G00263380

Hype Cycle for Governance, Risk and Compliance Technologies, 2014

Published: 17 July 2014

Analyst(s): John A. Wheeler

As companies seek to transform into the "digital businesses" of the future, they are faced with a dynamic "cyber risk" environment that requires more advanced risk management capabilities. The resulting hype is driving greater demand for governance, risk and compliance (GRC) technologies.

Table of Contents

List of Tables

List of Figures

Analysis

What You Need to Know

This year's Gartner CEO and Senior Executive Survey highlights the adoption of a "risk-on" attitude by CEOs as they look for ways to transform their companies into digital businesses (see "The 2014 Gartner CEO and Senior Executive Survey: 'Risk-On' Attitudes Will Accelerate Digital Business") In fact, the survey noted that more than half of the business leaders intend to increase investment in technology and digital in 2014. At the same time, CEOs have a weak understanding of what digital business will mean for their company. Combined with ever-increasing cyber risks related to massive data breaches and system failures, the need for GRC technologies to help senior business leaders fully comprehend their digital risk profile is paramount.

The technologies discussed in this research are relevant to IT risk managers, IT operations managers, and those responsible for maintaining the configuration and integrity of the organizational information infrastructure. This Hype Cycle includes products that are used by IT to manage its own activities, and products for use by strategic and operational managers (for example, operational risk managers, enterprise risk managers, audit managers and legal officers) to evaluate risks, set policy and provide assurance that risks are mitigated effectively.

The Hype Cycle

The Hype Cycle for GRC technologies contains an assortment of services, software platforms, applications and tools that companies can use to enhance their abilities to better govern and control business processes to achieve desired business outcomes. Gartner defines GRC in the following way (see "Definition: Governance, Risk and Compliance"):

- **GRC** is a set of processes, supported by enabling technologies, that improve decision making and performance through an integrated view of how well an organization manages its unique set of risks:
  - **Governance:** The process by which policy and decision rights are set, maintained and effectively communicated throughout an organization.
  - **Risk management:** The process for ensuring that important business decisions and behaviors remain within the overall risk appetite and acceptable risk tolerances associated with the strategic objectives of an organization.

- **Compliance:** The process of adherence to policies through related controls. Policies can be derived from internal directives, procedures and requirements, or external laws, regulations, standards and contractual agreements.

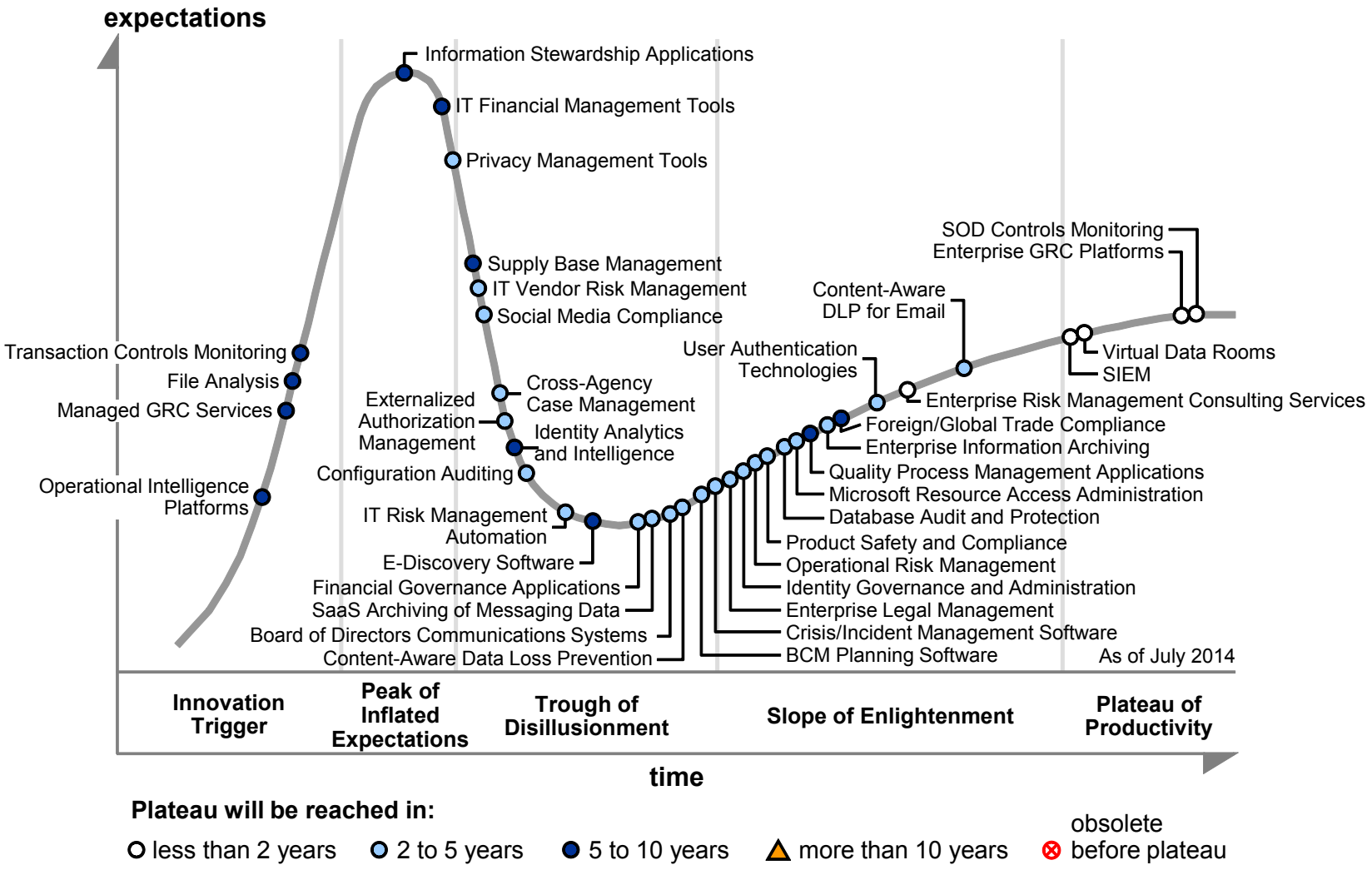
GRC remains a top business priority for senior executives, according to Gartner's 2104 CEO and Senior Executive Survey. In fact, it is on par with other critical business priorities, such as R&D and innovation, as well as efficiency and productivity. Given that GRC is viewed as a core priority of this sort, it is understandable that the market for GRC technologies has now matured beyond foundational solutions, such as enterprise and IT GRC platforms, to focus more on purpose-built applications that can easily integrate with the GRC systems of record.

As a result, Gartner is shifting its primary research focus on GRC technologies such as IT risk management, operational risk management, IT vendor risk management and business continuity management. In addition, increasing focus on strategies to build a cohesive and comprehensive GRC application portfolio is reflected in our evolving research of GRC pace-layering methodologies (see "How to Use Pace Layering to Build a GRC Application Strategy" and "Predicts 2014: Advances in Risk Management Technology Will Improve Corporate Performance and Public Policy").

This year's Hype Cycle also demonstrates the greater sophistication of risk management approaches and their related GRC technologies. Areas such as social media compliance, operational intelligence platforms and information stewardship are critical components of the evolving digital business landscape. Technologies found on this Hype Cycle provide the risk insights that are needed to create strategies to build successful digital business processes.

At the same time, continued changes in the regulatory compliance landscape dominate the demands placed on business today. Regulatory change ranked second on the list of factors acting as constraints on growth in the 2014 Gartner CEO and Senior Executive Survey. Areas such as third-party risk management, privacy management and enterprise legal management are driving demand for GRC technologies to support the associated compliance-related needs of companies today.

Figure 1. Hype Cycle for Governance, Risk and Compliance Technologies, 2014

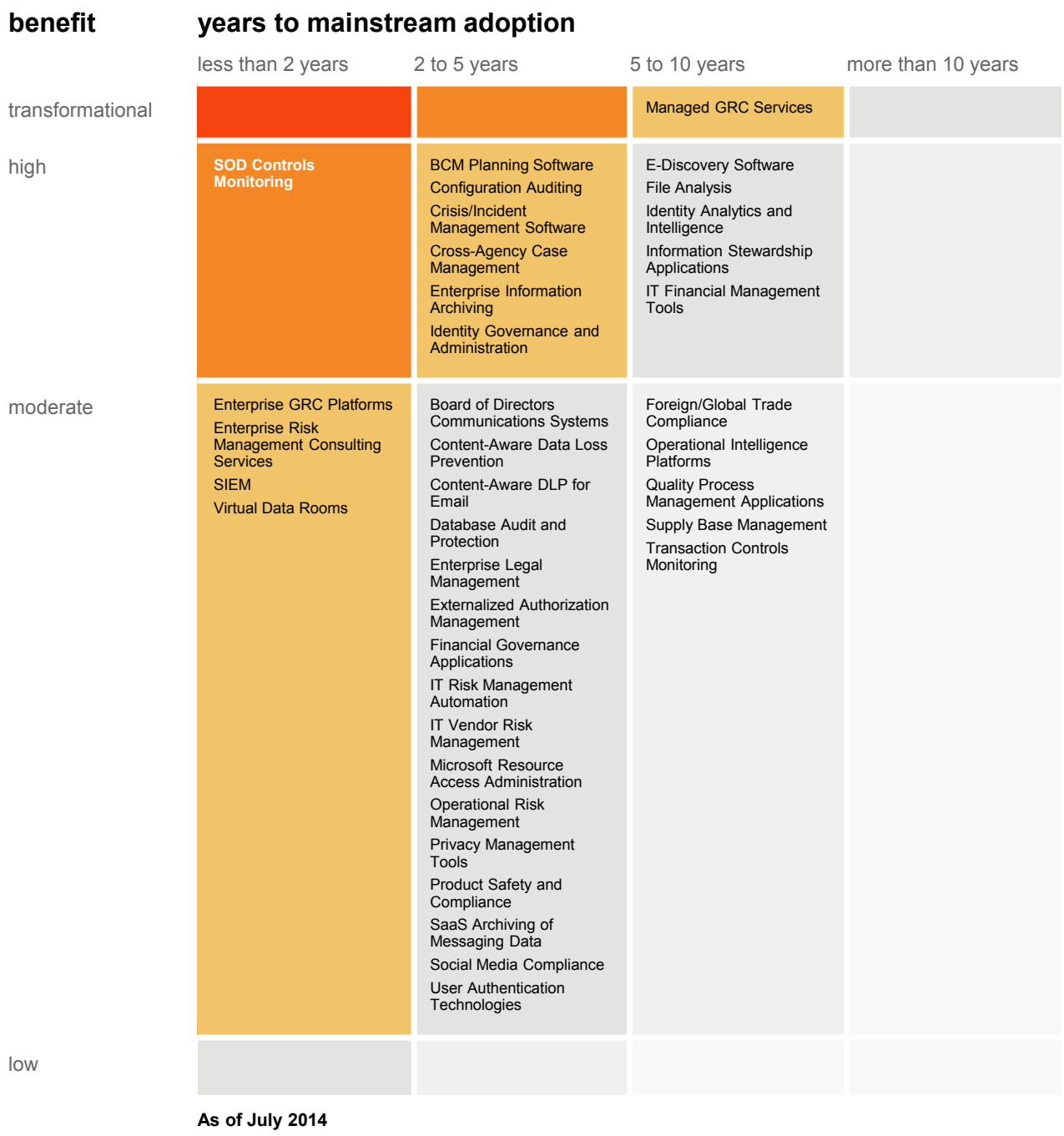


Source: Gartner (July 2014)

The Priority Matrix

The color and position of the technologies on this Hype Cycle tell the story of a maturing set of technologies and services that are rapidly becoming used as enterprise best practices in their applicable areas. Although only one technology provides transformational benefits and perhaps some others with a higher business value may be overly optimistic, the overwhelming majority provides solid utility. The managed GRC services technology represents the one area that may prove to provide transformational benefits for organizations looking to lower the overall cost of meeting regulatory requirements that are not core to their strategic objectives. Other technologies, such as business continuity management planning software and crisis/incident management software, can provide high benefit in managing risk events that could lead to significant disruption of business operations (see Figure 2).

Figure 2. Priority Matrix for Governance, Risk and Compliance Technologies, 2014



Source: Gartner (July 2014)

Off the Hype Cycle

- Enterprise risk management applications has been renamed and recast as "operational risk management."
- ERP separation (or segregation) of duties (SOD) controls, records management and SOD monitoring controls have matured beyond the Plateau of Productivity.
- IT GRCM has been renamed and recast as "IT risk management automation."
- Legal and regulatory case management has been subsumed within enterprise legal management.
- Legal GRC has been subsumed within operational risk management.
- Risk assessment for business continuity management (BCM) has been subsumed within BCM planning software.
- Social GRC has been subsumed within social media compliance.
- Third-party risk management has been replaced by IT vendor risk management.

On the Rise

Operational Intelligence Platforms

Analysis By: W. Roy Schulte

Definition: An operational intelligence platform is a suite of development and runtime software tools that monitor, alert or support interactive operational decision making using data about current conditions. These platforms typically have adapters to ingest events and other data; databases to hold context data; logic to find patterns, anomalies and other threats and opportunities; rule processing and analytics; interactive dashboards; alerting facilities; and capabilities to trigger responses in applications, devices or workflow tools.

Position and Adoption Speed Justification: This is still a relatively new product category. It will take several years to reach the Peak of Inflated Expectations and up to 10 years to reach the Plateau of Productivity.

The term "operational intelligence platform" was coined in 2012 because there was no general label for commercial off-the-shelf software that supported this role (see "Commercial Operational Intelligence Platforms Are Coming to Market"). However, the idea is not new as some companies have developed custom applications to serve this purpose, and commercial products that do this have been used in some industries for many years. They are known by labels specific to their usage scenarios, which include supply chain visibility, business process monitoring, business activity monitoring, manufacturing operations intelligence, customer contact center monitoring, truck fleet management and others. Operational intelligence platform is a broad category that encompasses such purpose-specific monitoring systems, as well as general-purpose products that can be tailored to virtually any operational business scenario.

Operational intelligence platforms can trigger responses automatically (decision automation) or provide information to people (decision support). They can address real-time or non-real-time decisions. When operational intelligence platforms are used for real-time decision automation, they are performing the role of a *real-time decisioning* platform, a technology that was previously listed (see "Hype Cycle for Business Intelligence and Analytics, 2013"). Operational intelligence platforms sometimes implement *decision management,* a discipline that uses rules or prescriptive analytics to generate complete decisions. In other situations, operational intelligence platforms provide descriptive, diagnostic or predictive analytics. These are not classified as decision management because they do not specify the decision to be executed, they only provide supporting information that helps people make the decisions.

User Advice: Architects and analysts should use operational intelligence platforms to provide a layer of monitoring oversight for processes and operations, or to provide value-added context information or analytics for interactive operational decisions. Operational intelligence platforms can do more than provide visibility. They may sense variances from a baseline of historical, expected or desired activity and send alerts or trigger responses.

Architects and analysts should work with business managers and users to identify what data needs to be maintained in the context store, and how long it should be held. A context store can integrate information from multiple applications, sensors or other sources inside and outside a company. Context information is continuously (or at least frequently) refreshed so that decisions reflect the most current and complete view of conditions.

Operational intelligence platforms are one of the technologies well suited to implementing intelligent business operations. They are relevant when retrofitting monitoring, alerting or interactive decision-making capabilities on top of processes or operations that will not be replaced or fundamentally modified, or when implementing monitoring systems across heterogeneous operations and processes that span multiple business units or disparate application packages. However, architects should consider intelligent business process management suite (iBPMS) products, instead of operational intelligence platforms, when implementing new business processes or making fundamental changes to processes. iBPMS products also have monitoring, alerting and decision support capabilities, so they overlap operational intelligence platforms. iBPMSs tend to have superior workflow, adaptive case management and structured process orchestration capabilities, but inferior monitoring and alerting capabilities.

Business Impact: Operational intelligence platforms give businesses a broad, holistic and current view of their operations. Without these platforms, most operational decisions rely on daily, weekly or monthly reports, or narrow views into individual applications or devices. Businesses have no way to monitor the up-to-the-minute status of end-to-end business processes, and have limited visibility into conditions in adjacent parts of the business or the outside world. Traditional BI systems report results, whereas operational intelligence platforms sense and respond to anomalies or other threats and opportunities.

Operational intelligence platforms operationalize objectives such as reducing customer churn, expanding sales and reducing the cost of manufacturing or delivery. They help people share a common operating picture, which improves their ability to collaborate when making business

decisions. They also improve the quality of decisions by providing more contextual information and logic to people and application programs.

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: Access Intelligence; Aha Software; Axway; C3global; ClearPriority; Feedzai; Greenlight Technologies; Guavus; Intelligent InSites; Kinaxis; Kofax; Lavastorm Analytics; Microsoft; OpsVeda; Oversight Systems; Rockshore; SAP; Software AG; Splunk; SQLstream; Tibco Software; VisionWaves; Vitria; West Global; XMPro

Recommended Reading: "Commercial Operational Intelligence Platforms Are Coming to Market"

"Use Intelligent Business Operations to Create Business Advantage"

Managed GRC Services

Analysis By: Jacqueline Heng

Definition: Managed governance, risk and compliance (GRC) services integrate and manage GRC components across an enterprise. This includes gathering information on the buyer's enterprisewide technology and business processes (applications, architecture, assurance and risk controls), via the provider's single group of external systems and processes, and then using business process outsourcing (BPO) to deliver managed GRC services to clients. A differentiator is the consulting component, used to analyze, interpret, prioritize and map risk-related data.

Position and Adoption Speed Justification: This is still an embryonic service. The adoption, which includes analysis and insight, is still low. It was limited to the Sarbanes-Oxley Act, now consultants have onshore service centers providing regulatory compliance services for the financial industry, offshore model validation services, internal audit co-sourcing and outsourcing solutions. The delivery is through a business process services and outsourcing (BPS&O) provider or managed services platform.

Generally, most business process service (BPS) providers give clients elements of GRC services (such as risk assessment at the operations level and managing controls) as part of their overall professional services offering. In addition, most of these providers are already hosting — or providing, through outsourcing — transaction-type services at the operations level in enterprises. These services include a variety of outsourced functions, such as payroll, customer contact centers and the management of compliance controls, whereby isolated GRC services are already provided to clients.

GRC investments that are focused not just on regulatory compliance, but also on efforts at enhancing Enterprise Risk Management (ERM), will be the differentiator for managed GRC services, thus improving the overall business performance. This can be achieved by providers consolidating and integrating disparate GRC services and resources, repositioning the bundled offerings in the

market, and providing strong consulting skills to tap into this potentially lucrative market. However, adoption remains immature in terms of integrating risk data with financial information and other data generated by transactions. Some companies recognize the importance of this integration and are trying to develop a solution with their risk consultants. But doing so means managing various sourcing vendors and the information they generate. Gartner has also been seeing more and more integrated platforms built on predictive risk analytics solutions that are highly likely to evolve into managed GRC services.

User Advice: Companies' adoption and understanding of strategic-level risk management is still being motivated by executives. GRC services are driven at the operations level (see "Introducing the ERM/GRC Blueprint for a Successful Risk Management and Compliance Program") and are still very much focused on compliance and managing or governing controls, sometimes using a holistic GRC platform. These services are driven at the operations, and consultants must understand and be able to provide a strong framework for managed GRC services with strong skills in analyzing risk. However, managed GRC is still not mature enough for multiregulatory integrated GRC and for enterprise risk management.

Consider the following when selecting a consultant:

- Risk consulting — and not just GRC skills — must reside within the service provider itself, or its partner's organization. This consulting will be an integral service for the team that is providing the analysis for the client's project.
- The service provider must understand and be able to provide an appropriate framework for managed GRC services when designing and building solutions to improve operations. The service provider must have strong skills in analyzing risk, and it must understand the client's enterprise environment very well, so it can produce relevant actionable information on an ongoing basis.

Business Impact: Once the relevant data has been integrated and analyzed, managed GRC services will give clients a deeper understanding of their risk environment. Today, risk assessment procedures are still cumbersome and can be found distributed throughout the organization. Both risk consultants and their clients still face the challenge of finding and isolating risk-related issues early. The key to providers' success for managed GRC services is to take one step further: to help clients interpret and even produce a meaningful risk map, rather than simply generating risk-related reports. It is important that BPS&O providers without this skill be able to work closely with a risk strategy consulting firm to produce the best results for clients. Otherwise, the likely failure of the initiative will leave clients disillusioned about what they are buying into and, worse, possibly leave some areas of risks undiscovered. This service is still not yet evolved into an all-encompassing solution offering as relevant data is not always integrated and analyzed, in order for clients to have a deeper understanding of their risk environment.

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Embryonic

Sample Vendors: Capgemini; EY; KPMG; PwC

Recommended Reading: "Emerging Service Analysis: Creating Opportunities With Managed GRC Services"

"MarketScope for Global Enterprise Risk Management Consulting Services"

"Introducing the ERM/GRC Blueprint for a Successful Risk Management and Compliance Program"

File Analysis

Analysis By: Alan Dayley

Definition: File analysis (FA) tools analyze, index, search, track and report on file metadata and, in some cases, file content. This supports taking action on files according to what was collected. FA differs from traditional storage reporting tools not only by reporting on simple file attributes, but also by providing detailed metadata and contextual information to enable better information governance and storage management actions.

Position and Adoption Speed Justification: FA is an emerging technology that assists organizations in understanding the ever-growing repository of unstructured data, including file shares, email databases, SharePoint, etc. Metadata reports include data owner, location, duplicate copies, size, last accessed or modified, file types, and custom metadata. Progressive and cost-conscious organizations are moving past "throw more disk" at their storage problems and realizing they need a better understanding of their data. The desire to optimize storage costs, implement information governance and mitigate business risks (including security and privacy risks) are among the key factors in the adoption of FA. The determination of file ownership and the enablement of more-accurate chargeback are also made available with FA, which can benefit all verticals.

User Advice: Organizations should use FA to gain a true understanding of their unstructured data, where it resides and who has access to it. Data visualization maps created by FA can be presented to other parts of the organization and be used to better identify the value and risk of the data, enabling IT, line of business, compliance, etc., to make more-informed decisions regarding classification, information governance, storage management and content migration. Once known, redundant, outdated and trivial data can be defensibly deleted, and retention policies can be applied to other data.

Business Impact: FA tools reduce risk by identifying which files reside where and who has access to them, allowing remediation in such areas as eliminating personally identifiable information, corralling and controlling intellectual property, and finding and eliminating redundant and outdated data that may lead to business difficulties, such as multiple copies of a contract. FA shrinks costs by reducing the amount of data stored. It also classifies valuable business data so that it can be more easily found and leveraged, and it supports e-discovery efforts for legal and regulatory investigations.

Benefit Rating: High

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Sample Vendors: Acaveo; Active Navigation; Aptare; CommVault Systems; EMC; HP-Autonomy; IBM-StoredIQ; Index Engines; Novell; NTP Software; Nuix; Proofpoint; SGI; STEALTHbits Technologies; Symantec; Varonis; Whitebox Security; ZyLAB

Recommended Reading: "Innovation Insight: File Analysis Delivers an Understanding of Unstructured Dark Data"

"Does File Analysis Have a Role in Your Data Management Strategy?"

"Best Practices for Data Retention and Policy Creation Will Lower Costs and Reduce Risks"

"Best Practices for Storage Administrators: Staying Relevant in an Information-Centric Data Center"

"Use These Unstructured Data Management Best Practices to Manage Based on the Time Value of Data"

Transaction Controls Monitoring

Analysis By: Khushbu Pratap; French Caldwell

Definition: Transaction controls monitoring (TCM) is a governance, risk and compliance (GRC) technology that monitors ERP and financial application transaction controls to improve financial governance and automate audit processes. TCM software helps identify exceptions to policies, business rules and built-in application controls.

Position and Adoption Speed Justification: TCM is a subset of continuous controls monitoring (CCM), which also includes segregation of duties. CCM is a subset of a broader set of technologies called "controls automation and monitoring," which includes infrastructure, systems and other application controls. CCM has also been referenced as "controls-monitoring analytic applications" in the broader packaged financial application market. Note that continuous monitoring has a context in traditional security controls and is not considered in this discussion.

TCM contributes value to risk management and compliance initiatives in three ways:

- Lowering compliance costs — A TCM solution can reduce the cost of audits by eliminating much manual sampling and minimizing the time it takes to gather documentation. When controls are automated, compliance professionals and auditors can test the automated control, which is less labor-intensive.
- Improving financial governance — TCM can increase the reliability of transaction controls, improve auditor trust and increase the effectiveness of anti-fraud controls. When the general computing controls are determined to be effective, auditors will consider automated controls to be of lower risk than manual controls.
- Improving financial organization operational performance — TCM controls, such as those that monitor duplicate payments, incorrect discounts or misapplied warranties, go beyond what

most people consider compliance. By preventing these violations of business rules, TCM can improve key financial processes and increase the availability of working capital.

Examples of the most common business processes that are covered under TCM are procure to pay, order to cash, travel and expense, general ledger, procurement card, and gifts/sponsorships and unusual payments.

Some of the regulations have been a primary driver of implementing CCM solutions — the Foreign Corrupt Practices Act (FCPA), Securities and Exchange Commission (SEC) and Department of Justice (DoJ) guidelines released in November 2012; the Federal Information Security Management Act (FISMA); and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 and SP 800-53. The TCM market is in its adolescence, and many vendors don't offer a complete solution, or they offer solutions that are targeted at specific ERP applications, but don't work as well in heterogeneous financial application environments. The awareness and implementation of TCM software is on a steady rise. Gartner has seen a very slow increase in interest or specific budgets for this initiative. Specifically, purchasing decisions for TCM were seen to rise according to the annual security and risk management survey conducted in 2013 and 2014.

Industry 2014*

- Manufacturing and natural resources: 17%
- Communications: 18%
- Services: 7%
- Government: 14%
- Education: 18%
- Retail/wholesale: 19%
- Banking: 18%
- Insurance: 13%
- Healthcare providers: 20%
- Transportation: 14%
- Utilities: 8%
- Others: 29%

*Percentage of respondents' plans to buy TCM solutions in 2014 (n = 54).

With these considerations, the position of TCM is revised to trigger peak midpoint.

User Advice: Enterprises should consider TCM if they want to lower compliance and audit costs, improve financial governance, or boost financial organization operational performance. In a homogeneous ERP environment, consider the ERP vendor's TCM solution and compare it with other TCM vendors that have solutions for that ERP vendor. In a heterogeneous ERP environment, if

a financial process involves more than one ERP system — for instance, invoices are in one, and payments in another — compare the costs of extending one of the ERP vendors' TCM solutions to the other ERPs with other TCM vendors that have solutions that are not specific to a given ERP vendor.

Business Impact: When financial processes are spread across multiple instances, and especially when there is a mix of ERP financial applications and/or other non-ERP financial applications, customizing controls and application integration add expense. The costs of customization should be balanced against what it would cost to migrate to a common ERP. TCM in combination with other integration technologies, such as business process management systems, which can automate the data collection across multiple platforms and reporting, could mitigate the need to move to a common ERP.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: ACL; BWise; CaseWare; Greenlight Technologies; Infogix; Infor; Oracle; Oversight Systems; Runbook; SAP; Security Weaver; SymSoft

Recommended Reading: "Transaction Controls Monitoring Can Improve Productivity and Financial Governance"

"MarketScope for Segregation of Duty Controls Within ERP and Financial Applications"

"Automate Segregation of Duties in ERP to Reduce Compliance Costs"

At the Peak

Information Stewardship Applications

Analysis By: Andrew White; Debra Logan; Saul Judah

Definition: Information stewardship applications are business solutions used by business users in the role of information steward (those who enforce information governance policies on the information assets for which they are responsible). These developing solutions represent, for the most part, an amalgam of a number of disparate IT-centric tools already on the market, but organized in such a way that business users can use them for the few minutes a week it takes for them to "do" information stewardship.

Position and Adoption Speed Justification: The emergence of consolidated tools (as a full-blown application) for information stewardship will soon challenge established implementation efforts, because the majority of legacy and new information management (IM) programs lack this level of capability. The functionality spans monitoring, enforcement, and root cause analysis related to issues identified in policy violations spanning data quality and consistency, security, privacy,

retention and standards. For example, too many master data management (MDM) programs never address the needs of monitoring the performance of the MDM program, and so the requirements for stewardship go unmet, even if MDM is hailed as a "successful implementation." This puts any information governance program at risk, since the business has no need to drive ongoing improvement and has no solution to support the operational responsibilities of governance and stewardship. In the long term, perhaps five to 10 years, these solutions will accompany many, if not all, information governance programs and efforts that need to steward information, spanning MDM, enterprise content management (ECM), content management, records management, data warehousing, business intelligence, big data, analytics, application integration, cloud and so on.

The work of information governance is very much based on people, not technology. That being said, the output of information governance needs to be operationalized — and enforced day to day — by business people, for business people. That is where information stewardship solutions come in. They emerged a few years ago, mostly oriented toward MDM programs. Today there are a wide range of stewardship dashboard in many areas (records management is one example), but these are really forerunners and earlier versions of the more complete stewardship solutions we refer to here. Almost all solutions covered by this tech profile started out as dashboards, but evolved as business users (i.e., information stewards) needed and demanded more functionality to do their work.

User Advice: Recognize the general lack of maturity (and the wide range of different capabilities) in technology offerings related to governing data across multiple hubs and application data stores. Today, most solutions are best suited for IT-focused users (while they need to be consumable by business users) and for specific scenarios and business applications (for example, data quality projects related to an application migration).

Some applications focus on stewardship of content (such as those offered by RDS) and others on structured data (such as those offered by Collibra). For organizations focused on master data, those MDM solutions offer rudimentary capabilities, but have led to the greatest interest and hype in this new information stewardship technology. For the next two to three years, most information governance implementations will focus on tools to manually define and manage governance with limited help from technology vendors across IM systems or the enterprise as a whole. Work with your technology providers to help them understand what must be made operational in the tools. If you have need to steward other data outside an information governance program, tread more carefully, as the lack of a unifying driver such as MDM or ECM could possibly lead to fewer vendor options.

Business Impact: The governance of information is a core component of any enterprise information management (EIM) discipline. Information governance cannot be sustained and scaled without an operational information stewardship role and function. At worst, the lack of effective governance will lead to the failure of EIM initiatives. At best, it will result in lower-than-desired benefits; the business case for EIM, for example, won't be realized. A successful stewardship routine will lead to sustainable and persistent benefits from programs like EIM, such as increased revenue, lower IT and business costs, reduced cycle times (in new product introductions, for example) and increased business agility.

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: BackOffice Associates; Collibra; IBM; Informatica; RDS; SAP

Recommended Reading: "How Chief Data Officers Can Help Their Information Stewards"

"Governance of Master Data Starts With the Master Data Life Cycle"

IT Financial Management Tools

Analysis By: Robert Naegle; Tapati Bandopadhyay

Definition: IT financial management (ITFM) tools are IT-owned and managed tools that provide IT leaders with a system of record in which to budget, forecast, and capture service definitions and all associated costs. ITFM tools provide the necessary financial transparency around both cost and value to support strategic IT decision making with dynamic reporting for budgeting, robust analytics and financial capabilities like IT budgeting and forecasting, project financial management, chargeback/showback, pricing and cost optimization.

Position and Adoption Speed Justification: ITFM tools (referred to by some vendors as IT business management [ITBM] tools) provide IT leaders with the means to manage the financial aspects of IT, or to "run IT like a business." Gartner has seen an increase in interest and adoption of these to support IT cost optimization, showback, chargeback and effective cost transparency. Interest in ITFM tools continues to grow, at an estimated 15% to 20% over the last 18 months. The interest in these tools has grown due to increased interest in cost optimization and service-based costing, the increasing share of virtualization (shared infrastructure) in the production environment, interest in cloud computing service delivery models and service portfolio management, and the need to provide greater IT cost and value transparency.

ITFM tools will continue to gain modest adoption as the pressure increases on enterprise IT to run IT like a business. Interest in cloud computing and SaaS solution models increases the importance of cost transparency to facilitate build-versus-buy sourcing decisions. It also means that this technology may be bundled by CMP vendors (for example, VMware and HP) as part of their offerings. More organizations are beginning to see the benefits of effective financial transparency and the value of better budgeting, forecasting, cost optimization, performance metrics and benchmarking.

However, adoption of ITFM tools by many IT organizations may be at risk due to the complexity and cost, and the time and resource-intensive nature of ITFM tool implementation coupled with the IT maturity level required to successfully drive an ITFM initiative. These factors have given reason to lengthen our time-to-plateau estimates.

User Advice: Most IT organizations will require significant operational and financial changes to become trusted service providers to the business. Aligning IT operations to define and provide services as opposed to managing technologies, understanding cost drivers in detail, and providing

transparency of IT costs and value delivered, will be key. Most corporate financial systems lack the granularity and flexibility IT operations require, while spreadsheets lack the desired features, reporting and historical context. ITFM tools, when properly implemented and maintained, are positioned to provide the business with improved cost optimization, transparency to external stakeholders, demand management of critical IT resources, and an indication of IT financial compliance to efficiency requirements.

IT leaders should consider ITFM tools to understand IT costs and value at various levels — from tactical activities to business service views. As IT moves toward a shared-service delivery model and external sourcing in an increasingly complex computing environment, these tools will enable more responsible and accurate financial management of IT. However, users must be willing to invest in the processes and resources required, including dedicated IT financial management capabilities, to maximize the successful implementation of these tools.

Business Impact: ITFM tools impact the IT organization's ability to perform accurate cost allocation and the value of the services provided. When IT organizations move from a cost center to adopt a service mode of operations, with a well-defined service catalog and portfolio, it is imperative to associate cost with each service defined in the catalog or at the portfolio level. ITFM tools enable the business and IT to manage and optimize the demand and supply of IT services. This enables enterprises to provide critical insights into IT costs and, as required, to fairly apportion IT services based on business unit service consumption, and to demonstrate how the IT organization contributes to business value.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Apptio; CloudCruiser; ComSci; Nicus; UMT; VMware

Recommended Reading: "IT Financial Management Tools Vendor Landscape"

"Best Practices in Implementing IT Financial Management Tools"

"How to Use IT Financial Management to Validate I&O's Relevance to Business"

"IT Financial Management Implementation Model Defines I&O Core Competencies"

"Using IT Financial Management to Improve Business Outcomes"

"IT Financial Management; CIO Desk Reference Chapter 23, Updated Q2 2012"

Privacy Management Tools

Analysis By: Carsten Casper

Definition: Privacy management tools help organizations conduct privacy impact assessments, check processing activities against requirements of privacy regulations, and track incidents leading

to unauthorized disclosures (investigation, remediation and reporting). They analyze and document data flows of personal information (the nature of the data, purpose of processing and the data controller), support authoring and distribution of privacy policies (for which they provide templates), and track user awareness (users acknowledging having read the policies).

Position and Adoption Speed Justification: Privacy management tools are still in the top three of technology-related privacy priorities (ranking second in Gartner's 2014 privacy survey), although interest has decreased from last year (when it was ranked first). Regulatory pressure and heightened awareness remain strong drivers in many countries, including Europe, Australia and the U.S., and the tools are emerging in Singapore via its latest Personal Data Protection Act.

The resulting complexity of requirements drives privacy officers to automate some of their activities. Governance, risk and compliance (GRC) management tools are an excellent aid for privacy officers, who can use the repository, workflow and control mapping capabilities of GRC management tools for their privacy activities. On the other hand, most GRC tools are priced at a level that is prohibitive for privacy officers, who have only a very limited budget or no budget at all. Since the budget for GRC management tools comes from other departments, the privacy officer has little influence over the choice and configuration of an enterprisewide GRC platform. This hinders the adoption of such tools for privacy management purposes.

Still, the privacy officer has specific requirements that must be met, with or without GRC platforms (such as documenting personal data flows or obtaining granular regulatory content). A few purpose-built privacy management tools have emerged that have a narrow focus on certain industries (healthcare) or jurisdictions (Canada and Germany). Now, these tools are slowly moving out of their respective niches, targeting adjacent markets. Feature sets vary widely, driven by customer requirements in their home markets. Compliance tracking and breach notification are the most relevant use cases, whereas demand for privacy policy management is trailing. Thus, this market is evolving, albeit at a slow pace.

User Advice: Privacy officers should articulate their demand for support of privacy impact assessments, privacy policy management (increasingly for mobile device privacy policies as well), and privacy incident management for organizational roles that are involved in GRC activities (for example, the enterprise risk manager, compliance officer and information security officer). If possible, privacy officers should participate in these GRC initiatives and ensure that GRC tools are sufficient to cover their demands. If this is not possible (for instance, because requirements are too different or license costs are too high), then privacy officers should evaluate dedicated privacy management tools like the ones we discuss below.

Privacy *management* tools should not be confused with privacy *control* tools, which help organizations protect the processing of personal data (for example, data masking tools, content-aware data loss prevention [DLP], encryption, redaction, data wiping and destruction, and website compliance analyzers). However, the use of privacy management tools can support and optimize the use of privacy control tools, because privacy management tools allow privacy officers to capture business and legal requirements about which privacy control tools to implement. Also, privacy management tools facilitate privacy compliance reporting (that is, which privacy control tool fulfills which legal or business requirement). The IT security team's business case for the

deployment of DLP might be strong — it is stronger if the privacy officer can show how DLP reduces privacy risks.

Business Impact: Privacy management tools improve information governance in areas where personal information is processed — for example, in HR management, CRM and marketing. Organizations with operations in multiple jurisdictions benefit from this technology, as well as organizations in healthcare (particularly in the U.S.), in financial services and in Europe (where additional and changing regulatory requirements for privacy must be obeyed). Two particular points of concern are the use of mobile devices — creating the need for mobile device privacy policies — and international transfers of personal data — creating the need to document data flows and manage contractual privacy agreements.

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: 2B Advice; AvePoint; Co3 Systems; FairWarning; iubenda; Jordan Lawrence; Nymity; otris software; TRUSTe

Recommended Reading: "Privacy Audits Make Privacy Investments Visible"

"Magic Quadrant for Enterprise Governance, Risk and Compliance Platforms"

Sliding Into the Trough

Supply Base Management

Analysis By: Magnus Bergfors

Definition: Supply base management (SBM) solutions support supplier information, risk and performance management with survey tools, scorecards, approval workflow, document management and dashboards.

Position and Adoption Speed Justification: The vision of this solution — a single repository of key supplier data and analytics to identify and manage strategic issues such as risk tracking — is not being met by current offerings because of solution immaturity, high data integration costs and evolving requirements. Many organizations are also struggling with aggregating all relevant data that exists within the organization as well as unstructured, public domain data and lack an overarching plan to collect and maintain supplier data. As a result, SBM solutions are continuing their slide toward the Trough of Disillusionment.

There are also concerns that SBM solution costs may not yet be in line with benefits, particularly for smaller programs tracking fewer than 25 suppliers. Movement along the Hype Cycle is, therefore, steady, but slow.

SBM has become one of the foundational pieces of strategic sourcing suites and is included in offerings from almost all strategic sourcing suite vendors. However, the capabilities vary to a great extent from simple supplier information management to more complete modules with advanced risk and supplier management capabilities. This, in combination with the relative solution immaturity and unevenness, manifested in a lower customer satisfaction for SBM modules compared to e-sourcing and spend analytics in a recent Gartner survey. Implementing SBM alongside other modules, such as spend analysis and contract life cycle management (CLM), makes sense, because data can be more readily pulled into SBM dashboards when there is a shared platform. In the long term, we expect general-purpose SBM solutions to be absorbed into broader strategic sourcing suites, while niche vendors with extended services offerings, such as prequalification and vetting of vendors, specializing in specific verticals will remain as stand-alone providers. Independent vendors, in some cases, will partner with suite vendors as an extension when specific capabilities or services are needed.

User Advice: Consider SBM solutions, rather than supplier information management (SIM), supplier performance management (SPM) or supplier relationship management point solutions. These subtypes are rapidly converging in the market. Invest cautiously, however, because requirements are still evolving, many entrants are new and solutions have gaps in functionality.

Consider SBM applications offered as elements of broader procurement suites to make e-sourcing events more efficient by leveraging SIM data in sourcing events and creating cross-functional dashboards and workspaces related to specific vendors.

If investing in a niche SBM vendor, be aware of the risk that the vendor might be acquired by a suite vendor.

Business Impact: Organizations that holistically track their suppliers and leverage internal and external data sources to achieve a best-in-class supply base will significantly outperform organizations that don't. However, as already noted, SBM solution costs may not yet be in line with benefits, particularly for smaller programs tracking fewer than 25 suppliers.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Aravo; BravoSolution; Decideware; Elementum; EMC (RSA); Fullstep; Hiperos; HICX Solutions; IBM (Emptoris); Ivalua; Mediagrif Interactive Technologies; MetricStream; Pool4Tool; riskmethods GmbH; SAP

Recommended Reading: "Best Practices for Sequencing Procurement Solution Investments"

"2014 Strategic Road Map for Supply Risk Solution Deployment"

"Toolkit: How to Scope a Supply Risk Program and Solution"

"Magic Quadrant for Strategic Sourcing Application Suites"

IT Vendor Risk Management

Analysis By: Gayla Sullivan; French Caldwell; Christopher Ambrose

Definition: Vendor risk management (VRM) is the process of ensuring that the use of service providers and IT suppliers does not create an unacceptable potential for business disruption or a negative impact on business performance. VRM technology supports enterprises that must assess, monitor and manage their risk exposure from third-party suppliers that provide IT products and services, or that have access to enterprise information.

Position and Adoption Speed Justification: The growing reliance of enterprises on third-party service providers, the large number of major corporate data breaches and the increasing regulatory activity on privacy policies of those service providers, all provide a steady stream of hype for VRM. Many businesses, as well as government agencies and other organizations, increasingly rely on IT vendors and service providers to support their core business processes and provide the hardware, software and licenses needed for IT operations. This reliance exposes them to greater risk of delivery disruption or failure, damage to their reputation and impacts on business performance. Essentially, it extends the enterprise risk boundaries to include the many business and IT risks facing their IT suppliers, and as enterprise risk management (ERM) adoption grows, so does VRM. Challenging economic conditions compound these risks (see "Vendor Risk Management: Criteria You Can Use to See Whether Your Vendor Is in Trouble").

Furthermore, compliance mandates that require monitoring the risks of third-party suppliers are proliferating, as are third parties. The rapid progress of cloud adoption is increasing the demand for VRM solutions. Standards for VRM — such as the Cloud Security Alliance, SOC 1 and SOC 2 (see "SAS 70 Is Gone, So What Are the Alternatives?") — are beginning to stabilize, which also makes VRM solutions easier to deploy. Two issues that could impede adoption and extend the slide of VRM through the Trough of Disillusionment are: the high level of resources needed to provide ongoing monitoring and tracking of vendors, and the lack of mature vendor management functions in many enterprises.

User Advice: VRM solutions are emerging to enable the assessment and management of risks from third-party service providers and IT suppliers. VRM is an important element of enterprise and IT risk management, and is mandated by many privacy and data breach notification regulations (such as the Gramm-Leach-Bliley Act in the U.S. and the Federal Data Protection Act or Bundesdatenschutzgesetz in Germany).

Business performance can be improved through the VRM process. As part of a vendor management program, VRM can be a catalyst for improved vendor performance by identifying risks early and mitigating them through effective controls and process improvements:

- Utilize VRM technology solutions that can provide a common system of record for all the parties involved in that program.
- Ensure that the processes and methodologies used in the enterprise's approach to VRM are supported by the functionality and services offered by the vendor. One element commonly

ignored is ongoing monitoring of strategic and high-risk vendors, which may require external vendor tracking and alert services that are not inherent in the VRM software.

- Develop a road map for improving the maturity of vendor management and VRM. Without that, a technology solution will not deliver the expected value.
- Ensure that all relevant parties are involved, including strategic vendors, even though the evaluation of a VRM solution may be led by the enterprise risk management, procurement, vendor management or IT organization.

Business Impact: VRM enables a shared understanding of the full risk exposure — both within the enterprise and between the enterprise and its service provider/IT supplier partners. Some industries, including banking, healthcare and telecom, have industry-specific regulations that mandate monitoring third-party supplier risk. Most other enterprises also face compliance pressures to improve VRM, because of Payment Card Industry (PCI) data, state-level and national data breach notification regulations, and other privacy regulations. For enterprise risk management purposes, it is important to have a thorough understanding of the risk to business performance from vendor performance failures and disruptions. Furthermore, business performance can be improved, because VRM can be a catalyst for improved vendor performance by identifying risks early and mitigating them through effective controls and process improvements. At a strategic level, a vendor can facilitate VRM when approached as a business partner.

To get the most value from VRM:

- Treat vendor risks as drivers affecting the quality of service and quality of products defined in vendor engagement contracts.
- View vendor risks in tandem with overall business unit and/or enterprise risk. Do not view individual vendor risks in isolation. For example, integrate results from the VRM solution with the larger set of risk assessment results from enterprisewide risk assessment initiatives.
- Engage in regular communication with vendors. Planned and surprise assessments, and being aware of a vendor's overall performance in the market, are vehicles for identifying vendor risks.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Agiliance; Avior Computing; BWise; EMC; EMC (RSA); Evantix; Fusion Risk Management; Global AlertLink; Hiperos; IBM; LockPath; Markit; MetricStream; Modulo

Recommended Reading: "SAS 70 Is Gone, So What Are the Alternatives?"

"Toolkit: How to Scope a Supply Risk Program and Solution"

"2014 Strategic Road Map for Supply Risk Solution Deployment"

"Magic Quadrant for Enterprise Governance, Risk and Compliance Platforms"

"Gartner's Simple Vendor Risk Management Framework"

"Toolkit: Getting Started at Vendor Risk Management"

Social Media Compliance

Analysis By: Stessa B Cohen

Definition: Social media compliance technology enables banks, credit unions, community banks, building societies, investment services providers, brokerages and wealth managers to enforce their policies and procedures throughout all their social presences, whether on the financial services institution (FSI)-owned site or a third-party social networking or social messaging site.

Position and Adoption Speed Justification: Social media has become a more mainstream communication tool for large numbers of individuals and businesses. As part of this, FSIs have begun using these capabilities to communicate with prospects and clients. Given the highly regulated nature of industry sectors such as banking and brokerage, there is a need to tie social media use by employees who use it on behalf of the organization back to regulatory and compliance policies from enterprises and regulators. Social media compliance tools are gaining acceptance as a means to leverage technology to manage these processes, and this is partly why this technology continues to advance on the Hype Cycle.

While most media attention focuses on three dominant social networks — Facebook, Twitter and LinkedIn — financial services presence is not limited to these worldwide social sites. FSIs have established presence on social sites that may be more local (such as Weibo or Qzone in China) or location-based (such as Foursquare and Gowalla). FSI staffs may join FSI-oriented networks, such as linkedFA (a financial advisor peer forum), or cbanc. FSI staffs also may use private social networks to communicate with prospects and customers.

Elements of social media compliance include:

- The identification, registration and monitoring of FSI staffs using social media to communicate with clients or prospects.
- Processes for identifying content that is permitted or prohibited based on use case and situation, and the implementation of automated monitoring rules and permission levels.
- Workflow tools for handling policy exceptions or violations.
- Archiving for all communications, within the tool itself or through integration with existing enterprise information archive (EIA) solutions.

While the hype around social media is extensive, its use by consumers and businesses is very fluid, and its use in a commercial context — while growing — is less defined. Although many FSIs have established one or more presences on some social networks, most are still cautious about their use of those presences. This caution is the result of their fears about security and regulatory risks. However, although the level of consumer use of social media for commercial interactions or

financial services is uncertain, it is clear that the proliferation of social media will continue and expand, and FSIs that participate in social networks will have to find tools to manage that participation (see "Report Highlight for User Survey Analysis: Trends in Consumers' Use of Social Media"). Further, various government agencies in a variety of countries have been developing compliance guidelines and regulation for social media use, including the U.K. Financial Services Authority (FSA), the U.S. Securities and Exchange Commission (SEC) and the U.S. Federal Financial Institutions Examination Council (FFIEC; see "The Regulated Social Media Risk Management Survival Guide").

Further, recent events show the immediate financial effects that social media can have. The "#hashcrash" of 23 April 2013 — where a hacking of the Associated Press (AP) wire service's Twitter feed resulted in a short-term market drop of more than 100 points on the Dow Jones Industrial Average within minutes — illustrates the potential for social media to affect stock prices. Although not related to FSI employee use, this incident is a clear example of why effective compliance tools are necessary to preclude the fraudulent use of social media.

User Advice: Avoiding the use and management of social media is no longer an option. The goal must be compliance and management, not prohibition.

- Before identifying and implementing social media compliance policies or technologies, determine your social media strategies — reactive and proactive:
- Reactive strategies revolve around monitoring and understanding what is being communicated by social media participants about your firm and having an organized, thoughtful process for managing any response processes. It also includes surveillance activities by automated systems and human staff to prevent or react to unauthorized use by other staff members.
- Proactive strategies include identifying how the FSP's social presences fit into the organization's overall business processes, market and customer service processes, and prospecting efforts; how social media will be used by the staff; and what policies, procedures and technologies will be used to monitor and manage this use.
- Once these initial strategy decisions are made, determine which social media compliance technology solutions will best fit those needs, and which will integrate most efficiently with existing compliance or archiving processes and tools. FSPs that use field agents should select tools that have good content management, distribution and compliance for product-related information that the agents will share with their prospects and clients outside the FSP's network or control.
- Create a plan and process for archiving social media posts, messages and content. Banks can expect local governmental agencies to extend regulations to include social media content. The bank will need to determine whether the existing archiving systems have capabilities to archive social media content; otherwise, the bank must seek out another provider. In either case, the bank must be able to search and extract archived social media content as required for review, compliance and legal processes.

Business Impact: As part of the continuing shift of power and control of the terms of trade from the enterprise to the consumer, social media introduces new means for customer communications and

service. It may also forge new opportunities for delivering financial services. However, the way many social sites work enables FSI employees to easily post content or opinions that may violate regulatory customer communication protocols. In many countries, regulations regarding FSI use of social sites are still unclear. Consequently, for FSIs, social media compliance is a necessary part of participating on social sites, remaining compliant with regulations, and maintaining the balance between risk and transparency. Additionally, social media compliance technology enables FSIs with field agents to enforce the agreement between agent and FSI with regard to brand, messaging, advice and so on.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Actiance; Arkovi; brandprotect; Compliance11; Erado; Hearsay Social; Netbox Blue; salesforce.com (Radian6); Smarsh; SocialComply.com; Socialware; SunGard

Recommended Reading: "The Regulated Social Media Risk Management Survival Guide"

"Making Sense of Changing Regulatory Guidelines for Social Media in Banking"

"Social Media Changes Advisor Communication for Wealth Management"

"Banks Should Pass on Pinterest for Now, but Watch for Opportunities"

"Report Highlight for User Survey Analysis: Trends in Consumers' Use of Social Media"

"Use of Social Media in Wealth Management Requires Compliance, Not Prohibition"

"The Antisocial FSI Will Miss the Last Dance"

"Operational Failures Should Not Tempt Banks to Retreat From Social Media"

Cross-Agency Case Management

Analysis By: Rick Howard

Definition: Cross-agency case management applications incorporate service-oriented architecture (SOA) principles, open standards and a modular design approach to enable business process flexibility and service interoperability across multiple government agencies.

Position and Adoption Speed Justification: In 2013, the increased pace of cross-agency case management procurements has pushed penetration past the middle of the 5% to 20% range among local and regional governments. This reflects more mature applications and industry adoption of open standards (such as Content Management Interoperability Services and Web services), EA frameworks, SOA and application adapters that support integration within the government and partner IT ecosystem.

However, the value of commercial off-the-shelf (COTS) software and configurable workflow templates depends on the client's willingness to accept significant change to legacy processes and service models. Enterprise-class case management frameworks often test the maturity of shared service governance mechanisms and competencies for business process management or organizational change.

Unmanaged expectations or constraints that force overcustomization to "out-of-the box" capabilities create huge implementation risks. For this reason, cross-agency case management is firmly positioned in the Trough of Disillusionment. Subject to a growing base of client referrals and the demonstrated benefits from cloud-based solutions, the rate of case management modernization is expected to increase through 2018.

User Advice:

- Inventory your case management application portfolio. "Case management" is a broadly defined term that applies to capabilities found in enterprise content management (ECM), client relationship management (CRM), and business process management (BPM) applications, as well as specialized case management applications for social services, tax and revenue, investigation, or healthcare.
- Establish a business process competency center (BPCC). Identify and categorize case management functions and workflows that are common among programs and can be configured to accommodate differentiated business needs.
- Develop a comprehensive library of case management use cases. No single COTS framework or vendor can fulfill all the end-to-end services needed to manage multiple types of cases and workflows. Well-constructed use cases will reveal gaps and identify which solutions and technical architectures will yield the greatest business value.
- Use Gartner's Pace-Layered Application Strategy to rationalize your case management portfolio. Manage risk and deliver value sooner by avoiding "rip and replace" projects in favor of an overall case management modernization program. Take an incremental approach to large-scale application migration and consolidation.

Business Impact: Most governments maintain a bewildering array of stand-alone, custom-made case management applications that are designed under brittle, tightly-coupled architectures and built with nonscalable or unsupported technologies. Because legacy case applications are reaching the end of their life cycles, government CIOs and agency administrators are turning to modular, configurable COTS solutions that are capable of supporting a variety of simple and complex use cases spanning multiple programs, agencies and tiers of government.

Agency leaders and CIOs should anticipate that the primary impediment will be necessary organizational and cultural change. The greater value a case management solution brings, either to individual program areas or entire lines of service, the more critical it will be to invest in effective governance, EA and BPM capabilities. These competencies will encourage stakeholder participation and help garner sustained support for transformational change.

Government policy analysts and program managers should also consider how to enhance case management with other tools and social networks. By making context-driven business intelligence and case analytics available at the user interface, such solutions can enable government agencies to improve worker productivity and outcomes.

Software as a service (SaaS) or cloud-based case management offer small or midsize governments a number of viable, cost-effective alternatives with higher levels of security than they might otherwise obtain in-house. Agency governance, risk management and compliance (GRC) programs must verify that any case management solution — whether on-premises or cloud-based — is capable of securely processing sensitive data such as legally protected personally identifiable information (PII) or personal health information (PHI).

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Sample Vendors: Accela; Athena Software; BizFlow; Capgemini; ClientTrack; Column Technologies; EMC; IBM (Curam); Infor (Hansen); Iron Data; K2; Kana (Lagan); Kofax (Singularity); MicroPact; Microsoft; Oracle; Pegasystems; SAP; Social Solutions; Therap Services; Tyler Technologies

Recommended Reading: "Critical Capabilities for Case Management Frameworks"

"How to Develop a Pace-Layered Application Strategy"

"The Case for Case Management Solutions"

Externalized Authorization Management

Analysis By: Gregg Kreizman

Definition: Externalized authorization management (EAM) is an authorization decision and enforcement technology used to grant, resolve, enforce and revoke fine-grained access to applications, systems and data.

Position and Adoption Speed Justification: EAM provides the ability to enforce technical policies for access at a fine-grained level — that is, it evaluates the appropriateness of an access action of a user or service, and allows or denies the action. EAM can base these decisions on a variety of inputs, using a combination of attributes and rules, and can protect a variety of objects, such as Web pages, files and database objects. EAM has administration and logging capabilities, but is primarily focused on the resolution and enforcement of entitlements. Identity governance and administration (IGA) technology helps provision entitlements and informs people of the access that users have been assigned. EAM enforces those assignments and reports according to the results of that enforcement.

One historical inhibitor to EAM adoption has been that authorization is an embedded function for most applications. This remains the most common way of providing authorization functions — including SaaS applications. EAM solutions offer a framework that is external to applications and systems, and provide a common and consistent way of defining, deciding and enforcing entitlements. Conceptually, abstracting authorization decision and enforcement functions from applications, and having a consistent framework for centralizing policy management, have been appealing to some chief information security officers (CISOs), compliance managers and enterprise security architects.

However, EAM implementations are rare compared with authentication and coarse-grained authorization systems, such as Web access management (WAM), because relatively few organizations have IGA and access management disciplines that are mature enough to justify the effort and cost of EAM implementation. Enforcing fine-grained access policies successfully requires that organizations also successfully manage the administrative aspects of entitlements.

Another inhibitor involves the proprietary nature of vendors' policy enforcement point (PEP) APIs. These PEP APIs are used by developers to invoke the EAM capabilities from applications. This means that customers who develop custom applications and invest in EAM would be inhibited from moving to another vendor's EAM. The OpenAz standard is being worked on by core EAM vendors, and if this standard API becomes the PEP API for most or all vendors, then enterprises will have one less inhibitor for adoption.

Gartner clients have reported that maintaining a fine-grained access policy across a large number of custom or complex applications can be a daunting and expensive proposition. Clients report better experiences working with EAM PEPs for commercial off-the-shelf (COTS) applications, and having PEPs that can be configured to support access policies, rather than requiring application development.

Vendors have begun to include or bundle EAM with other entitlement administration and access solutions. This will reduce friction to adopt EAM — it will reside "under the hood" and be available to administer traditional coarse-grained access and fine-grained access policies.

User Advice:

- To be successful with EAM, enterprises should establish an architectural position for future application development that addresses the externalized authorization issue. This position can be used as a certification method for future development or application purchase in the enterprise, and can enable the realization of a long-term answer to EAM.
- Enterprises should align their strategies for WAM and IGA with their EAM strategies to ensure there is minimal duplication and good integration to enable easier or more consistent gathering of data to be used for identity and access intelligence (IAI).

Business Impact: EAM is a long-term investment in an architecture for granular control of application and data access. Its use in business applications and data systems can significantly change the level and consistency of reporting detail about access, resulting in better audit and compliance results over a broader set of applications and data.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Axiomatics; Dell (Quest Software); IBM; NextLabs; ObjectSecurity; Oracle

Recommended Reading: "Technology Overview for Externalized Authorization Management"

"MarketScope for Web Access Management"

Identity Analytics and Intelligence

Analysis By: Felix Gaehtgens; Brian Iverson

Definition: Identity analytics and intelligence (IAI) encompasses a variety of technologies used for collecting, correlating, analyzing and reporting from identity, entitlement, activity and event data. The output of most analytics is referred to as intelligence. IAI tools provide intelligent processing of big data from IAM and related systems, such as data loss prevention (DLP) and security information and event management (SIEM), into customizable, easy-to-interpret, on-demand business-relevant information. IAI is a subset of security intelligence.

Position and Adoption Speed Justification: IAI is a stand-alone product category of its own; however, some existing identity and access management (IAM) products can also have some IAI functional capability that is used within the scope of that product. Specifically, IAI product features can be found in identity governance and administration (IGA), and some basic IAI capabilities can also be found in SIEM, DLP and generic log management products.

IAI is noted separately for two reasons: (1) IGA is using IAI heavily to deliver access certification and remediation reporting; and (2) recent focus on security big data issues has highlighted the need for a more structured approach to correlating output from IAM, SIEM, DLP and related products. IAI is a subset of security intelligence and many products associated with data and application protection.

While most IAI is used by IT to improve the access experience and provide better governance, IAI can also be combined with business intelligence (BI) and business analytics to provide an identity node for BI and give identity context to business decision data. Early examples of business use of IAI include HR context placement and skills assignment, sales and marketing context for verification of training, and healthcare use to verify payment metrics for patients. Additional examples include the extensive work done by consumer-facing vendors such as Google and Amazon with tools such as Splunk and Hadoop. However, access accountability and transparency pressures remain the primary reasons that IAI is used in the enterprise, and IGA is the primary beneficiary.

IAI is maturing as more varied use cases are verified; expanded use in security forensics, access modeling, simulation and analytics occurs; and better integration with other security products is initiated. The convergence of user administration and provisioning (UAP) and identity and access

governance (IAG) into IGA, but also several stand-alone IAI products, are resulting in a small, specialized product area for advanced identity engineering such as:

- Risk scoring
- Classification of enterprise applications based on risk scores
- Risk assessment of users
- Deriving meaningful inferences out of usage patterns and activity logging
- Role engineering and discovery
- Entitlement discovery and cataloging
- Forensic analysis

In addition, consumer-facing vendors are deriving real business value by connecting the dots between people, and what they do, like and want — all of this is IAI.

Gartner believes IAI growth will be modest due to the predominantly low to medium maturity of existing IAM programs — many enterprises remain focused on the complex issues of deployment and simple operations around access and administration. Analytics, while important, is considered secondary until the basic structures of IAM are in place. Innovative companies are currently pursuing IAI more aggressively and account for most of IAI growth. Efforts in big data in the general IT community may accelerate this forecast.

User Advice:

- Understand that IAI is a functional capability with features present in all IAM products. Derive IAI value by developing organizational and process flows to use intelligence from these products as a value-added service to IT and the business.
- Look to leveraging IAI capabilities built into and shipped with IGA and other governance, risk and compliance (GRC) tools to transform technical information into business-relevant actionable advice, derive key compliance controls and discover policy violations.
- Leverage existing IGA solutions as an ideal starting point for leveraging IAI, since governance will require log collection, correlation, analysis and reporting on identity and access events and activities for compliance purposes as a starter.
- Choose specific IAM products (such as IGA) that have rich and flexible logging functions, as well as good integration capability with non-IAM products, because this information can be leveraged for IAI.

Business Impact: Chief information security officers, security and risk management leaders, compliance officers, IT risk management officers, application developers, IT infrastructure managers, and identity management project managers should consider implementing a repeatable process to deliver IAI. Competitive advantage or eventual cost savings can be significant if IAI is leveraged effectively.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Bay31; Beta Systems; Brainwave; CA Technologies; Courion; CrossIdeas; Deep Identity; Dell Software; e-trust; Evidian; GuruCul; Hitachi ID Systems; iSM Secu-Sys; IBM; Omada; Oracle; RSA (EMC); SailPoint; SAP; Securonix; Symantec; Tuebora; UpperVision; Veriphyr; Whitebox Security

Recommended Reading: "Magic Quadrant for Identity Governance and Administration"

"Realize That Big Data Security Is Not Big Security Nor Big Intelligence"

"Use Big Data Analytics to Solve Fraud and Security Problems"

"Cool Vendors in Security Intelligence, 2014"

Configuration Auditing

Analysis By: Ronni J. Colville

Definition: Configuration auditing tools provide change detection and configuration assessment. Some can also provide reconciliation against approved change requests or remediate to a desired state. Company-specific policies or industry-recognized security configuration assessment templates maintain the fidelity of the system for auditing, hardening or improved availability. These tools mainly focus on requirements specific to servers or PCs, but some also address networking, applications, databases, and virtual and cloud infrastructures.

Position and Adoption Speed Justification: Configuration auditing continues to be a top driver for adopting server automation in physical and virtual data center infrastructures. There is still a heightened awareness of security vulnerabilities and missing patches, as well as the requirement to provide documented change control for internal and external auditors. IT organizations establish policies that are translated to templates with specific configuration settings. Systems are then assessed against these company-specific policies or industry-recognized security configuration assessment templates. Some tools provide change detection in the form of file integrity monitoring (FIM), which can be used for PCI compliance, and to support other policy templates (such as the USGCB). Exception reports can be generated; some tools automatically return the settings to their desired values or block changes. Reports are generated that are leveraged by change managers, system administrators, internal auditors, external auditors and security staff. IT organizations can use configuration auditing tools as a mechanism to track and validate changes across data centers and extending to public cloud resources, and enforce corporate standards.

Configuration auditing has two major drivers: external (regulatory compliance) and internal (improved availability). Technology implementation is gated by the organization's process maturity. Prerequisites include the ability to define and implement configuration standards. Although a robust, formalized and broadly adopted change management process is desirable, configuration auditing

tools offer significant benefits for tracking configuration change activity without automating change reconciliation. Although these tools focus on requirements specific to servers or PCs, some address network components, applications, databases, virtual and cloud infrastructures. As cloud projects continue to expand, compliance will be a "day two" requirement, especially for hybrid clouds. IT organizations must understand how that access and visibility is enabled by CSPs. CSPs will drive placement of VMs and applications based on capacity, which may fly in the face of the overall compliance requirements of the business. This will fall back to the IT organization; adoption of configuration auditing (functionality and specific tooling) will help.

A new use case is beginning to emerge for configuration auditing, taking its functionality beyond infrastructure to applications. With the uptick of DevOps projects focused on improving release velocity, new Web-based applications are being updated weekly, daily, hourly and in some instances, continuously. This frequency of change is introducing a heightened risk for disruption and for compliance. New tools, including open source offerings, are emerging to address this requirement; Gartner expects existing tools to expand.

User Advice: Develop sound configuration and change management practices before introducing configuration auditing technology in the organization. Greater benefits can be achieved if robust, proactive change management processes are also implemented. Process and technology deployment should focus on systems that are material to the compliance issue being resolved; however, broader functional requirements should also be evaluated, because many organizations can benefit from more than one area of focus, and often need to expand support within 12 months.

Define the specific audit controls required before selecting configuration auditing technology, because each configuration auditing tool has a different focus and breadth. IT system administrators, network administrators and system engineers should evaluate configuration auditing tools to maintain operational configuration standards and to provide a reporting mechanism for change activity. Security officers should evaluate the security configuration assessment capabilities of incumbent security technologies to conduct a broad assessment of system hardening and security configuration compliance independent of operational configuration auditing tools. Enterprise and cloud architects must insist on specific compliance policies and governance capabilities that meet company regulatory and availability requirements. DevOps project leaders focused on increasing release cycles should evaluate configuration auditing tools that support the ability to track application environment changes.

Business Impact: Businesses must select reasonable and appropriate controls based on reasonably anticipated risks, and should build a case that their controls are appropriate for the situation. This is not a "one and done" exercise. Continually review and revise policies to ensure that regulatory standards are kept up-to-date and that new technologies introduced into the computing infrastructure have the appropriate level of compliance governance applied. Although configuration auditing has been tasked individually in each IT domain, as enterprises begin to develop an IT service view, configuration reporting and remediation (as well as broader configuration management capabilities) will ensure reliable and predictable configuration changes, and will offer policy-based compliance with audit reporting.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Sample Vendors: BMC Software; CFEngine; Chef; Evolven; IBM; NetIQ; Puppet Labs; Qualys; ScriptRock; Tripwire; VMware

Recommended Reading: "Server Configuration Baselining and Auditing: Vendor Landscape"

"Market Trends and Dynamics for Server Provisioning and Configuration Management Tools"

"Security Configuration Management Capabilities in Security and Operations Tools"

IT Risk Management Automation

Analysis By: Paul E. Proctor

Definition: IT risk management automation supports IT risk management (ITRM) functions and workflows that IT risk and security teams use to support better risk-based decision making. Primary functionality of the key ITRM critical capabilities and supporting workflows includes:

- Policy management
- Compliance mapping/reporting
- Security technology data analysis
- IT risk assessment
- Incident management

Position and Adoption Speed Justification: Adoption is driven by a need to automate good IT risk management processes, unify and add business context to IT-related activities, operationalize compliance activities, and support the implementation of mature, risk-oriented security programs.

Until 2014, Gartner used the term "IT GRC" to describe these functions, but the term GRC is too flexible in the marketplace to help connect our clients to appropriate technologies that support their requirements. We further separate IT risk management functions from IT security functions (see "Technology Overview for IT GRC: Clarifying IT GRC to Match Technology to Need").

In 2014, there is little evidence that security technology data is being used in any material or comprehensive manner to directly support senior IT and business-related decision making. However, there is an important evolution in the prioritization and remediation of vulnerability and security configuration management data using business context that is changing vulnerability management and other security operations use cases. This evolution will be covered separately from ITRM automation. For example, vulnerability management tools are evolving to include business context to support the patching priority of IT operations.

User Advice: There is no single best product for all organizations, but there is typically one (or more) best product for a specific set of requirements. Organizations should identify IT risk

management processes that are mature enough for automation, and use these processes to define requirements for product selection. Use our definition of ITRM automation to develop appropriate requirements and select vendors based on their support of your highest value requirements.

Organizations that want to deploy ITRM automation must understand that the labor associated with policy development is significant. There are wide variations in the scope and functional capabilities in the current set of solutions.

The biggest factor affecting success with ITRM automation tools is an organization's readiness to use these tools. An organization should have sufficient process maturity and a need to automate those processes before looking at vendor offerings.

ITRM automation products are usually packaged as a suite with purchase options for different modules. The No. 1 advantage, however, is the integration of the modules, particularly in correlated roll-ups of associated risk measurements. If an organization does not need correlated information from technical controls, control self-assessment and policy compliance, then a best-of-breed vendor in one of these areas may be a better choice.

Business Impact: ITRM automation can improve an organization's ability to analyze IT risk, add business context to security assessments, support internal and external audits, and reduce compliance-reporting costs. Organizations can reduce compliance-reporting costs by applying ITRM automation to the management of written policy content, the assessment of process-oriented controls and the audit of technical configuration settings. The technology can make it easier for an auditor to evaluate IT controls, which should reduce the number of unnecessary audit findings.

Organizations also may take advantage of the benefits of control transparency to move toward the ideal of using better risk management to affect corporate performance. For example, a documented control infrastructure with a known state of accepted risk may help ease the integration of an acquired company. Being able to integrate the two networks faster, with greater confidence, will have a direct impact on the bottom line.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Agiliance; Allgress; ControlCase; LockPath; MetricStream; Modulo; Rsam; RSA The Security Division of EMC

Recommended Reading: "Technology Overview for IT GRC: Clarifying IT GRC to Match Technology to Need"

"MarketScope for IT Governance, Risk and Compliance Management"

"Toolkit: IT Governance, Risk and Compliance Management RFP"

"A Comparison Model for the GRC Marketplace, 2011 to 2013"

"Magic Quadrant for Enterprise Governance, Risk and Compliance Platforms"

E-Discovery Software

Analysis By: Jie Zhang

Definition: Electronic discovery (e-discovery) software facilitates the identification, collection, preservation, processing, review, analysis and production of electronically stored information (ESI) to meet the mandates imposed by common-law requirements for discovery. These demands may be due to civil or criminal litigation, regulatory oversight, or administrative proceedings. The Electronic Discovery Reference Model (EDRM) maps traditional common-law discovery into a six-step, nine-process framework for technology.

Position and Adoption Speed Justification: The position of e-discovery software remains the same as in 2013 and has not reached the Trough of Disillusionment, as vendors continue to make improvements to their offerings and new buyers come into the market. Adoption remains between 20% to 50% of enterprises. Users have now begun to ask for more-comprehensive products that cover either the entire left-hand side of the EDRM or the entire EDRM. The e-discovery software market is going through a major transition, with the buying center shifting from legal solution providers to corporate buyers.

A majority of companies use multiple products to cover the whole process but are looking to consolidate handling more e-discovery steps in-house. The most common steps of e-discovery performed in-house are information governance, identification, preservation, collection and processing and early case assessment. Interest is also growing in using information governance techniques and tools to control the amount of data that is kept by enterprises.

Best practices are forming, especially around the identification and preservation of ESI in enterprises, an area of substantial risk for legal counsel, as well as companies in general. Gartner sees more vendors focused on the right-hand side of the EDRM wanting to move to the left-hand side by extending their offering's functionality in order to own the relationship with the ultimate end user or corporate buyer**.**

User Advice: The move to acquire e-discovery software is driven by efforts to gain more control over costs, data and process, while also reducing risk. The savings result from paying less to outside e-discovery service providers and ultimately outside counsel. Information management software, such as file analysis and enterprise content archiving, can improve a company's litigation readiness and save money in storage and labor costs for IT.

Legal and IT services should always work together to specify a best-practice-based process to use when discovery becomes necessary. Legal and IT should work together before e-discovery ever becomes an issue and also assume joint responsibility for information governance, information privacy and security issues. Suspending the routine deletion of data and managing legal holds in a coordinated manner (rather than treating each legal hold in isolation and seeking tools to make the process defensible and auditable) are the main points that need to be specified in the working process between legal and IT. E-discovery software is also proving useful in other areas of

enterprise data management, such as separating redundant, outdated and trivial data from data that is business-critical or current or that has a status as a business record.

End users should evaluate products that can aid in the identification, preservation and collection of potential evidence, especially those that can collect from a variety of data sources and devices, including mobile devices and off-premises sources. Another important area of functionality is the ability of these tools to create, communicate, enforce and document compliance with legal hold orders. Other areas of increasing interest are early case assessment and early stage processing — to avoid sending large amounts of redundant data to either outside processing providers or, worse (in terms of expense), to outside legal counsel. Enterprise legal management platforms are another emerging area of interest for corporate IT departments.

The enterprise market continues to consolidate a set of tools to handle information management or information governance functions, identification, collection, preservation, and processing. Aspects of the problem remain difficult, particularly those relating to information access and finding relevant data fast (deadlines are often imposed by courts) in the mass of content owned by many enterprises.

Using predictive coding can cut down on the amount of human reviewing necessary in any given case, which in turn reduces costs because attorney review is the most expensive part of the legal process. More automation is being applied to all aspects of the litigation process, which most believe to be necessary — given the volume of information generated by modern businesses.

Business Impact: Major enterprises undergo dozens, perhaps even hundreds, of investigations each year, which can result in high costs to specialized legal solution providers and outside law firms. Software that supports the ability to conduct and manage discovery activities in-house not only saves money, but also enables enterprises to have higher levels of control over investigations. This is not to say that some matters should not be handled by outside providers. In fact, many highly litigious businesses employ a hybrid strategy, managing some matters internally with tools they own, as well as using outside firms in some cases.

As awareness and knowledge of the issues spread in the legal community, corporate lawyers are in need of advice from IT specialists. The most important considerations are specifying a defensible and repeatable best-practice business process (like any other business process), making sure that the parties involved are well-trained in what they must do, understanding the legal ramifications of the task, and being equipped with the right tools to carry it out.

The market is maturing, with point products that handle part of the process being the norm. Market consolidation has slowed, with best-of-class offerings dominating either the EDRM's left-hand-side or right-hand-side functionality, accompanied by point-product vendors specializing in legal hold or information governance.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: AccessData Group; Catalyst Repository Systems; CommVault Systems; Daegis; EMC; Epiq Systems; Exterro; FTI Technology; Guidance Software; HP Autonomy; iCONECT; IBM; Integreon; Ipro; kCura; KPMG; Kroll Ontrack; LexisNexis; Nuix; Orange Legal Technologies; Recommind; Symantec; Ubic; Xerox Litigation Services; ZL Technologies; ZyLAB

Recommended Reading: "Magic Quadrant for E-Discovery Software"

"Magic Quadrant for Enterprise Legal Management"

Financial Governance Applications

Analysis By: John E. Van Decker

Definition: Financial governance applications are suites of applications that include disclosure management, close/reconciliation management and financial consolidation. These suites automate and manage the financial close processes that happen outside the general ledger (GL). Financial consolidation applications are the links between financial governance and corporate performance management (CPM).

Position and Adoption Speed Justification: Financial governance solutions combine elements of ERP; financial governance, risk and compliance (GRC) management; and CPM suites (particularly in office of finance CPM) to build additional process controls around financial consolidation in order to support financial close processes and the production of periodic financial statements for regulators.

Since 2007, a distinct market segment for financial governance has emerged that is focused on financial consolidation, financial close management and disclosure management. Many business applications can be used in the finance organization to address GRC requirements. Many CFOs wrestle with the issue of improving the governance of financial processes. To improve governance, they have to deploy and integrate disparate applications, usually from different vendors, and this is still the appropriate approach for most firms. These applications typically address specific tactical needs, but do not provide an overall solution. Consequently, we anticipate that, through 2015, new components will merge that are workflow-focused (for example, interentity billing and corporate tax planning) and that extend financial governance suites. These offerings will be targeted directly at the needs of the CFO and finance function. In 2013, we saw further consolidation of this functionality with the CPM suite as CPM vendors extended their products in office of finance CPM.

Financial governance suites are maturing into end-to-end solutions for close/reconciliation management functionality and financial statement production/disclosure management. For example, in November 2012, Trintech launched its Cadency offering. While much purchasing is still characterized by point buying of close/reconciliation management and disclosure management solutions, many finance teams are approaching financial governance more holistically.

User Advice: Although users may have to wait for vendors to bring integrated financial governance functionality to market, they can start their initiatives by finding opportunities for specific solutions in financial governance areas where they do not have a technology solution or where they are overwhelmed with manual processes. Many of the cloud solutions today promise the ability for end users to bring in these solutions with minimal support from IT; however, IT still must be in the loop

to ensure consistency for interfaces and standards. Over time, we believe that this functionality will be built into the general ledgers of in-memory computing ERP systems; however, it will be five to seven years before this is commonplace.

If there is a tactical need for a point solution from a specialty vendor, do not defer evaluations; instead, evaluate the appropriate point solutions. However, view such evaluations in two ways:

- First, consider the investment on a five-year basis — the time frame in which more-comprehensive financial governance solutions will become available.
- Second, give preference to point solutions from CPM, ERP, or finance and audit GRC management vendors with whom you have a strategic relationship, because these vendors are the most likely sources of more comprehensive offerings.

IT professionals must help balance these short-term needs with longer-term strategic investments, and should understand the plans of their ERP, business intelligence and CPM vendors.

Business Impact: Financial governance applications build additional process controls around financial consolidation to support financial close processes and the production of periodic financial statements for regulators. The emphasis on financial governance applications centers around two components: close management (including reconciliations management) and disclosure management. Financial governance applications augment the compliance controls in finance GRC management solutions with broader controls that monitor capabilities, and, when delivered as a comprehensive solution, they will enable CFOs to better manage financial risk. While financial governance solutions mature, CFOs will be faced with the challenge of addressing their most pressing governance issues with a variety of point solutions.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: BlackLine Systems; Oracle; SAP; Tagetik; Trintech

Recommended Reading: "Magic Quadrant for Corporate Performance Management Suites"

"IT Market Clock for Financial Management Applications, 2013"

SaaS Archiving of Messaging Data

Analysis By: Alan Dayley

Definition: SaaS archiving of messaging data includes email, instant messaging and social media. Compliance and regulatory requirements drive retention of messaging data, with hosted archiving increasingly becoming the repository of choice. Capture of messaging content occurs at either the time of creation or as it enters the organization's communications systems, where it can be stored on immutable write once, read many (WORM) storage.

Position and Adoption Speed Justification: SaaS archiving solutions are mature. Many users find administration tools for SaaS archiving solutions to be more user-friendly than those available from on-premises solutions. As the journaling feature is turned on in the email administration console, capture is as simple as pointing the journaled email to the hosted provider's site. Instant message archiving is as mature as email and is usually stored in an email format in the archive repository. Social media archiving is newer, and capture is usually through APIs provided by the social media applications. Though social media data can be stored in an email format in the archive, the industry trend is to store it in native format.

Unlike backup or disaster recovery as a service, archive users are less concerned about latency and more about accurate capture of metadata and chain-of-custody of data; therefore, the speed of Internet connections is not a major concern. This, coupled with easy-to-use administrative and supervision tools, has led many organizations to choose a hosted solution, enabling archive expenditures to shift to an operating expenditure (opex) model and away from a capital expenditure (capex) model. As government and industry regulations proliferate, hosted archiving vendors have been nimble in quickly updating the compliance requirements of offered solutions. Most SaaS archiving vendors offer end users access to messaging data through either a search interface or, in some cases, a native application folder view. Basic e-discovery capabilities of hosted solutions receive high marks from customers and are noted as another reason for adoption.

User Advice: Organizations in highly regulated industries will find hosted message archiving solutions to be mature, secure and reliable enough to meet the most stringent requirements. Any organization with message archiving needs will find the hosted option easy to administer, price-attractive and an opportunity to optimize internal IT resources. Most organizations do not face internal or external requirements or regulations that require that data reside on-premises, so the willingness to consider cloud revolves primarily around company culture regarding risk, security, data sovereignty and costs. When considering a solution, focus on indexing, search and discovery capabilities to ensure needs are met either within the offering or through integration with a third-party e-discovery vendor. The migration of legacy email archives, including into and out of a hosted solution, can be expensive and should be scoped during the selection phase. When determining the costs versus the benefits of SaaS archiving, include soft expenses associated with an on-premises solution for personnel and IT-involved discovery requests.

Business Impact: Organizations switch capex for opex costs when selecting a hosted archive solution. Pricing is typically based on a per-mailbox or per-user basis paid as a monthly subscription. IT departments are relieved of updating legacy on-premises archive systems when hardware and software need to be refreshed. Compliance and legal personnel within organizations directly access the hosted solution without IT involvement and more easily provide access to the hosted archive message data to outside parties as required.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Sample Vendors: ArcMail; Bloomberg; Global Relay; Google; HP (Autonomy); Microsoft; Mimecast; Proofpoint; SilverSky; Smarsh; Sonian; Symantec

Recommended Reading: "Magic Quadrant for Enterprise Information Archiving"

"Best Practices for Data Retention and Policy Creation Will Lower Costs and Reduce Risks"

"How to Determine Whether Your Organization Needs Website Archiving"

"Five Factors to Consider When Choosing Between Cloud and On-Premises Email Archiving Solutions"

Board of Directors Communications Systems

Analysis By: Jay Heiser

Definition: The board of directors communications systems are trusted portals for corporate internal and external board and committee members. Their primary functions are: (1) creation of the quarterly board book; (2) pushing it to encrypted endpoint applications on PCs and iPads; (3) reading and annotation; and (4) remote deletion of the board book. Board communications systems (BCSs) also provide calendaring and secure messaging, and they are based on hardened and encrypted servers.

Position and Adoption Speed Justification: This market has seen rapid growth since the introduction of iPad clients in early 2011, and organizations that were understandably reluctant to undertake the support burden of providing laptops to technology-challenged board members have found tablets to be a virtually no-maintenance endpoint. Although a growing variety of file sharing and collaborative products could meet the security and basic functionality of a board portal, the ability to completely segregate the board from the general corporate environment ensures that corporate administrators have no access to the sensitive material discussed at board meetings.

The majority of Gartner clients with a board portal are using one from a relatively small group of first-tier vendors. These providers offer end-to-end control over the board book and other board communications, targeting corporations and other large institutions that are concerned about unauthorized access to their boards' written materials.

The ability to reliably delete annotated board books and other communications, both from the server and iPads, ensures that records management policies can be met (avoiding the potential for e-discovery). Seatholders have technical support available 24/7. A second tier of vendors targets the boards of community banks, credit unions, healthcare services and charities with less-expensive offerings that provide lower levels of support and less protection for the board book. Virtually all the vendors in this space also provide iPad applications, and both tiers of the BCS market have been growing rapidly during the past three years.

The relative simplicity of this highly specific use case, and the fact that the major vendors have reached functional parity, means that the technology reached maturity and stability relatively quickly, and the word of mouth between board members is encouraging market maturation. Most

buyers remain satisfied with their first choice, and board portals have bypassed the Trough of Disillusionment, and they will reach the Plateau of Productivity within several years.

User Advice: Provide the board of directors with information on the relative differences in risk between the shipping of paper board books and the distribution of electronic board books so that the board can formally accept a recommendation to migrate to a software as a service (SaaS) board portal.

There are surprisingly few decisions to make at the time of purchase. One of the basic decisions to make is whether board members or committee members will be limited to online access, or whether they will be able to synchronize and store the board book locally. This approach, which uses a thick client, provides a richer and more reliable user experience, but it may mean paying extra. Gartner does not consider the generic device protection of the iPad's OS to be sufficient for protecting proprietary and regulated data, so while forcing board members to use a PIN to access their iPads is useful, it is not a replacement for a trusted application. Highly regulated or very visible organizations should use a Tier 1 product that provides end-to-end encryption, and they should allow the corporate secretary to remotely delete the board book after a board meeting.

Although it is possible to log in to a board portal using the Web browser on a Mac, PC or virtually any tablet, board members overwhelmingly prefer that the board book, messages and calendar be synchronized to their device for convenient offline reading. The demand for iPad use is near universal, and the vendors have concentrated their endpoint client development efforts on iOS and Windows.

The majority of Gartner clients are best-served by one of the top-tier vendors. These sellers emphasize end-to-end data protection through server and client encryption and user friendliness, and they offer 24/7 support directly to the board members, through SaaS offerings that have either a SOC2 or ISO 27001 evaluation.

Business Impact: Board portals bring multiple benefits, and it is extremely rare for any organization to revert to paper after having tried a digital system. The early adopters of board portals justified their purchase and use based on cost savings. Traditional, paper-based board books require a great deal of hands-on time on the part of the corporate secretary and the corporate counsel's office. Organizations also save in avoiding the printing and air freighting of 80,000 to 200,000 pages a year.

The most common reason cited for using board portals is the board members' desire for the convenience of being able to access the board material on their tablets.

The Tier 1 products include role-based access controls, server and desktop encryption, and remote deletion from the endpoint. Arguably, these products enable a higher level of control than is possible with old-fashioned paper board books. The ability to reliably delete board book annotations facilitates compliance with records management policies and avoids the potential for e-discovery.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: BoardVantage; Diligent Board Member Services; Nasdaq; Thomson Reuters

Recommended Reading: "Managing Mobile Access to the Cloud"

"Securing the Executive's iPad"

"Mobile Collaboration Will Drive Innovation in Your Workplace"

"Securing Board and Executive Communications on iPads"

Content-Aware Data Loss Prevention

Analysis By: Eric Ouellet

Definition: Content-aware data loss prevention (DLP) tools enable the dynamic application of a policy, based on the content and context at the time of an operation. These tools are used to address the risk of inadvertent or accidental leaks, or exposure of sensitive enterprise information outside authorized channels, using monitoring, filtering, blocking and remediation features.

Position and Adoption Speed Justification: Content-aware DLP technologies include hardware and software solutions that are deployed at the endpoint (desktop and servers), at the network boundary and within the enterprise for data discovery purposes. These technologies perform deep-content inspection using sophisticated detection techniques that extend beyond simple keyword matching (for example, advanced regular expressions, partial document matching, Bayesian analysis and machine learning). Content-aware DLP products also maintain detailed logs that can be used to support investigations.

Organizations continue to struggle with mobile devices and establishing appropriate terms of use — especially as they relate to the interaction with sensitive data. None of the DLP vendors listed in the Sample Vendors section of this technology analysis offer integrated DLP solutions on the mobile device itself, due, in part, to variability of platform versions (Android), closed system architecture (iOS) or computing power available for real-time analysis (Android and iOS). Many are providing pseudosupport by leveraging forced VPN connections to the corporate network and inspecting content data as it exits the internal enclave via DLP network appliances.

Organizations are also beginning to leverage the cloud as a meaningful component of their data centers. Content-aware DLP vendors are now providing offerings to support these initiatives. Content-aware DLP use is rising, and it is becoming an expected practice for many organizations dealing with personally identifiable information (PII) and other regulated data. It is unlikely that an organization would be considered negligent for not having implemented content-aware DLP. However, more and more, content-aware DLP is part of the standard of due care in the U.S., and it will be by 2015 in the EU and in the Asia/Pacific region.

This market continues to experience rapid and steady growth, with estimated total gross revenue over $800 million in 2014. A key factor in the ongoing maturation of the market for content-aware

DLP technology offerings, and the offerings themselves, is the acquisition of small, venture-capital-backed startups by large security suite vendors. These large vendors are able to support complex development life cycles, and they have extensive sales, partner and reseller networks that can deliver content-aware DLP offerings to more-varied client deployment environments.

More vendors of non-DLP products — for example, email, intrusion detection, and identity and access management (IAM) technologies — added or enhanced single-channel content awareness to their products during the past two years. The embedding of content awareness in more products will enable the broad, effective application of protection and governance policies across the entire enterprise IT ecosystem, and throughout all the phases of the data life cycle, becoming what Gartner refers to as "content-aware enterprises."

User Advice: Content-aware DLP technology is commonly perceived as being an effective way of preventing the theft of intellectual property and for prevention of accidental disclosure of regulated information. In practice, it has proved much more useful in helping identify and correct faulty business processes and accidental disclosures and as a means of providing users task- and function-specific policy and procedure education, which is increasingly identified by organizations as the leading value of content-aware DLP deployment. Inadvertent data leakage actually represents the lion's share of the problem, so these automated controls and education are proving useful. However, motivated insiders will always find ways to steal data, and no technology will fully control this.

Organizations should anticipate coverage beyond initial requirements, and they should develop a phased, comprehensive strategy. Based on analysis of the Gartner client base, 35% of organizations start with the network (data in motion), 20% start with discovery (data at rest) and 45% start with a content-aware endpoint. Deployment trends show that organizations start deployments with either network or endpoint capabilities, then follow up with discovery.

As the market continues to develop more content-aware mechanisms, the definition of DLP gets more complicated, vendor marketing messages become more convoluted and finding the right product gets that much harder. Products claiming to be in the DLP market have widely diverging definitions. Beware of vendor claims that present the "real" definition of DLP and the constant reassurance that, whatever you are looking for, it is what they have. It is critical at this stage of market development that organizations approach vendors with a set of independently developed, enterprise-specific requirements.

Lastly, content-aware DLP is not a transparent security control like antivirus protection, firewalls and other security technologies. This means that end users will be impacted when deployed in any mode other than monitoring only. End users need to be trained on the proper way to interact with DLP systems, as well as educated on the proper handling of sensitive data.

Business Impact: This technology is not foolproof, and it is relatively easy for a smart attacker to circumvent, but it effectively addresses the 80% of leakage that is due to accidents and ignorance. Organizations with realistic expectations are finding that this technology does, indeed, meet their expectations and significantly reduces nondeliberate outflows of sensitive data. It is also considered one of the best user education tools because it is capable of reminding a user of an applicable policy at the time of use.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Absolute Software; CA Technologies; Code Green Networks; EMC (RSA); General Dynamics Fidelis Cybersecurity Solutions; GTB Technologies; InfoWatch; McAfee; Symantec; Trend Micro; Trustwave; Verdasys; Websense

Recommended Reading: "Anticipate and Overcome the Five Key Obstacles to Success in Content-Aware DLP Deployments"

"Magic Quadrant for Content-Aware Data Loss Prevention"

"2013 Buyer's Guide to Content-Aware DLP"

"How to Communicate Enterprise Content-Aware DLP Value to Your Senior Executives to Ensure Project Funding"

Climbing the Slope

BCM Planning Software

Analysis By: Roberta J. Witty

Definition: Business continuity management planning (BCMP) software is the key tool used to manage BCM programs. It provides risk assessment; business impact analysis; business process, supplier or vendor, and IT dependency mapping; plan management functionality; and program management metrics and analysis. Some tools also offer plan exercising, resource modeling, and "lite" support for crisis/incident management and emergency notification.

Position and Adoption Speed Justification: Organizations increasingly need usable recovery plans of all types from response to restoration, and a consistent and repeatable plan development process. Also, the growing focus on BCM program metrics has resulted in increased sophistication in BCMP tools. In addition, they integrate with other BCM tools, such as emergency or mass notification service (EMNS) and crisis/incident management (C/IM), GIS, and geospatial tools, creating an ecosystem for real-time situational awareness during an actual disaster. Mature BCM programs use these tools for business and program management analysis with a goal of building more resilience into day-to-day business operations. The biggest competitors to using a BCMP tool are Microsoft Office tools and SharePoint for document management.

With more than 30 vendors, the BCMP market has a 2013 revenue estimate of $162 million, a 24.6% growth over our 2012 estimate of $130 million. The three-year average annual growth rate is 16%. Pricing for this market remains competitive for simpler implementations, while pricing for large, multinational implementations can be in the high six figures or more. Large or regulated enterprises, as well as government agencies, typically use the tools, while small and midsize firms

are increasingly looking to do so. The financial services market and organizations with complex business operations lead the pack in implementations.

Coordinating, analyzing and managing large amounts of availability information are almost impossible to do without a tool. Therefore, the significant growth in adoption of BCMP tools — 24% from 2010 to 2011, 38% from 2011 to 2012, and 42% from 2012 to 2013 (as measured from our annual security and risk management survey) — indicates that organizations are realizing these tools can help standardize and manage recovery plan development, as well as manage the BCM program itself. Having current, effective and exercised recovery plans is the key to success during a disaster, and these tools are essential for effective crisis and business recovery.

We anticipate adoption to continue to grow in the next five years, given the increased focus from government agencies, regulators and private-sector preparedness initiatives. Some of the future growth will come through the governance, risk and compliance (GRC) market as more are providing BCMP capability as part of the broadening operational risk management toolkit. In this year's Hype Cycle, we moved the BCMP market position up by one spot to post-trough 20% from the 2013 Hype Cycle position of post-trough 15%.

User Advice: Consider a BCMP tool when:

- You are starting a new BCM program and want to follow standard practices throughout the organization.
- You are updating your current BCM program and processes.
- You are maturing your BCM program and need more analytics than traditional office management tools can provide.
- You need to integrate plans and partial plans from a number of departments and business units into one consistent, accessible and easily updated plan.
- A merger or acquisition has presented you with the need to create a BCM program reflecting all the elements of your organization.
- You want to conduct the research and planning process in-house, with minimal assistance from outside consultants.

Do not overbuy. Focus on:

- Ease of use in the hands of business users, not IT or BCM program office users only
- Ease of customization — by you, not the vendor — to your organization's continuity delivery framework and so forth
- Ease of reporting, including modifying the report formats provided by the vendor, as well as creating new report formats
- Ease of integration with other important business applications — such as enterprise directories, HR tools, business process management tools (whether internally developed or purchased), change and configuration management databases (CCMDBs), IT asset management tools,

BCM software that your organization may already have purchased (such as EMNS or C/IM software), and news feeds to a BCM program dashboard

- Mobile device (smartphone or tablet) support for recovery plan access and execution at the time of a business disruption.

In addition to a financial statement or strategic plan, a recovery plan is an organizational document that is most likely to result in lost revenue, damaged reputation or worse if it is not current or is unavailable (or nonexistent) at the time of a business disruption. Moreover, like all organizational policies and procedures, the best recovery plan can rapidly become obsolete. Therefore, organizations must consider the recovery plan a living document that needs a continuous review and update process for regular plan reviews (annually, at a minimum, or when there are major business or infrastructure changes) and event-triggered plan reviews (such as changes in operational risk profiles, business or IT processes, and applicable regulations, as well as exercise results showing a gap in plan actions versus current recovery needs).

Business Impact: BCMP tools will benefit any organization that needs to perform a comprehensive analysis of its preparedness to cope with business or IT interruptions, and that needs to have in place an up-to-date, accessible plan to facilitate response, recovery and restoration actions. If used to its fullest potential, a BCMP tool can be used to enhance business operations and resilience outside of recovery and in areas such as HR management, business and IT re-engineering, and mergers and acquisitions.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Avalution Consulting; Bis-Web; BOLDplanning; Continuity Logic; Coop Systems; eBRP Solutions; EMC (RSA); Factonomy; Fusion Risk Management; Inoni; KingsBridge; Linus Information Security Solutions; Metric One; MetricStream; Modulo; Paradigm Solutions International; Phoenix IT Group; Quantivate; RecoveryPlanner; Rentsys Recovery Services; Strategic BCP; Sungard Availability Services; Tamp Systems; Virtual Corp.

Recommended Reading: "Research Roundup: Business Continuity Management and IT Disaster Recovery Management, 2Q13"

"The Continuity Delivery Framework Is Essential for Ensuring Measurable and Sustainable BCM Planning Tool and Program Benefits"

"Business Impact Analysis: Enabling Effective Business Continuity Management"

Crisis/Incident Management Software

Analysis By: Roberta J. Witty; Leif Eriksen

Definition: Crisis/incident management (C/IM) software is used to manage the actions of the workforce and other key stakeholders in response to an incident in a consistent manner so as to return to normal as soon as possible. C/IM functionality includes crisis communications and collaboration, recovery plan repository, plan training/exercising, task and expense management, workforce scheduling, a geographic information system, social media analysis, data visualization, support for multichannel/application viewing, and government agency reporting.

Position and Adoption Speed Justification: The goal of C/IM is to contain and minimize the impact of a crisis or incident (such as earthquakes, power outages, transportation delays, product failures, market shifts, adverse management activity, workplace violence, fires, floods, collapsing bridges, severe weather conditions, terrorist attacks, chemical spills and accidental discharges) on individuals, localities, businesses and public agencies. Damage can be done to an organization's reputation, operations and revenue streams, as well as a government's ability to reduce any adverse impact on public safety. Information security incidents are usually handled by a specialized team under the chief information security officer, but may turn into a larger event that can impact business operations to the point that a disaster is declared. In those cases, the event management would transition to the broader C/IM team.

In recent years, specialized C/IM software tools originally designed for government agencies and utilities have been commercialized for the private enterprise. These tools are used for the following purposes:

- Managing relationships with all organization stakeholders (internal and external)
- Managing response, recovery and restoration actions for the crisis, incident or situation through task and workforce management
- Managing media communications, including national services and social media traffic
- Communicating information internally and externally, typically via emergency/mass notification services
- Providing postmortem reviews of the crisis or incident for regulatory training, reporting and business continuity management (BCM) process improvement efforts

Solutions may be:

- Specialized to the operations of one industry — for example, government, electric utilities, transportation, or oil and gas.
- Generalized for the management of any type of crisis or incident, such as found in a business continuity management planning (BCMP) tool.
- Part of an environmental, health and safety (EH&S) application.
- Part of a case management tool. Many of these products are evolving into centralized "systems of record" and general risk management tools.

