or services.

Regulatory Content and Intelligence

Regulatory content is a key requirement in CCO solutions, as they are used to populate policies, map controls and control activities to specific regulations. While content is important, the ability to connect the data points to provide intelligence and value is also important. Some organizations want to connect their internal loss data with regulatory requirements to understand the sanctions they may face and aggregate risk data across silos so that it can be used to make better business decisions. Certain verticals or regions have their own unique regulatory requirements. Regulatory feeds should not be limited to a vendor's own regulatory content library, but should also allow regulatory feed from third parties. More vendors are expanding the range of content-based solutions to support this requirement.

Industry Alignment

It is important for an organization to select a vendor that has a good background and strength in the organization's industry so that the vendor is able to provide the necessary feeds, content and expertise. Some vendors focus on specific industries and their compliance requirements, while some do not offer customized capabilities or features for different verticals. Some verticals are more unique than others. Examples include energy and utilities, mining, and construction, all of which are safety-based, or pharmaceutical and biotech, which have FDA requirements that are not common in other industries. These type of organizations may wish to consider compliance management vendors that focus only on their industry.

Geographical Alignment and Support

Organizations are becoming more complex. They are covering different business processes, jurisdictions and even languages. Vendors' geographical alignment, presence and support can be key considerations, especially for global organizations. Customer support level and multilingual support varies by different vendors. Most vendor tend to be more present in North America and Western Europe, which are the regions with the highest level of market penetration for CCO solutions. Organizations operating outside of these regions should ensure that offerings and support are available in locales where the organizations conduct business and compliance activities.

Move to Integrated Risk Management

Gartner sees a growing focus from organizations around risk management and the integration of compliance with risk management. Some large organizations look for a single compliance management solution to serve all compliance functions and activities, and in many cases seek integration with risk management and audit practices. Scalability of the CCO solution is important for organizations looking to leverage the platform for other IRM solution (see Note 1) use cases, such as operational risk management, IT risk management, IT vendor risk management, audit management, enterprise legal management and business continuity management. For organizations that have implemented integrated risk management solutions, the CCO capabilities to support control assessments, policy management, regulatory change management and reporting should be

supported from the platform. With some solutions, continuous monitoring of transactions for gifts and entertainment expenses may also be supported, which is a helpful capability for anti-bribery compliance. Ethics compliance training content often must be separately sourced; ethics compliance vendors can confuse buying decisions by marketing themselves as risk management solution vendors, but most of them cannot effectively support the workflow, analysis and reporting needed for SOX compliance.

Third-Party Compliance

A growing area of interest concerns third-party compliance management. With the increased regulatory focus on third-party risks and expanding regulatory vendor risk management (VRM) oversight requirements, Gartner has seen organization's efforts to improve the visibility into their exposure to third-party risks and third-party compliance. Many CCO solutions have functionality that allows third-party users to access compliance-related assessments, notify third parties of required controls and policies, and provide a platform for third parties to attest to their compliance knowledge. In addition, many CCO solution providers have IT VRM capabilities (see "Magic Quadrant for IT Vendor Risk Management").

Integration With Third-Party Systems

Integration with third-party systems is important. Many CCO solutions in the market today can be integrated with other enterprise applications such as ERP systems. These systems leverage operational and business data such as HR, assets and materials so organizations are able to get full data and business process integration with core business operations, and visibility and control across the organization.

Representative Vendors

The CCO market is composed of two broad categories of providers:

- IRM solution vendors that provide enhanced abilities or modules that support the mandates of compliance leaders
- Purpose-built, stand-alone compliance software and service providers, generally targeted at specific industries

Due to the significant overlaps and synergies in compliance support with other IRM categories, the majority of vendors with products in the CCO space fall into the former category.

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.

- 4C Strategies
- ACL Services
- Allgress

- BWise
- Convercent
- Dell Technologies (RSA)
- GAN Integrity
- Greenlight Technologies
- IBM
- Ideagen
- LockPath
- MetricStream
- Navex Global
- ProcessGene
- Protiviti
- Quantivate
- Resolver
- Riskonnect
- Rsam
- SAI Global
- SAP
- Thomson Reuters
- Wolters Kluwer

Market Recommendations

Buying decisions for CCO solutions are based on organizational size and geography, scale of compliance program, level of regulatory oversight, number and types of nonregulatory compliance requirements, geographic spread of teams, and relationships with IT and other risk management functions.

Security and risk management leaders supporting compliance programs in selecting CCO solutions should:

- Select vendors based on alignment with current and future IRM initiatives and investments, especially if there is buy-in and readiness from enterprise risk, compliance, business operations,

IT, security, vendor management, audit, and business continuity teams to implement integrated risk management solutions.

- Evaluate compliance-focused vendors, especially if compliance is a significant business driver. Many vendors in the market focus their compliance management offerings on the requirements and needs of specific industries. For some organizations, it may be advisable to focus on the narrower needs of your industry, rather than investing in larger, broader, more expensive IRM solutions.
- Shortlist vendors based on alignment with prioritized requirements such as pricing (see Note 2), delivery options, geographical alignment and support availability, industry alignment, regulatory content availability, integration capability, and scalability of the platform to add other IRM solution modules.
- Assess your needs and the availability of regulatory content. It is critical to have a clear understanding of what types of content you need to access, now and in the future. All offerings come with the basics, but depending on your industry, ensuring that the products you evaluate meet your organization's needs regarding regulatory content is key.
- Assess deployment options in line with your organization's information classification, outsourcing, business continuity and information security management policies. Identify short- and long-term appetite for SaaS, hosted or on-premises deployment models.

Gartner Recommended Reading

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

"Definition: Integrated Risk Management Solutions"

"Hype Cycle for Risk Management, 2017"

"Market Guide for Integrated Risk Management Solutions"

"Security Compliance and Audit Management Primer for 2017"

"Transform Governance, Risk and Compliance to Integrated Risk Management"

Note 1 Definition of Integrated Risk Management (IRM) Solutions

Gartner defines IRM as a set of practices and processes, supported by a risk-aware culture and enabling technologies that improves decision making and performance through an integrated view of how well an organization manages its unique set of risks. Consequently, Gartner recommends an IRM approach to build and sustain successful risk management programs.

Note 2 Pricing Model

Most offerings are licensed on a per-user basis, with most vendors offering multiple tiers of user accounts with price levels commensurate with the level and type of usage.

Power users — Are heavily involved in compliance management, regularly use the CCO system and, typically, have primary compliance program responsibilities

Standard users — Do not have primary compliance program responsibilities, but need access to the system for periodic assessments, collaboration and reporting

Casual users — May access the system infrequently for specific "asks" such as responding to surveys, reviewing policy or accessing training

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp