Market Guide for Corporate Compliance and Oversight Solutions

Published: 30 January 2019 **ID:** G00341322

Analyst(s): Elizabeth Kim

Security and risk management leaders should seek CCO solutions that enable a cross-enterprise approach to compliance activities that most affect the regulatory oversight of corporate governance.

Key Findings

- Corporate compliance and oversight (CCO) tools provide support for standardization of compliance activities and automation to increase efficiency and effectiveness of compliance management programs.
- The CCO solution market is fragmented due to the dynamic nature of regulatory requirements and the various ways organizations approach compliance management.
- Organizations typically leverage either static tools (such as spreadsheets or pure-play compliance management solutions), or integrated risk management solutions for their compliance management needs. Most first-time buyers approach CCO solutions from a need for a specific capability, which can eventually lead to organizations investing further in other applications within the CCO solution suite.

Recommendations

Security and risk management leaders procuring CCO solutions as part of managing technology, information and resilience risk:

- Assess the maturity of your compliance program. CCO solutions are about automating many of the workflows and processes, so make sure to have a level of process maturity.
- Evaluate vendors based on alignment with your organization's size, geographic spread, scale and maturity of the compliance program, level of regulatory oversight, number and types of nonregulatory compliance requirements, and relationships with IT and other risk management functions.
- Develop an effective "shortlist" of vendors by evaluating them against your current and future integrated risk management (IRM) initiatives, as leveraging the same platform for multiple risk and compliance management applications is cost-effective.

Strategic Planning Assumption

By 2023, more than 30% of total organizations' spending on IRM will be from CCO solutions, up from approximately 24% in 2018.

Market Definition

Corporate compliance and oversight is part of a growing category of integrated risk management solutions (see "Top Use Cases and Capabilities for Integrated Risk Management"). CCO tools provide the 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 and management, aggregation and normalization, control assessment and monitoring, workflow and business process management, and investigative case management (see Figure 1).

Figure 1. Corporate Compliance and Oversight Solutions

Source: Gartner (January 2019)

Market Description

Policy implications of the regulatory environment, regulatory change management, control automation, and case and incident management continue to be an important part of an organization's IRM strategies. To support an organization's compliance management program, CCO solutions need to provide capabilities that align with and support the following areas.

Policy Development and Management

Policies and policy statements are among the most critical strategic controls for asserting management perspective and requirements. Policies influence 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
- Policy 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 compliance leader's role 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 input 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 U.S. Foreign Corrupt Practices Act, Gramm-Leach-Bliley Act and Sarbanes-Oxley Act
- Industry-specific regulatory guidelines, such as from the U.S. FDA, FERC, FAA, HACCP and FAR; Basel III; anti-money-laundering controls; and New York State Department of Financial Services
- Information security and privacy regulations, and other similar mandates, such as from the U.S. HIPAA, ISO 27001, NIST 800-53 and PCI DSS; EU GDPR; and China's Cybersecurity Law
- Risk frameworks such as COBIT, the Committee of Sponsoring Organizations of the Treadway Commission and ITIL
- Business continuity management frameworks, such as the FFIEC Business Continuity Planning handbook, ISO 22301 and ISO 22317, NFPA 1600, and the National Incident Management System/Incident Command System of the United States Department of Homeland Security/ Federal Emergency Management Agency
- Fraud management and other business-aligned risk areas
- Access to additional data feeds (for example from LexisNexis, Thomson Reuters or law firm websites) to supplement out-of-the-box content
- Ability to support custom compliance requirements

- Ability to address conflicts between various requirements in a defensible manner

Control Assessment 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 facilitating communications 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
- 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, invariably, there will 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

Areas CCO Solutions May Not Fully Address

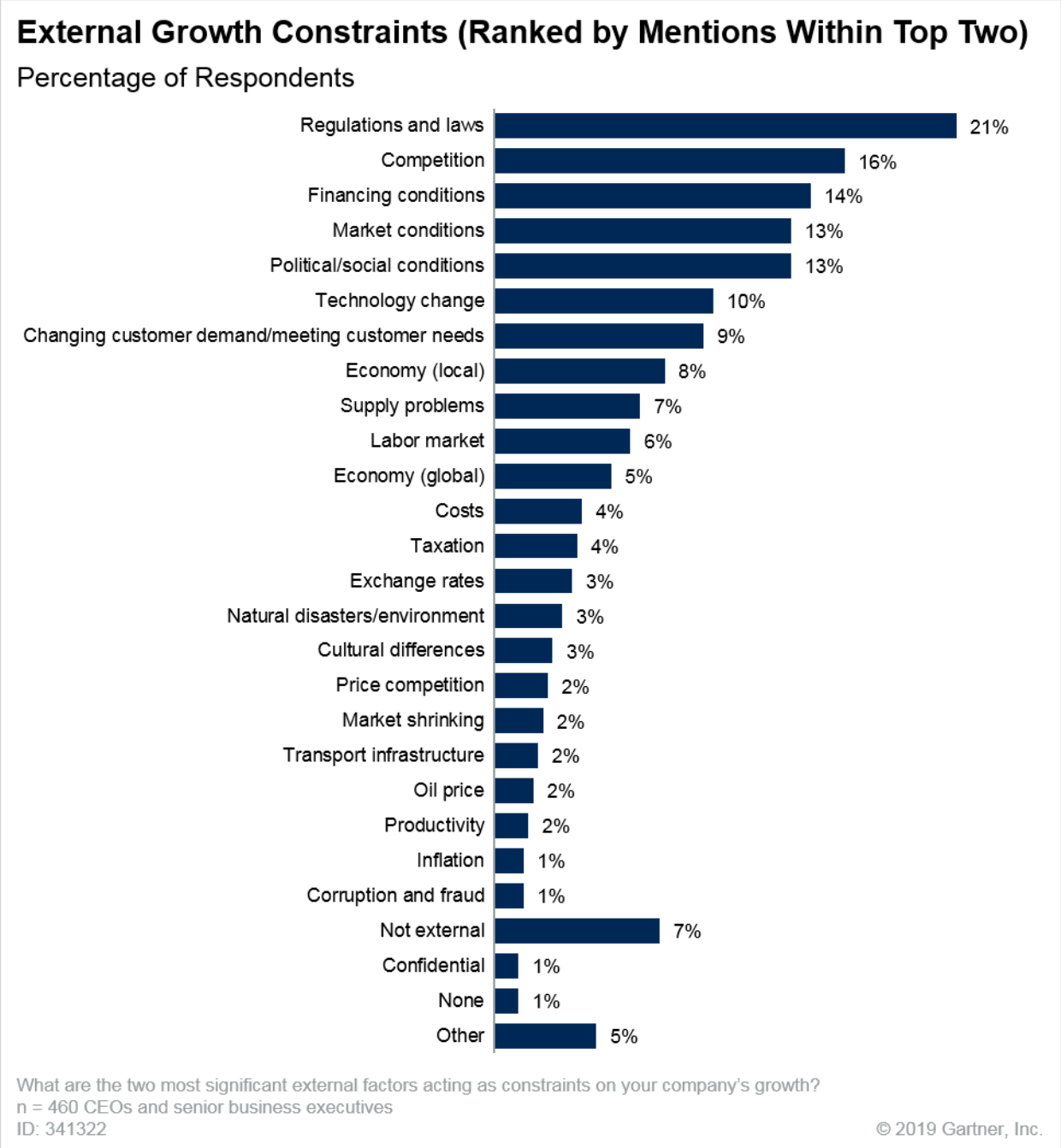
It is important for potential buyers of CCO solutions to note areas that vendors may have some capabilities, but may not fully support today. These include, but are not limited to:

- Use of machine learning and natural language to interpret regulations
- Ability to track compliance requirements and map them to existing practices for the purpose of budget allocations that are otherwise deprioritized
- Ability to track efforts in compliance activities in order to track the cost of control testing, audit prep, audit support and remediation coordination. Currently, most organizations track only cost of control implementation and associated advisory/consulting services.

Market Direction

With regulatory proliferation and the increased pace of regulatory change, the global legal and regulatory landscape continues to become more complex. As a result, compliance leaders have seen their roles become more visible, more challenging and more important within their organizations during the past 10 years. Compliance leaders are facing increased demands from customers, partners, boards of directors, and regulatory bodies to ensure that all applicable compliance obligations are met consistently. Additionally, they are demanding that organizations stay up to date and be prepared for the risk of noncompliance (which compliance teams should do by consulting legal counsel). Based on the 2018 Gartner CEO Survey, the highest percentage of CEOs and senior business executives responded that regulations and laws were the most significant external factors acting as constraints to their company's growth (see Figure 2).

Figure 2. External Growth Constraints (Ranked by Mentions Within Top Two)



Data is based on Gartner's 2018 CEO Survey.

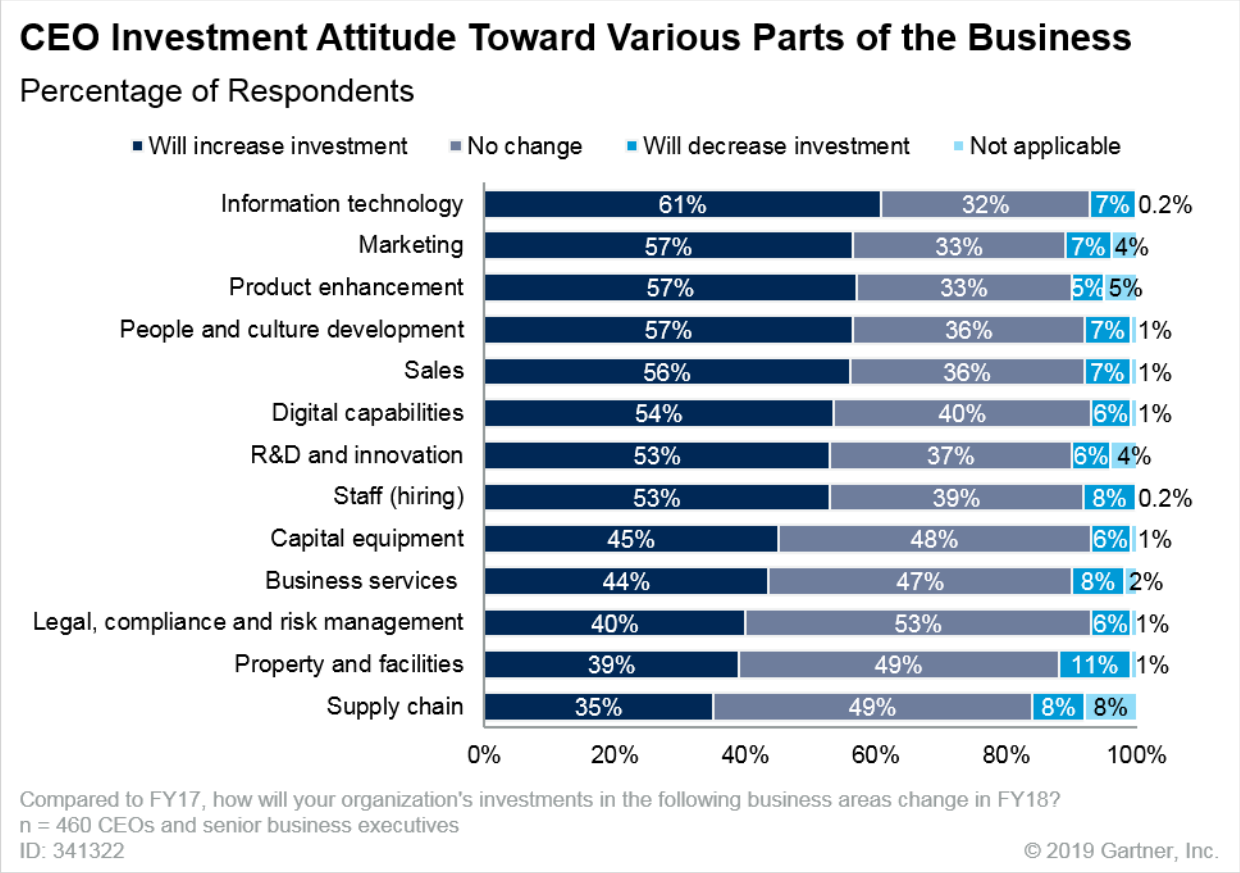
Source: Gartner (January 2019)

Additionally, the "Cost of Compliance 2018" survey by Thomson Reuters Regulatory Intelligence indicated the top challenges identified in the year ahead by risk and compliance practitioners.

Those top challenges were continuing regulatory change, data privacy and GDPR, enhanced monitoring and reporting requirement, increased regulatory scrutiny, and implementation of regulatory change.[1]

With such complexity of the regulatory landscape, and greater scrutiny from internal and external stakeholders around regulatory compliance, compliance leaders are starting to move away from manual processes. Compliance leaders are moving away from the use of static tools such as Microsoft Excel spreadsheets and Word documents to manage compliance requirements, to solutions that help automate and standardize compliance management processes. Gartner's survey showed that 93% of CEOs and senior business executives indicated that they will either maintain, or increase investments in legal, compliance and risk management (see Figure 3).

Figure 3. CEO Investment Attitude Toward Various Parts of the Business



Data is based on Gartner's 2018 CEO Survey.
Percentages may not total 100% due to rounding.

Source: Gartner (January 2019)

CCO technology offerings are some of the most mature in the risk management solution marketplace. However, use of CCO solutions as a means to support an organization's broader compliance efforts is low. This is partly because organizations find it difficult to align different

compliance functions and their varying working methods, including the solutions they use that reasonably meet their own isolated needs. As a result, CCO solutions are often used to comply with a specific regulatory requirement, most commonly, the Sarbanes-Oxley Act (SOX) and similar financial reporting rules. Ideally, organizations should take a holistic approach to compliance versus managing compliance requirements in silos. Organizations that treat each set of compliance requirements as separate projects across different teams and departments will end up spending more money and time. At the same time, it will result in a lack of coordination that is required to be well-prepared to respond to audits. Merging all the compliance requirements and looking at them through a single compliance lens will help organizations achieve economies of scale through unified and standardized compliance and tool investment.

On the other hand, some organizations, especially first-time buyers, approach CCO solutions from a need for a specific capability. For example, the hotline and case management function is a popular requirement of organizations. This can eventually lead to organizations investing further in other applications within the CCO solution suite. As such, the vendor landscape for CCO solutions will continue to be highly fragmented due to the diverse nature of compliance requirements and the various angles that organizations approach compliance management. The CCO solution market is not dominated by IRM platform providers unlike much of the other risk management solution markets, and we see equally strong market presence from pure-play compliance management solution providers.

Market Analysis

Selecting a solution in a fragmented market may be difficult. Based on feedback from organizations that have implemented a CCO solution, the following criteria should be considered, in addition to the vendor's ability to sufficiently fulfill the key features outlined above.

User Experience and Solution Scalability

Compliance is an area that touches on all parts of the organization and requires input from all areas of the business — from audit, legal, privacy, IT and security, to all business functions. One of the organization's pitfalls is not getting all the relevant stakeholders involved in managing compliance, ending up with a lot of gaps in policies and controls, and a lot of information not being shared properly across the organization. This implies that CCO solutions not only should support the requirements for managing a compliance program, but also focus on sufficiently supporting the collaborative nature of compliance management. This can be done by providing a simple and user-friendly platform for even the nonexpert and infrequent users. This may include small things such as autosave functions, requiring fewer clicks and, for ethics compliance management solutions, an interactive code of conduct that is engaging for employees. Some CCO solutions are supported on users' mobile devices so they can do simple tasks such as signing off on policies using those devices.

Additionally, to support the cross-organizational nature of compliance management, a CCO solution should be evaluated in how scalable the solution is to meet the requirements of a small team supporting a large number of employees and third parties.

Reporting Function and Quality of Reports

CCO solutions should ease the organization's efforts in gathering data and producing reports, as Gartner finds that some customers end up spending hours producing reports. CCO solutions should not only help organizations reduce the time they spend pulling out reports, but the quality of reports is also an important factor. As such, CCO solution vendors continue to place emphasis on the visualization capability and ability to drill down to underlying information rather than providing static reports. Some CCO solution vendors provide a benchmarking capability. This is to meet the needs of organizations that want to understand how they compare to their industry peers, as well as which metrics other organizations are reporting to the board.

In addition, some global organizations that have leveraged CCO solutions cited the vendor's ability to produce a high quality of translated reports as an important factor in vendor selection.

Regulatory Content and Intelligence

Regulatory content continues to be a key requirement in CCO solutions, as they are used to populate policies, map controls and control activities to specific regulations. Organizations increasingly seek out-of-the-box content, and many organizations seek a central source for all the regulations their organizations need to comply with. 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, in order 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.

Integration With Third-Party Systems

Integration with third-party systems is important. Many CCO solutions in the market 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 can get full data and business process integration with core business operations, and visibility and control across the organization.

Deployment Model

There are three primary deployment options: cloud, hosted and 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. However, we will continue to see a shift to a SaaS-based deployment model. This is because 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. With organizations in the EU, there are requirements for the solution provider's data center to reside in EU due to data residency issues.

Implementation

Organizations report variations in their experience implementing a CCO solution. Solutions that allow customers to take greater control of deployment from the beginning without significant implementation effort reduce consulting costs and ensure the internal support team understands the solution, making it easier to sustain. Furthermore, the level and quality of professional services as they relate to the implementation, onboarding and training provided by the CCO vendor and/or its partners are an important part of a successful implementation, in addition to the tool itself.

While organizations seek solutions that require no external consulting beyond initial training and on-site support during the initial design phase, this may not be realistic for some. A large number of organizations are first-time buyers of CCO solutions, and they seek expertise in framework and methodology on how to approach risk and compliance. Depending on the maturity of the compliance management programs, some organizations may require a higher level of consulting. Most CCO solution providers do not provide the full extent of consulting services, but they have partnerships with consultancies.