Regional and national-scope disasters require enterprise-based C/IM for the critical infrastructure sectors to interact — at least at the level of status reporting and communicating with one another

and with government agencies. As a result, the Federal Emergency Management Agency (FEMA), through the Unified Incident Command and Decision Support (UICDS) Project (a middleware framework to tie together many disparate technologies used for C/IM), will help remove some process barriers in place today, as well as provide meaningful situational-awareness information to public and private organizations. In addition, government and regulatory agency requirements, such as those of the U.S. Occupational Safety and Health Administration (OSHA), National Incident Management System/Incident Command System (NIMS/ICS) and FEMA, are driving more organizations to move to automation.

In the 2014 Hype Cycle, C/IM software remains at the post-trough 20% position because we aren't seeing enough private-sector usage to change the adoption rate. Private enterprises, other than large, multilocation and often multinational organizations, find them rather complicated to use or fit for purpose to only one standard — for example, the NIMS/ICS. Less-complex tools are required for market adoption to rise, and can be found in the BCMP tools market.

User Advice:

- Match the type of C/IM software solution deployed to the most likely and critical types of crises or incidents that pose the greatest operational risk to a company based on a formal, board-approved risk assessment. A financial services company might opt for a solution that provides functionality aligned with an IT outage, a natural disaster or a pandemic, while a heavy-industry manufacturing entity might choose one with functionality tailored for response to EH&S-related crises or incidents.
- Buyers need to be realistic about the initial benefits and the level of effort required to reach these benefits, and they should expect years of slow but steady improvement in the value they extract from this category of product.
- Ensure that the chosen software solution adheres to public-sector crisis/incident protocols relevant to the geographic regions in which the solution is deployed. For example, in the U.S., any solution targeted to respond to physical crises or incidents, such as environmental mishaps, safety issues, or natural disasters affecting health and safety, should adhere to the NIMS/ICS process, as mandated by the U.S. Department of Homeland Security. This will ensure interoperability with public-sector response agencies.
- Manufacturers with exposure to EH&S issues as a result of disruptions caused by natural disasters should adopt solutions that are interoperable with regional public-service protocols to ensure timely and efficient responses to minimize brand damage, and consult with their corporate counsel for jurisdictional issues relating to privacy and rules of evidence.

Business Impact: C/IM processes and software solutions help organizations manage the following actions taken in response to a critical event or disaster that interrupts the delivery of goods and services:

- Improve the organization's ability to protect public safety and to restore business services as quickly as possible.

- Improve the efficiency of crisis/incident command and related emergency responses by continual communication and progress assessment when responding to a disaster.
- Ensure the recovery of expenses incurred during the disaster from business interruption insurance policies.
- Protect the reputation of the organization in the eyes of all stakeholders — employees, customers, citizens, partners and suppliers, auditors, and regulators.

Using a system that imposes a standardized best-practice or leading-practice model extends uniform managerial controls across the organization. It also cuts staff training time and ensures better integration with the broader internal and external community involved in recovering from a disaster.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Crisis Commander USA; Enablon; Enviance; ERMS; Global AlertLink; IHS; Intelex; Intergraph; Intermedix; IntraPoint; Ixtrom Group; MissionMode; NC4; Previstar; ReadyPoint Systems; Reality Mobile; RMSS; SAI Global; Send Word Now; SIS EmerGeo Solutions; Sungard Availability Services; Swan Island Networks; VirtualAgility; Witt O'Brien's

Recommended Reading: "How Gartner Defines Crisis/Incident Management"

"Toolkit: Requirements for Crisis Command and Emergency Operations Centers"

Enterprise Legal Management

Analysis By: John A. Wheeler

Definition: Enterprise legal management (ELM) now encompasses a growing category of corporate software applications focused on supporting the legal department, corporate secretaries, board of directors and senior management through better documentation, spend management, information availability and collaboration. It includes legal matter management, which is focused on managing all aspects of a legal matter and associated cases through the litigation life cycle.

Position and Adoption Speed Justification: Regulations, such as the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 in the U.S., are putting extraordinary demands on the enterprise to exercise good governance, improve transparency and stakeholder communication, manage risk and address a multitude of mandates designed to restore stability to financial markets. The days of trying to manage legal department core processes with word processing, email and spreadsheets are ending. Ad hoc interpersonal relationships and "good enough" information will be replaced with integrated frameworks, templates and workflows that are subject- and domain-focused.

While there are a number of technology providers in this market, the influx of new regulations will create a substantial amount of uncertainty between what is needed and what the products deliver. The rules that will make up the regulations are still being written, even as enterprise legal management suites are being enhanced.

User Advice: IT professionals should begin by assessing how their in-house legal team currently manages day-to-day activities. This includes internal timekeeping and expense data, internal matter and custodian tracking, preservation hold notifications, collections, productions to outside counsel, tracking of billable hours for outside counsel and event scheduling. Additionally, IT needs to be aware of who has input and who makes the final decisions, in terms of governance and risk management. Finally, what are the deliverables that constitute the fulfillment of all the necessary mandates?

IT should expect this process to be challenging. For example, recent amendments to the Federal Rules of Civil Procedure have placed a much higher level of professional responsibility on lawyers to understand their organizations' and clients' technological infrastructure, data security operations, policies and procedures. On top of an increase in regulations, the legal profession is finally realizing that it, too, will need to embrace new ways of doing its job. ELM software will help legal professionals maintain the necessary legal matter documentation and collaborate with key internal and external stakeholders. In addition, the software will provide greater transparency into the financial operations of the legal department.

Business Impact: In-house counsel can lower costs, increase efficiency and avoid risk by adopting either on-premises or cloud-hosted solutions. Enterprise legal management is, however, closely related to a number of other systems, and specific components of suites often lack all the functionality of point solutions. This is particularly true for e-billing, which helps the corporate legal department to track its spending with outside law firms. Moreover, vendors from a number of adjacent markets, such as e-discovery, enterprise content/document management, and legal governance, risk and compliance (GRC), as well as professional services players, are interested in building better relationships and offerings that may further expand this market.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Sample Vendors: Bottomline Technologies; Bridgeway; CSC; Datacert; Economic Analysis Group (EAG); Legal Suite; LexisNexis; LT Online; Mitratech; Serengeti Law; Thomson Reuters; Wolters Kluwer

Recommended Reading: "Magic Quadrant for Enterprise Legal Management"

"IT Planning Guidance for Legal Professionals: The Gartner Legal IT 2020 Scenario"

Identity Governance and Administration

Analysis By: Felix Gaehtgens; Brian Iverson

Definition: Identity governance and administration (IGA) is for: (1) managing the identity life cycle; (2) requesting, approving, certifying, remediating and auditing access to applications, systems and data; and (3) fulfilling requests for automated provisioning, modification and termination of user access on target systems and resources. IGA can also provide identity analytics capability, role design and access modeling features. IGA solutions combine both business user interface and IT administration functionality to govern access in the enterprise.

Position and Adoption Speed Justification: IGA is now fully recognized as a distinct market, and it is difficult for vendors to get traction in this market without both governance and fulfillment capabilities outside of markets with minimal compliance obligations, such as education.

Organizations seeking IGA tools tend to focus on the following capabilities when writing RFPs:

- Configurable business-centric interface for end-user interaction, including new identity creation, access requests, password management and monitoring the status of outstanding requests
- Workflow for orchestrating approval processes
- Policy management to support connecting users with application access, based on rules, roles, and detection of segregation of duties and other policy violations
- Role and entitlement discovery, and mining and engineering tools to build an identity data model
- Connectors to directories; identity and access data repositories; and applications and systems for bidirectional control and data collection, provisioning, deprovisioning, and data synchronization
- Log data monitoring, collection, and correlation of identity and access activities and events (including administrative events)
- Analytics for modeling, and simulation for audit, compliance, forensics and intelligence purposes

The primary drivers for IGA in the enterprise are:

1. Internal audit reporting for regulatory compliance directives
2. Operational efficiency

IGA is also extending to other use cases, such as managing external identities and facilitating the adoption of new technology. Additionally, due to the horizontal nature of IGA within organizations, business enablement is starting to emerge as a driver for this technology. IGA can help organizations become more agile, help organizations undergo transformation, and drive innovation by acting as an enabler for reorganization and adoption of new business models.

The IGA solution market came from the convergence of two related identity and access management (IAM) markets: user administration and provisioning (UAP), and identity and access governance (IAG). Some providers of IGA tools and services come from either the UAP or IAG side, and are supplementing or partnering with other vendors to resell features in the corresponding technology area. Other providers have acquired or merged, or are in the process of merging the UAP and IAG platforms by eliminating overlapping functions and expanding the pool of decision makers for acquiring the solution. Progress for IGA has been slow due to the ongoing convergence of the platform. This convergence also initiates the creation of a smaller, more focused market for identity analytics and intelligence (IAI) tools, also in the Hype Cycle.

User Advice: Focus on defining and refining approval and certification processes before selecting and implementing IGA tools. Use these processes to gauge product feature requirements, particularly for user experience — IGA is first a business tool and then an IT tool, and should be deployed as such.

- Start IGA deployments by first focusing on access governance features like access requests, access certification and policy administration. Use IGA to drive manual fulfillment initially, and add automated provisioning and deprovisioning only where it adds value for systems that are easy to integrate or with high transaction volumes.
- Establish an identity data and log model that aligns with specific business processes and the use of access certification controls.
- New use cases around mobility, cloud and external identities are driving IGA vendors to develop capabilities that are differentiators for IGA products. Also, organizations are establishing multiple parallel product-based teams that create requirements beyond the single hierarchical relationship model traditionally catered for by these products. Evaluate vendor road maps in light of these capabilities to align with your midterm to long-term vision.

Business Impact: IGA is the second-generation IAM solution for identity administration, governance and intelligence that consolidates functions in those areas into a single platform. IGA provides hands-on governance capabilities to the business owners of identity for direct accountability of access to their business information, transparency for audit and compliance, and granular control of that access.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Adolescent

Sample Vendors: AlertEnterprise; Atos; Avatier; Beta Systems; Caradigm; CA Technologies; Courion; CrossIdeas; Deep Identity; Dell Software; e-trust; Evidian; Fischer International; FSP GmbH; Hitachi ID Systems; iSM Secu-Sys; IBM (Tivoli); Microsoft; NetIQ; Omada; Oracle; RSA Aveksa; SailPoint; SAP

Recommended Reading: "Magic Quadrant for Identity Governance and Administration"

"Best Practices for Managing Identity Data and Log Models to Optimize Identity Data Quality"

Operational Risk Management

Analysis By: John A. Wheeler

Definition: Operational risk management (ORM) software applications support the ORM discipline within a broader enterprise risk management (ERM) program. Operational risks are defined by Gartner as those risks that "relate to the uncertainty of daily tactical business activities, as well as risk events resulting from inadequate or failed internal processes, people or systems, or from external events."

Position and Adoption Speed Justification: ORM software applications allow organizations to aggregate and normalize data from multiple data sources, including operational and financial systems, as well as external sources such as regulatory alerts and loss event databases. By providing a better understanding of the risks to business objectives, ORM enables better business performance and capital allocation. ORM applications also help companies address the increasing pressure from regulators to improve the risk reporting in annual reports and improve the board of director's role in enterprisewide ORM oversight. ORM applications usually include functions for risk analytics as well as risk indicators to support decision making.

ORM applications are becoming increasingly important because of the growing need for organizations to meet compliance and regulatory requirements and the desire to avoid severe punishment from regulators. This is especially true in North America and Europe, and is the primary reason for the increase in technology maturity. ORM applications are not only implemented in developed markets, but are also gaining importance in developing markets, such as China, South Africa and India, where the local regulators are increasingly emphasizing the role of ORM to combat fraud, bribery and other persistent risks. Although elements of ORM have been in existence for many years, sophisticated analytics and modeling capabilities are increasingly in demand, which has attracted analytics vendors like IBM, Oracle, SAP and SAS to the market.

User Advice: Companies must ensure that they are using comprehensive and integrated ORM applications to assess the various risk types in their organizations. Regulators and other stakeholders will pay much more attention to risk management practices as part of their financial supervision, and the lack of comprehensive ORM modeling and reporting use could not only result in lower credit ratings by financial services providers, but also threaten the public accreditation of organizations.

ORM applications also require consistent risk management policies, which often necessitate staff retraining, as well as the implementation of new compliance policies and procedures. The change management associated with establishing a risk-aware culture and implementing new policies is often the most difficult aspect of adopting ORM.

In addition, it is crucial to harmonize and consolidate data sources across the company on a continuous basis, rather than a single point in time. This may create some challenges from a process, as well as an IT redesign perspective. The integration of various data sources is, on the other hand, critical for the eventual success of a top-down risk management dashboard that is

accurately displaying bottom-up data. While some companies may aspire to have a single ORM application to cover all risks, it may be more practical to have several ORM applications that focus on related risk areas such as information technology risk. The ultimate goal should be deploying ORM applications that can be integrated and fit the existing IT architecture.

Business Impact: The use of ORM applications will help organizations to improve data quality and support adequate reporting to national and international regulation authorities to avoid regulatory risks. Without the appropriate ORM applications, organizations will not have adequate analysis and insight into their aggregate risk positions, or the ability to comply with new capital adequacy regulations, such as Basel III and Solvency II.

When done well, ORM can improve the ability of an enterprise to achieve its strategic objectives — it is a critical tool for improved governance in that it is the primary means to ensure that process and behavioral tolerances remain within the bounds that optimize performance to meet objectives. ORM will always be a work in progress because of adaptations to new regulations or business processes. The positive news is that ongoing attention to risk management is increasing the degree to which organizations use a single ORM framework, breaking down the barriers between corporate silos, leading toward an ever greater consolidation of risk data and providing ever more comprehensive understanding and management of the overall risk portfolio within the executive suite.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Active Risk; BWise; Cura Technologies; IBM; Mega International; Methodware; MetricStream; Optial; Oracle; Resolver; Riskonnect; RSA The Security Division of EMC; SAI Global; SAP; SAS; Software AG; Sword Achiever; Symbiant; Thomson Reuters; Wolters Kluwer; Xactium

Recommended Reading: "A Risk Hierarchy for Enterprise and IT Risk Managers"

"How to Use Pace Layering to Build a GRC Application Strategy"

"The Gartner Business Risk Model: A Framework for Integrating Risk and Performance"

"Introducing the ERM/GRC Blueprint for a Successful Risk Management and Compliance Program"

"Seven Keys to Successful and Cost-Effective Risk Oversight"

Product Safety and Compliance

Analysis By: Janet Suleski

Definition: Product safety and compliance applications are a subset of the environmental, health and safety (EH&S) market, designed to provide support and enforcement for a range of processes: the management of content, such as substance and regulatory databases; the management of

documents, including material safety data sheets (MSDSs); and the associated compliance reporting.

Position and Adoption Speed Justification: Every manufacturer is affected by product safety regulatory mandates, whether they are a producer or user of potentially hazardous materials. Examples of regulations governing product safety and compliance include the European Union's Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH) and the Restriction of Hazardous Substances (RoHS), and the U.S.'s Dodd-Frank Wall Street Reform and Consumer Protection Act clauses restricting the use of conflict minerals. In addition, there is a broader movement to incorporate sustainability into the product life cycle management (PLM) process. Overseeing all this in the context of increasingly complex global supply chains and ever-changing regulatory environments is driving new investments and approaches to managing the product safety process. As the market consolidates, integration to enterprise systems is an ongoing concern.

The market for product safety and compliance is somewhat mature in industries such as industrial equipment. A combination of acquisitions and organic growth by market leaders has left only a handful of major vendors. Owning the content and providing the analytics to support new product development that is consistent with safety and compliance requirements are differentiators. However, in industries such as apparel and footwear design and manufacturing, the technology landscape is immature, and the business process remains highly manual. A largely automated end-to-end product safety and compliance process is still an aspiration for many in this industry. Broadly speaking, new and fast-changing compliance requirements — particularly around sustainability and green supply chains — as well as the ongoing evolution of quality and safety compliance, means that this software market has slipped backward from its 2013 maturity level to a more adolescent stage of market development.

The market continues to innovate to keep up with changing product safety and compliance requirements. In particular, the market is seeing a move toward business process outsourcing (BPO) as companies acknowledge the challenges of keeping up with changing regulations and suppliers. Product safety and compliance BPO can be in the form of simple outsourcing of internal processes or the use of third-party hubs to serve as a central repository of supplier data and regulatory content. The latter is a more nascent capability that will keep the market somewhat unsettled for the near term.

User Advice: Product safety and compliance are not optional activities, and managing the process manually is inefficient and prone to error. In addition, ongoing changes to regulations — such as the 2012 Occupational Safety and Health Administration (OSHA) decision to align the current Hazard Communication Standard (HCS) with the United Nations' Globally Harmonized System of Classification and Labelling of Chemicals (GHS) — add to the challenge of staying in compliance. The developing maturity of the technology options reduces the risk of replacing manual processes or legacy systems.

The choice of provider is a function of the needs of the buyer. Any industry with a need to bring new products to market in a timely and cost-effective manner will need a vendor that can support the full range of authoring, analysis and management functionality. The importance of integration to PLM and ERP systems comes to the fore in these scenarios as well. On the other hand, for companies

simply in need of limited-volume, inbound MSDS management, there are low-cost options, including the use of some form of cloud service. Some vendors can provide both.

One area of innovation to be aware of is the effort of several vendors to build product safety and compliance "hubs" or services to streamline the process of ensuring that the components or materials received from suppliers are compliant and/or will not adversely affect the final product's own compliance profile. These efforts promise to make the product compliance more efficient for all parties and, more significantly, reduce the time to market of new or modified products. However, the true value of the hubs is only realized once a critical mass of suppliers is onboard. It's also not clear what role the more generic supply chain hubs will ultimately play in this development. Several are in a good position to add or acquire functionality in this area, thereby contributing to the consolidation and innovation still possible in this market.

Business Impact: Failure to effectively manage hazardous materials and adhere to the local regulations regarding the safe use of products can result in fines or, more significantly, injuries to employees or customers. Although these risks have been well-defined and subject to regulation in many jurisdictions for a number of years, what is changing is the need to factor in an increasingly global approach to managing product risk and compliance. The use of globally diverse suppliers increases the complexity of compliance and adds risk to business metrics, such as perfect order and product cost. Therefore, although often thought of as a cost of doing business, product safety and compliance can be used as a competitive advantage.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Adolescent

Sample Vendors: 3E Company; Actio; EtQ; icix; IHS; Safetec; SAP; TEXbase; UL Workplace Health and Safety

Recommended Reading: "Magic Quadrant for Environmental, Health and Safety Management Systems"

"EQM Hubs Unite Quality Management IT Systems Across the Value Chain"

"Building Sustainable Supply Chains"

Database Audit and Protection

Analysis By: Brian Lowans

Definition: Database audit and protection (DAP) tools provide a centralized security for different relational database management systems (RDBMSs). The core capabilities of DAP tools have developed beyond basic activity monitoring to include data discovery and classification, threat and vulnerability management, application user analysis, intrusion prevention, and activity blocking. Most tools also offer data protection options through encryption, tokenization or data masking.

Position and Adoption Speed Justification: Databases are typically the main repository for regulated data, such as healthcare, financial, personal and credit card, as well as intellectual property. DAP provides a real-time forensic and preventive control. It mitigates risks that are not addressed solely by preventive controls, such as identity and access management and encryption.