Geographical Alignment and Multilanguage Support

The level of customer support and multilingual support varies across vendors. Most vendors tend to have more presence 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. Furthermore, CCO solutions should support multiple languages. For example, employee portals should be able to support various languages, and hotlines should provide native language support for employees across multiple regions.

Representative Vendors

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.

Market Introduction

At a very high level, CCO solution providers are either pure-play providers, or IRM solution providers. Pure-play compliance management solution providers focus solely on providing compliance management functionality (most likely, supporting a specific compliance requirement). On the other hand, IRM solution providers offer compliance management features as part of their broader risk management solution portfolio. While it is difficult to capture all the CCO solution providers in this dynamic market, Table 1 represents a list of vendors that are frequently mentioned in Gartner's interactions with end users. (Notes 1 and 2 provide more detail about vendor selection and Gartner's initial market coverage for this Market Guide.)

Table 1. Representative Vendors in Corporate Compliance and Oversight Solutions

Vendor
4C Strategies
ACL
Allgress
BWise
Convercent
Dell Technologies (RSA)
GAN Integrity
i-Sight
IBM
Ideagen
Lockpath
MetricStream
Mitratech
NAVEX Global
Optial
ProcessGene
Protiviti
Quantivate
Resolver
Riskonnect
Rsam
SAI Global
SAP
StarCompliance

Vendor
Thomson Reuters
Wolters Kluwer
Workiva

Source: Gartner (January 2019)

Market Recommendations

Security and risk management leaders supporting compliance programs and audit management in choosing CCO solutions:

- Assess the maturity of your compliance management program. Process comes before the tool, which means that understanding what is going on in your compliance management program is critical before implementing any solution. CCO solutions are about automating many of the workflows, so you need to have a level of process maturity.
- Understand the resources for implementing and running the tool, including the level of effort and dedicated staff with corresponding skills to implement and maintain the tool over time.
- Establish cross-functional relationships with relevant functions such as security, audit, legal and privacy to identify where compliance management processes such as the regulatory requirement tracking and control mapping and implementation overlap with these functions.
- Develop an effective shortlist of vendors by evaluating their capabilities against your current and future IRM initiatives and investments. This means understanding how much risk management capability you require now and in the future. Many providers offer solutions that span compliance and risk management; so, for users that have implemented IRM solutions, CCO capabilities should be supported from the platform. This includes CCO capabilities to support control assessments and testing, risk assessment and remediation, policy management, regulatory change management, and reporting. Leveraging the same platform for multiple applications can be cost-effective.
- Evaluate vendors based on the scope of compliance they cover. For example, ethics compliance vendors can confuse buying decisions by marketing themselves as risk management solution vendors; however, most cannot effectively support the workflow, analysis and reporting needed for other compliance requirements such as SOX compliance. Similarly, not all CCO solution providers have capabilities to support IT compliance requirements.
- Consider the following when selecting a CCO solution provider:
  - Your organization’s size
  - Geographic spread of the teams

- Scale and maturity of your compliance program
- Level of regulatory oversight
- Number and types of nonregulatory compliance requirements
- Relationships with IT and other risk management functions

Acronym Key and Glossary Terms

COBIT	Control Objectives for Information and Related Technology
FAA	Federal Aviation Administration
FAR	Federal Acquisition Regulation
FDA	Food and Drug Administration
FERC	Federal Energy Regulatory Commission
FFIEC	Federal Financial Institutions Examination Council
GDPR	General Data Protection Regulation
HACCP	Hazard Analysis Critical Control Point
HIPAA	Health Insurance Portability and Accountability Act
ISO	International Organization for Standardization
NFPA	National Fire Protection Association
NIST	National Institute of Standards and Technology
PCI DSS	Payment Card Industry Data Security Standard
SOX	Sarbanes-Oxley Act

Gartner Recommended Reading

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

"Hype Cycle for Risk Management, 2018"

"Magic Quadrant for Integrated Risk Management"

"Critical Capabilities for Integrated Risk Management"

"Top Use Cases and Capabilities for Integrated Risk Management"

Evidence

[1] "Cost of Compliance 2018 Report: Your Biggest Challenges Revealed," Thomson Reuters

Note 1 Representative Vendor Selection

The vendors named in this Market Guide were selected because they provide functionality to support the five key requirements for managing a compliance program: policy development and management, aggregation and normalization, control assessment and monitoring, workflow and business process management, and investigative case management. Gartner has received the most client interest (end-user inquiry) about these vendors.

Note 2 Gartner's Initial Market Coverage

This Market Guide provides Gartner's initial coverage of the market and focuses on the market definition, rationale for the market and market dynamics.

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