There are four primary use cases for DAP:

1. **Privileged user monitoring:** This identifies and assesses the who, what, why, where, when and how of database administrators, system administrators and other users with highly privileged access. This use case covers access to data, as well as anything that goes on "under the covers," including configuration changes, schema changes and account management activity.
2. **Application user monitoring:** Users with legitimate access may use this access, either accidentally or maliciously, to violate policy and cause exposures. Accessing too much data too fast, or mistakenly leaking data to which they have access, may result in a significant security incident.
3. **Attack prevention:** The ability to identify and mitigate open vulnerabilities or exposures within the RDBMS and then map them to malicious activity is growing in importance with Gartner clients and has become more common as DAP tools continue to mature the extended capabilities.
4. **Data privacy/residency:** The ability of DAP to manage the segregation of duties of privileged and application users has shown increased interest by Gartner clients to protect the privacy of data within geographic jurisdictions. This has led to increased interest in adding data protection through encryption, tokenization or data masking.

DAP's move through the Hype Cycle has slowed because of the enhancement of functionality. The core monitoring capabilities are quite mature, but the extended capabilities are still continuing to develop to include big data platforms such as Hadoop.

The DAP market continued to experience moderate growth through 2013/2014, due to organic growth of existing customer deployments, strong growth to cater for data residency issues and adding new clients in EMEA and Asia/Pacific. While the preventive controls continue to mature, vendors need to continue developing the capabilities for protection at rest and also in use. Use of encryption, tokenization and data masking can offer enhanced segregation of duties for particular use cases.

User Advice: DAP provides a comprehensive security suite compared with alternatives. Moreover, DAP provides comprehensive, cross-platform support in heterogeneous database environments. Clients should implement DAP functionality to mitigate the high levels of risk resulting from database vulnerabilities, to address audit findings or to enforce segregation of duties. However, alternative technologies can be used in limited use cases:

- Consider security information and event management (SIEM) tools as an alternative option in cases where native logging is available, overheads fall within acceptable limits and there is minimal need for granular monitoring.

- Consider content-aware data loss prevention (DLP) tools as an option only in cases where the focus is skewed toward the data accessed from the database, with the understanding that DLP can't tell you anything about what goes on within the RDBMS structures "under" the data.

Business Impact: DAP is an important addition to risk management programs and to implement enterprise data security governance strategies. It is a worthwhile investment for clients with RDBMSs or Hadoop deployments containing regulated or business-critical data. It is also showing increasing value to simplify audits, and it is enforcing the segregation of duties.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Sample Vendors: Fortinet; GreenSQL; IBM; Imperva; McAfee; Oracle; Trustwave; WareValley

Recommended Reading: "Apply the Nine Critical Capabilities of Database Audit and Protection"

"Big Data Needs a Data-Centric Security Focus"

"Five Cloud Data Residency Issues That Must Not Be Ignored"

Microsoft Resource Access Administration

Analysis By: Felix Gaehtgens

Definition: Microsoft resource access administration (RAA) products manage access rights to users for resources specific to the Microsoft environment. RAA also reports on user access to those resources, and provides users with a view of only the resources to which they have access.

Position and Adoption Speed Justification: There are two major RAA product types on the market: (1) midrange and mainframe — covering IBM i, IBM z/OS, HP NonStop and so on; and (2) Microsoft. Examples of resources covered by this latter category include folders, files, printers and other system objects shared among groups of end users and resources managed by Microsoft applications such as SharePoint. Other file system environments, such as network-attached storage (NAS) or other file servers, can also be managed. RAA products use grouping constructs from Microsoft Active Directory to assign access, and manage access control lists associated with protecting these resources.

Some of these products expose capabilities that are found with unstructured data access governance products:

- Audit of what resources a particular group construct will grant access to
- Automated scanning and classification of data
- Certification of access to high-risk data or resources

While Microsoft provides some RAA functions in various products, Microsoft partners and other unaffiliated vendors provide specific products for Microsoft RAA.

The position of the Hype Cycle entry for Microsoft RAA reflects some progress in adoption, but challenges remain:

- Increased functionality overlap with other identity and access management (IAM) products — such as identity governance and administration (IGA), and data access governance (DAG) — which continue to offer competitive alternatives
- The rapidly changing Microsoft infrastructure and software environment, and its increasing demands for alternative administration needs, particularly for Microsoft's Windows-Azure-based services and Microsoft Dynamic Access Control (DAC)
- Coordinating with storage vendors for marketing and selling together, and aligning product road maps

Some organizations acquire these products as administrative tools to compensate for gaps in Microsoft's administrative tooling. In this case, while there is some overlap with other IAM products, the focus tends to be different, and these tools provide a "good enough" capability targeted toward IT administrators who are managing a smaller-scale deployment on a relatively tight budget. Other organizations acquire RAA tools as part of overall IGA requirements, or as supplemental options to existing IGA products (in some cases, through OEM relationships).

Patterns of adoption follow the adoption of large-scale Microsoft software implementations, such as SharePoint and Exchange. Barriers to adoption include the increasing number of RAA features incorporated into competitive IAM products.

User Advice: Consider RAA for Microsoft products when you need to:

- Manage resources in a delegated model (that is, allow the end users, or branch or store managers, to manage resources specific to them)
- Audit or report on object ownership (or access) from a group, end-user or resource perspective
- Provide users with a restricted view of network-available resources
- Use identity and access governance products for reporting needs by resource
- Manage simple or smaller-scale deployments, have no plans for deploying IGA technology at this point, and are looking for a targeted solution to address specific gaps within Microsoft's native tooling

Business Impact: Microsoft RAA products may benefit any organization that manages Microsoft Active Directory security groups and uses them to manage access to resources on supported Microsoft-based target systems.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Sample Vendors: Beta Systems; BeyondTrust; CionSystems; Dell Software; Hitachi ID Systems; Imanami; NetIQ; STEALTHbits Technologies; UpperVision; Varonis Systems; Whitebox Security

Recommended Reading: "Active Directory: Options to Mitigate Commonly Cited Weaknesses"

"Active Directory Bridge Products: Reducing Management Complexity"

"Effective Active Directory Group Management"

Quality Process Management Applications

Analysis By: Simon F Jacobson

Definition: Quality process management applications are a subset of quality management systems (QMSs) that digitally represent standard operating procedures that govern, support and enforce conformity to quality standards ranging from internally defined business rules to International Organization for Standardization (ISO) standards or other industry-specific and customer-mandated quality standards.

Position and Adoption Speed Justification: For most organizations, the various methods and procedures for quality management are enforced through fragmented business processes and IT architectures populated with point applications for specific functions. In several instances, these have been acquired out of defensive need to improve an individual quality process such as nonconformance management, failure modes and effect analysis (FMEA), or auditing. Blended homegrown applications or different systems from multiple providers result in loosely integrated data models and workflows that increase data latency, cost and risk, and lead to a lack of visibility and accountability across production units and functions.

Moving toward a complete approach to enterprise quality management necessitates common systems, processes and data definitions. Buyers are seeking vendors that can deliver a full application suite to support this. Buyers find that QMS vendors have morphed into full-scale software providers using cloud delivery models, supporting mobile devices, and offering analytics modules and graphical modeling environments to orchestrate processes such as inspections or audits globally. Additionally, ERP; governance, risk and compliance (GRC); and product life cycle management (PLM) vendors also seek to provide modules in this area. Within manufacturing operations, manufacturing execution systems (MES) vendors are offering some capabilities as well. Lastly, the target market has some fragmentation to it. Quality standards differ by industry (such as the U.S. Food and Drug Administration [FDA] regulations specific to life sciences), which drives some companies to be specialists within segments. This will impact selections and capabilities in some markets.

This class of quality management applications remains stable on this year's Hype Cycle. While many companies are floating RFIs and RFPs in the market for a single vendor application, a smaller subset is making selections and reporting complete, multiple process deployments. In many cases, Gartner clients report provider technology advancement ahead of customer readiness. The root

cause is often the absentia of a disciplined approach to enterprise quality architecture as a whole, challenging the ability to execute a holistic deployment. As these full-scale deployments take root, this will progress toward the plateau.

User Advice:

- Start with a single process like nonconformance management, change control or audits, and then expand into multiple processes. Ensure a closed-loop for feedback as part of the process design.
- Look for a complete solution that links with your overall enterprise quality management approach. Today's quality process management vendor should have a cloud deployment capability, analytics (not just reporting) and support for mobile devices either in future releases or on the long-term road map. This also includes support for other supply chain functions beyond manufacturing.
- Where suitable, extend process support to suppliers (such as advanced product quality planning [APQP] and production part approval process [PPAP]) and to trading partners.
- Balance the approach between products, processes and services added alongside products sold.

Business Impact: Corporate operations and supply chains continue to be exposed by gaps in their quality processes and supporting data, with the financial performance implications and risks only increasing. Businesses that have multinational and offshore manufacturing centers are particularly vulnerable to negative brand impact from quality issues, such as lead paint in children's toys or poor quality in automobile tires. A stringent quality-compliance program supported by robust tools can prevent unsafe, dangerous or shoddy products from reaching the market.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: EtQ; Intelex Technologies; MasterControl; Oracle; Pilgrim Software; PTC; SAP; Siemens; Sparta Systems

Recommended Reading: "Best Practices for Taking Quality Beyond Manufacturing and Into a Business Capability Supporting the Value Chain"

"Cost of Poor Quality Is a Component of Supply Chain, Not Just Manufacturing"

"EQM Hubs Unite Quality Management IT Systems Across the Value Chain"

Enterprise Information Archiving

Analysis By: Alan Dayley

Definition: Enterprise information archiving (EIA) solutions provide tools for capturing all or selected data in a distributed or centralized repository for efficient storage and access. EIA supports multiple data types (including email, file system, social media, Web, mobile and Microsoft SharePoint). These tools provide access to archived data via a stub or pointer or via browser-based access to the archive, and some manage the data in place. EIA tools support operational efficiency, compliance, retention management and e-discovery.

Position and Adoption Speed Justification: The number of vendors offering EIA solutions continues to increase, with most offering functionality and deployment models appropriate for the markets they target. Market growth remains healthy, particularly as the utilization of archiving as contributing technology for compliance and e-discovery gains favor with organizations implementing information governance programs. Archiving software as a service (SaaS) for messaging data, including email and social media, has gained significant traction as an alternative to on-premises deployments (and is now growing at a faster pace).

Support for the capture and supervision of social media (for example, Twitter, Facebook and LinkedIn) has become a requirement in the regulated financial services industry (and is interesting to other industries). File system archiving as a component of enterprise information archiving is evolving with an even stronger focus on storage management as unstructured data grows in volume. Overall, enterprise information archiving products that support multiple content types are replacing application-specific archiving solutions. Some companies are looking to replace their current archiving products with others (particularly as public cloud solutions gain traction), and more and more consulting companies are offering migration services. In addition, there is growing interest in managing the compliance and retention of data "in place" instead of moving to a different repository.

Companies with large volumes of data and long retention periods overtax the system so that it might not be scalable or reliable, thus requiring improved index methods and, in some cases, major architectural changes. The appetite for email-only archiving solutions remains, but most organizations are looking to vendors with existing solutions or a road map for enterprise information archiving products.

User Advice: As requirements to store, search and discover old data grow, companies should implement an enterprise information archiving solution now, starting with email as the first managed content type. Mailbox size for on-premises email implementations continues to grow, creating both storage and compliance concerns. Many organizations are alternatively looking to migrate to cloud email and productivity solutions such as those offered by Microsoft and Google, and when migrating, associated compliance and regulatory retention requirements need to be considered. Consolidating archived data into regional repositories, a centralized repository or the cloud can support a quick response to discovery requests and will facilitate a quick implementation of the organizational retention policies. Migrating personal stores, such as PSTs, to the archive should be part of the deployment of an email archive system.

Business Impact: Enterprise information archiving improves application performance, delivers improved service to users, and enables a timely response to legal discovery and business requests for historical information. Archived data can be stored on less expensive storage, with the

opportunity to take some data offline or delete it. Moving old data to an archive also reduces backup and recovery times.

Archiving is designed to keep the active data stores as small as possible, improve application performance and reduce recovery times. Email remains the predominant content type archived as part of an enterprise information archiving implementation. In this case, the need for users to maintain personal stores is eliminated, and established stores can be migrated to the archive, leading to less risk associated with loss or theft of devices housing these personal archives. Archiving offered via SaaS is increasing in popularity because of the benefits associated with offloading low-business-value tasks, such as the management of aging data, to a third party, as well as reduced capital and operational expenses. SaaS-based message data archiving (namely email, but with increased interest in social media and Web content) is leading the way because it is currently priced on a per user, per month (PUPM) basis with no storage overages. Over time, as cost structure and integration issues are ironed out, look for more file system data and application data to be archived in the cloud.

Enterprise information archiving has become an important part of e-discovery, providing functionality identified as part of the information management category of the Electronic Discovery Reference Model (EDRM). Features such as legal hold, retention management, search and export are used to meet discovery and compliance requirements. Supervision tools for sampling and reviewing messages (email, instant messages and, in some cases, social media content) are available with many enterprise information archiving products in response to requirements specific to the regulated portion of the financial industry. To meet the requirements of mobile workers, enterprise information archiving offers a way for organizations to have the option of keeping data compliant within an archive while providing access to it via mobile devices.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: ArcMail; Barracuda Networks; Bloomberg; C2C Systems; CommVault Systems; dataglobal; EMC; Global Relay; Google; Gwava; HP-Autonomy; IBM; MessageSolution; Metalogix Software; Microsoft; Mimecast; OpenText; Proofpoint; SilverSky; Smarsh; Sonian; Symantec; ZL Technologies

Recommended Reading: "Magic Quadrant for Enterprise Information Archiving"

"Best Practices for Data Retention and Policy Creation Will Lower Costs and Reduce Risks"

"How to Determine Whether Your Organization Needs Website Archiving"

"Five Factors to Consider When Choosing Between Cloud and On-Premises Email Archiving Solutions"

Foreign/Global Trade Compliance

Analysis By: William McNeill; C. Dwight Klappich

Definition: Foreign/global trade compliance (GTC) addresses the rules, regulations and costs (such as duties and taxes) when conducting cross-border trade. GTC is a main component of a broader category of software called global trade management (GTM), which also looks at the logistics and financial aspects of conducting global trade.

Position and Adoption Speed Justification: GTC solutions have three primary components: the business application, the trade content and, where necessary, connectivity with customs authorities for document filing. Trade content is the repository of the data, rules and costs for each harmonized tariff schedule code by source or destination country, as well as the special rules governing regional trade agreements. Some GTC vendors provide the application and the content, while others provide only the application, with the customer sourcing the content independently, either from a third-party subscription service or manually, directly from the appropriate government sources. Holistic GTC solutions cover restricted, denied or sanctioned U.S. Office of Foreign Assets Control (OFAC) screening; import compliance; export compliance (sometimes referred to as license determination); and support for regional trade agreements, free trade zones and other duty drawback programs.

Although elements of GTC, such as restricted party/OFAC screening regulations, have been in place in the U.S. since World War I, knowledge of these rules is widespread in some industries, but less extensive in others. While the OFAC affects consumers individually as well, few have heard of it, except as a Cold War artifact restricting their access to Cuban cigars and rum. The usefulness of sanctions as a tool of statecraft has been questioned, but trade sanctions and interdiction lists are an increasingly popular "action other than war" to enforce national policies with a limited risk of casualties.

GTC is a mature application category, but solutions continue to evolve to cover more geographies within a single solution and to enable broader trade compliance coverage. However, GTC remains underautomated, largely because many companies lack the internal expertise to perform it in-house, regardless of the availability of good systems, so they outsource GTC to third parties, such as customs brokers, third-party logistics (3PL) providers or freight forwarders. However, even in an outsourced environment, the shipper (i.e., brand owner) is still ultimately responsible for compliance issues and should maintain some visibility into operations. Ideally, compliance issues should be sorted out ahead of time and not at the point of order. Gartner finds the GTC vendor landscape changing, with new entrants moving in front of more established vendors for several reasons, including newer and more flexible technology, richness of trade content or the availability of GTC as part of an integrated GTM suite. Today, no single GTC application covers every type of trade control across all industries or geographies, so specialized solutions remain (for example, free trade zone management). Furthermore, as the scope of global trade controls expands, specialized solutions will emerge, and these capabilities will continue to be merged into broader suites from GTM, ERP and supply chain management (SCM) vendors. We believe global trade content has the potential to affect more strategic sourcing, product life cycle management (PLM) decisions and applications, as well as go-to-market strategy. Restricted party screening has been used in other areas, including screening in human resources and as part of e-commerce websites.

User Advice: Users must understand that the business application and the trade content are two independent, but tightly connected, aspects of GTC solutions. They must first understand their content needs and then use this information as they evaluate GTC offerings to ensure that the solutions address their compliance needs. Although there are advantages to a single-vendor offering of the application and the content, this should not overshadow all other considerations, such as integration with back-end systems, vendor domain expertise and the cost of ownership. Additionally, users should evaluate software based on whether they will be doing their own document filing directly with various customs bureaus or outsourcing document submission. In the case of the latter, direct electronic connections are not as important as the document generation itself or the visibility layer to track the status of submissions.

Users must be cognizant of the evolving nature of compliance mandates, such as the Registration, Evaluation, Authorisation and Restriction of Chemical (REACH) substances, International Traffic in Arms Regulations (ITAR), Restriction of Hazardous Substances (RoHS), regulations around conflict minerals and other new and changing mandates. The U.S. Customs and Border Protection website is a good place to start, but will not cover everything. Other sources include the U.S. Department of Commerce. As these regulations continue to change, users need to consider the flexibility and adaptability of the application to support change. Some of these regulations (ITAR, for example) have not only document filing requirements, but also rules for data storage and use, which extend beyond the expertise of many GTC providers, and have created the rise of special vendors that address this security issue. Therefore, IT managers also need to understand how these compliance regulations affect their systems and processes, as well as master data management issues.

Implementation time for these applications varies widely. If a company is simply instituting denied party screening (DPS), for instance, then the project time can range from nothing (for example, the company simply signs up for a third-party content service, and enters names and addresses manually on an ad hoc basis) to a few weeks or months (for example, the DPS system is incorporated into the workflow of other business processes, such as order management or customer creation). More complex compliance systems for global companies with many locations around the world often take 12 months or more, typically rolled out in several phases. Additionally, most companies take a conservative and somewhat slower approach to systems implementation to mitigate risk and accommodate the necessary change management processes that often include new training for all employees, not just on systems, but on regulations as well.

Enterprises and individuals should prepare for unannounced shifts in enforcement emphasis and ever-tightening regulations. Essentially, the heat can be turned up or down at will (for example, through the granting of humanitarian exemptions) without legislative or judicial input, as a way of fine-tuning government pressure on a foreign entity. Additionally, any act of terrorism or instability has the potential to elevate the criticality or magnitude of certain compliance requirements.

Business Impact: While any company that conducts cross-border trade has to comply with global trade compliance rules and regulations, it has the option either to outsource these capabilities to customs brokers or to bring these capabilities in-house, supported with GTC technologies. GTC is an important application category, but not many companies are using it as a value-adding area. It is important because not adhering to the rules that govern trade can result in delays, and, in some cases, fines, seizures of goods and jail time, all of which expose the company to unnecessary risk. Effective and efficient GTC processes and systems can increase supply chain agility and inventory

velocity by allowing product to be processed and shipped in a timely manner, especially if the company is part of voluntary trade programs like Free and Secure Trade (FAST) or Customs-Trade Partnership Against Terrorism (C-TPAT).

Being "world class" at trade compliance is not a source of business differentiation for most companies. However, leading companies will use it to promote the brand in ethical business practices or as part of a more strategic sourcing effort. The business benefits can include reduced administrative costs, avoidance of penalties and less disruption in the flow of goods. For example, by automating these processes, many companies find that the cost of processing documents and the money spent on couriers fall dramatically. Additionally, by using regional trade agreements and duty drawback programs strategically, there are tremendous savings to be had. So, while this does not add competitive differentiation, cost avoidance can be significant. Even in outsourced environments, this software can give a company real-time visibility into the status of submissions placed on their behalf and reduce the time needed for any error mitigation.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Amber Road; Customs Info; Integration Point; Kewill; LexisNexis; MIC Customs Solutions; NextLabs; Oracle; QuestaWeb; SAP; Thomson Reuters

User Authentication Technologies

Analysis By: Ant Allan

Definition: User authentication technologies encompass a variety of products and services implementing a range of authentication methods in place of legacy passwords. Methods are typically classified by the kind of authentication attributes (or factors) that they use, alone or in combination; contextual authentication now supplements the canonical three factors. Authentication may be natively supported in products or services (including other security tools) or provided by discrete software, hardware or cloud-based services.

Position and Adoption Speed Justification: Legacy passwords remain a ubiquitous user authentication method, but one which is notoriously weak. As James Martin noted in 1973, "Passwords will keep out the casual intruder, but not one who is determined" (*Security, Accuracy and Privacy in Computer Systems*; Prentice-Hall). Neither increasing password length and complexity nor forcing periodic changes — either of which may be demanded by auditors in the name of regulatory compliance or sometimes explicitly demanded by regulations themselves — is effective against deliberate attacks or accidental leakage. Multiple incidents (most recently, as of May 2014, Heartbleed), as well as compliance hype, continue to highlight the weaknesses of legacy passwords.

User authentication technologies are well-established in some use cases, such as workforce remote access, at least among large enterprises. Many information security and IAM leaders are evaluating

and implementing new authentication methods as a way of improving trust and accountability in all use cases, even if not explicitly demanded by regulations.

Most organizations still address individual use cases discretely. However, a more strategic approach, based on an open, flexible authentication architecture supporting multiple methods suited to different use cases, can readily be implemented.

Many organizations, especially small or midsize businesses, are still not using new, risk-appropriate user authentication methods where they clearly should be (for example, relying on legacy passwords for workforce remote access). But those organizations that have invested in risk-appropriate methods are increasingly finding problems in carrying those over to support user access from smartphones and tablets, owing to technical integration issues, degradation of user experience (UX) or erosion of the level of trust that the methods provide. However, momentum around mobile-apt user authentication methods is increasing, and progress toward the Plateau of Productivity is easing forward.

User Advice: In some lower-risk situations, legacy passwords might provide appropriate levels of trust and accountability, but they are vulnerable to many attacks and abuses. Thus, with the increased exposure of corporate systems to external users, more sophisticated threats and more determined intruders, the convenience of staying with passwords is increasingly outweighed by the risks. This is true, even when organizations adopt the "robust" password policies dictated by some regulations.

While the prospect of a single, high-trust authentication method for all users across all use cases may be initially attractive, it is usually overkill because most users have access to only low- or medium-risk systems, and it may be unnecessarily costly. An emerging best-practice architectural principle is "risk-appropriate authentication." An information security or IAM leader must consider multiple use cases and, for each, evaluate minimum levels of trust and accountability commensurate with the level of risk. However, this must be balanced with UX, total cost of ownership (TCO) and the technical constraints imposed by different kinds of endpoints and who owns them. Thus, implementing a well-defined range of authentication methods that balances needs better in each use case may be the most effective and efficient approach.

Information security and IAM leaders should be wary of relying on endpoint identification (for instance, using "device certificates") alone as a surrogate for a second factor in user authentication (see "Defining Authentication Strength Is Not as Easy as 1, 2, 3; Update"); nevertheless, endpoint identity can usefully be consumed as an element of contextual authentication. While contextual authentication can elevate trust, leaders should note that few regulations accept such methods as a robust alternative to a canonical authentication factor.

IAM and other leaders should also evaluate the benefits of adaptive ("risk-based") approaches that dynamically evaluate risks and can invoke step-up authentication using a higher-trust method to balance trust against risk at the moment of access. This approach can improve UX by minimizing the times when higher-trust authentication must be used (see "Technology Overview for Adaptive Access Control").

However, no authentication technology is infallible. Malware-based and other session-hijacking attacks can succeed, regardless of whatever levels of trust and accountability authentication methods provide. Thus, information security and IAM leaders must also invest in complementary safeguards, such as fraud detection and monitoring, transaction verification, and network access control. This multilayered approach is particularly appropriate for online consumer security, but will increasingly have value in B2B and B2E use cases, too.

Business Impact: User authentication technologies can provide a necessary level of trust in the identity of any user accessing corporate systems and data, as well as a proper level of accountability, by strengthening the bond between users and their online activities. Thus, they add considerable value to other security and compliance initiatives, such as improved access controls (including enforcement of segregation of duties), monitoring, reporting, analytics and identity governance. Risk-appropriate authentication not only reduces the risk of unauthorized access to regulated and other sensitive data, but also can significantly improve individual accountability — and thus, the forensic value of audit trails — in support of a variety of internal investigations. It also adds value to other identity-centric activity logs in change management, workflow in business processes, records and document management, and so on.

However, because even the strongest authentication method can be bypassed by session hijack attacks, the benefit rating is only moderate, not high. Monitoring and adaptive access control technologies, such as online fraud detection, can address these limitations.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Sample Vendors: Authentify; BioCatch; CA Technologies; Duo Security; EMC (RSA); Entrust; Gemalto; HID Global; IdentityX; SafeNet; SecurEnvoy; Symantec; Technology Nexus; TeleSign; Vasco Data Security International

Recommended Reading: "Magic Quadrant for User Authentication"

"How to Choose New User Authentication Methods"

"Use Gartner Authentication Method Evaluation Scorecards When Selecting a New User Authentication Solution"

"A Taxonomy of User Authentication Methods"

"Best Practices for Managing Passwords: End-User Policies Must Balance Risk, Compliance and Usability Needs, 2012 Update"

Enterprise Risk Management Consulting Services

Analysis By: Jacqueline Heng

Definition: Gartner defines enterprise risk management (ERM) consulting as a set of expert services designed to help enterprises reduce uncertainty and lessen its impact on business performance. ERM consulting supports and informs the creation of an enterprise's overall risk management strategy and provides a mechanism to ensure that important business processes and behaviors remain within the limits of the enterprise's overall appetite for risk, and adhere to relevant policies, procedures, laws and regulations.

Position and Adoption Speed Justification: ERM consulting represents a holistic treatment of all strategic, operational, financial reporting and legal/compliance risks, including their IT and information management components. ERM consulting services' position on the Hype Cycle is now moving up the Slope of Enlightenment. This market has moved forward as providers of risk consulting services take a lead in adjusting their methodologies to include a strategic enterprise that includes cyber risk and security perspective. This is helping clients to look beyond operational and control issues within their risk environments, and to anticipate risks at the strategic level. All these services put a strong emphasis on using technology to support integrated risk management solutions.

The primary factors influencing the adoption speed and positioning of ERM consulting services on the Hype Cycle are as follows:

- The proliferation of regulatory, compliance frameworks around finance, cyber risk, security, data protection and growing involvement in risk management at the CxO level
- The drive for more efficiency through enterprisewide automation and analytics
- The risks to the reputation of private- and public-sector enterprises created by social media

User Advice: The barriers to enter this market are low. As a result, the market contains many consultants, who are generating hype that tends to create confusion. In addition, consulting services are offered not only by the traditional business and finance consultants but also by a host of alternative providers, such as software vendors and legal firms. They offer attractive proposals in the form of enterprisewide risk management and compliance solutions and even outsourcing services. But not all these solutions are mature enough to support all the CIOs' or chief risk officers' (CROs') requirements to manage risk and compliance across the enterprise. Gartner believes that skilled resources are very important and should be backed by robust methodologies, a suitable depth of experience in relevant risk and compliance areas, and sound client references.

The provider of ERM consulting services should:

- Have made significant investments in refreshing and renewing the subject matter expertise of its consultants (with ongoing professional education, training and certification), and in establishing overall thought leadership in risk practices. "Opportunistic" providers do not make substantial investments in training or thought leadership in this space.
- Provide full-time risk and compliance professionals on its staff, who can discuss the nature of their specialties and provide the training and experience that underlie them.
- Offer risk advisory services from a separate business unit, or embed these risk advisory professionals into various vertical-market and business-line teams.

- Demonstrate the breadth of knowledge to support broader risk issues that are likely to arise. This should cover geographical aspects, such as a new factory in a new country, legislative amendments to existing compliance obligations, or court rulings that affect the legal relevance of one particular compliance issue.
- Demonstrate in-depth knowledge of the regulations and the parties that are driving and influencing the applications that support compliance. Examine your specific needs, so that you do not mistakenly replace advisory services with "off-the-shelf" solutions that are more appropriate for straightforward, well-defined compliance requirements.
- Demonstrate methodologies, frameworks and tools to deliver risk advice. Although you can expect a relatively high degree of customization from any advisory service, providers that are dedicated to this space will be able to point to a portfolio of frameworks, tools and knowledge management activities that underpin their efforts.
- Provide several client references of whom you can ask in-depth questions about the provider's capabilities, experience, quality of delivery and, most importantly, cultural fit.

Business Impact: In the latest World Economic Forum (WEF) Global Risk 2014, "digital disintegration" was identified as one of the three risk focuses, which includes the breakdown of critical infrastructure, cyberattacks and "data/fraud and theft." Security services in the past were centered on governing and managing information data. Now, security services move into the strategic business arena coupled with risk management and intelligence analysis to pre-empt or predict cyber breaches and data loss.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Accenture; Capgemini; Deloitte; EY; IBM Global Business Services; KPMG; Protiviti; PwC

Recommended Reading: "Emerging Service Analysis: Creating Opportunities With Managed GRC Services"

"MarketScope for Global Enterprise Risk Management Consulting Services"

"Introducing the ERM/GRC Blueprint for a Successful Risk Management and Compliance Program"

Content-Aware DLP for Email

Analysis By: Eric Ouellet

Definition: Content-aware data loss prevention (DLP) for email is considered a channel DLP deployment because this solution is focused on creating DLP policies for use only within an email system and not the entire enterprise. Outbound corporate email is scanned for corporate and

regulatory compliance and for preventing the dissemination of sensitive information without appropriate protection or controls.

Position and Adoption Speed Justification: Channel DLP solutions are differentiated from enterprise DLP and "DLP lite" offerings in that they are focused on the creation and use of DLP policies within an email system only, versus supporting additional protocols or platforms. Often, they are simply included by a vendor as part of the main email, email encryption or secure email gateway product offering. Effective solutions leverage industry-specific or regulatory lexicons, dictionaries and preformulated policies. Fingerprinting and partial and exact data-matching techniques may also be included in some content-aware DLP for email offerings to support intellectual property protection or to protect critical business content. However, they are typically provided in a reduced capability form when compared with stand-alone enterprise content-aware DLP solutions.

Flagged-message remedial actions, such as encrypt, block, delete, archive, quarantine and forward, as well as delegated workflow for flagged messages, are critical requirements of content-aware DLP for email offerings. Increasingly, automated encryption is a necessary component of any content-aware DLP for email strategy because sensitive content that is confidential or under regulatory compliance still needs to be sent to customers and partners as part of overall business processes.

Functionality varies widely among vendors, and email security software-as-a-service solutions often lack significant outbound filtering capabilities. Instead of concentrating only on email, some companies that have advanced DLP requirements, including discovery of sensitive information on file servers, network-attached storage/storage area network and document management systems, may consider deploying multichannel, advanced, enterprise-class, content-aware DLP solutions. Policies to protect sensitive data need to be applied to all email channels, including HTTP, especially for Web email utilities, such as Gmail, Hotmail, Yahoo mail and those within social networking tools. As mobile devices become more pervasive within the enterprise, rules designed to address the portability of information on these platforms will become increasingly important. The messaging group will be more involved in rolling out policies for Web-based email and will drive the convergence of email and Web.

User Advice: Develop a plan for managing compliance and leak prevention across all networks and communications media. Start small, with the high-impact and probable business risks first, and gradually expand as you gain confidence in using tools and procedures. Consider the use of enterprise-grade, content-aware DLP tools for complex data definitions, workflows and policies.

Business Impact: Businesses seeking to reduce the risk of unfettered dissemination of intellectual property, and to address corporate and government compliance requirements, must invest in content-aware DLP for email and encryption.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Sample Vendors: Cisco (IronPort Systems); McAfee; Microsoft; Proofpoint; RPost; Symantec; Trend Micro; Websense; ZixCorp

Recommended Reading: "Anticipate and Overcome the Five Key Obstacles to Success in Content-Aware DLP Deployments"

"Magic Quadrant for Content-Aware Data Loss Prevention"

"2013 Buyer's Guide to Content-Aware DLP"

"Guidelines for Selecting Content-Aware DLP Deployment Options: Enterprise, Channel or Lite"

"Magic Quadrant for Secure Email Gateways"

Entering the Plateau

SIEM

Analysis By: Kelly M. Kavanagh

Definition: Security information and event management (SIEM) technology supports threat detection and security incident response through the real-time collection and historical analysis of events from a wide variety of event and contextual data sources. It also delivers compliance reporting and incident investigation through analysis of historical data from these sources. The core capabilities of SIEM technology are a broad scope of event collection and the ability to correlate and analyze events across disparate sources.

Position and Adoption Speed Justification: The increase in targeted attacks has caused a growing number of organizations to use SIEM for threat management to improve security monitoring and early breach detection, in addition to meeting regulatory compliance reporting requirements. Large and midsize companies continue to deploy SIEM for monitoring perimeter security controls, with growing adoption of other use cases that include monitoring of servers, database management system applications and users. There is growing interest in outsourced or co-managed SIEM with a range of support options from external service providers.

Capabilities that support the threat monitoring use cases and aid in targeted attack detection include user activity monitoring, application activity monitoring, profiling and anomaly detection, use of threat intelligence feeds, and effective analytics. Adoption of SIEM technology by a broad set of companies has fostered demand for products that are easy to deploy and support, and provide predefined security monitoring and compliance reporting functions. Data access and user activity monitoring for early detection of targeted attacks and data breaches has emerged as the high-priority use case for SIEM technology. Several vendors are developing big data security analytics platforms and integrations that increase scale of and types of security analytics available from SIEM technologies.

User Advice: Security managers considering SIEM deployments should first define the requirements for log management, user and resource access monitoring, threat monitoring, security

incident response and workflow, and compliance reporting. This may require the inclusion of other groups in the requirements definition effort, such as audit/compliance, network operations, server administration, database administration and application support areas. Organizations should also estimate event rates, document their network and system deployment topology, and anticipate deployment growth and analytic requirements. SIEM vendors can use this data to propose a company-specific solution. Technology and service selection decisions should be driven by organization-specific requirements in areas such as the relative importance of real-time monitoring and analytics, integration with established system and application infrastructures, and the IT security organization's technology deployment and operations capabilities.

Business Impact: SIEM improves the IT security organization's ability to quickly detect targeted attacks and data breaches, and improves incident investigation and response. SIEM also supports the privileged-user- and resource-access-monitoring activities of the IT security organization and the reporting needs of the internal audit and compliance organizations.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: AccelOps; AlienVault; BlackStratus; EMC (RSA); EventTracker; HP (ArcSight); IBM; LogRhythm; McAfee; NetIQ; SolarWinds; Splunk; Tenable Network Security; Tibco Software; Trustwave

Recommended Reading: "Magic Quadrant for Security Information and Event Management"

"Critical Capabilities for Security Information and Event Management Technology"

"Planning for an SIEM Technology Deployment"

"How to Deploy SIEM Technology"

"Using SIEM for Targeted Attack Detection"

Virtual Data Rooms

Analysis By: Jay Heiser

Definition: A virtual data room (VDR) is a service integrating a variety of security and control mechanisms into one convenient package to create a trusted portal for sharing sensitive data externally. Features include encryption on the server, encryption of downloaded documents, rights management (control over print, paste and save; and the ability to remotely delete data stored on the endpoint) and strong authentication.

Position and Adoption Speed Justification: A data room is a physically secure facility that is most often used to provide document access to the parties of a financial deal review, typically in support of a merger or acquisition. The first attempts at putting thousands of pages online took place during

the 1990s, using scans of physical documents. Physical data rooms have been completely replaced by virtual ones, which means that the original and, currently, the largest market segment has reached saturation and entered the Plateau of Productivity. The need to externally share large amounts of proprietary data, such as research results and unpatented intellectual property, makes life science the second most significant VDR market. A growing number of small and lower-cost vendors, relying entirely on online sales models, have made trusted portals affordable for additional use cases, some of which probably still remain undiscovered. The potential for growth in new external collaboration use cases means a continuing potential for new customers, and existing customers will continue to find new ways to use this form of highly trusted collaborative system. The majority of VDR services are offered on a software as a service (SaaS) basis.

Several related product categories, including managed file transfer and enterprise file synchronization and sharing (EFSS) services, are increasingly overlapping the traditional functionality of VDRs. While these alternatives are less likely to impact the original financial department use cases for VDRs, services offering somewhat less control and security functionality, at a lower cost, are increasingly appealing for a wide variety of less-critical scenarios. Responding to this market pressure, and looking for new market opportunities, VDR vendors are beginning to target lower-priced, less-critical internal and external collaboration scenarios. The increasing levels of market overlap are indicative of growing levels of interest in high-end and, especially, midrange secure collaboration. This market evolution represents a growing and possibly accelerating number of secure collaboration seatholders and enterprise customers, but it is also blurring the distinction between different forms of collaboration systems.

User Advice: If you are looking for temporary or permanent mechanisms to support controlled sharing of highly sensitive data outside the enterprise, then consider a VDR.

Document, monitor and control all current uses of VDRs to ensure that you understand and address the risks. Trusted portals are most often purchased by the line of business, and as is often the case with SaaS, IT may be unaware that such a system is being used.

Not every trusted portal is equally useful in every situation. Look for a service that is already successfully supporting your intended use case. Evaluate potential and existing vendors on their ability to meet your primary needs, but also consider that your organization may have additional secure communications needs that could also be met by a VDR. Determine what form of integration you'll need between a VDR and your existing content management and creation systems, and ensure that the portal service and IT can support that integration.

Business Impact: Virtual "deal" rooms not only have proved themselves appropriate for the purposes of a wide range of financial transactions, but also have become essential. While the savings in travel and office space are important, the improvements in efficiency are even greater. The participants in a deal are able to remotely view the relevant data whenever they need it and wherever they happen to be, and they can search for it electronically instead of paging through printed documents. By logging who is accessing which document at a specific time, VDRs also play an important role in dispute resolution.

Outside the financial world, VDRs offer the potential to enable a huge variety of virtual enterprise activities that may otherwise be considered too risky. The life science industry has been most aggressive in exploring ways for these portals to be used to share sensitive data outside the enterprise, while still maintaining the control necessary to satisfy regulators and protect intellectual property. It's likely that a large number of use cases — especially outside the finance and life cycle vertical industries — remains to be discovered and profitably exploited.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Brainloop; EthosData; Firmex; Intralinks; Merrill; RR Donnelley; V-Rooms; WatchDox

Recommended Reading: "Magic Quadrant for Social Software in the Workplace"

"Enterprise File Synchronization and Sharing: Thinking Through the Security Issues"

"Emerging Technology Analysis: Mobile Application Shielding"

"Quick Reference Guide to Life Science Clinical Resource Management Solution Providers"

Enterprise GRC Platforms

Analysis By: French Caldwell

Definition: The enterprise governance, risk and compliance (EGRC) platform provides functionality for integrated GRC activities, such as risk management, audit management, policy and compliance management, regulatory change management, and key supporting functionality — for example, reporting, policy distribution and attestation, policy life cycle management, integration with business applications, continuous controls monitoring, and the ability to collect and aggregate automated controls information.

Position and Adoption Speed Justification: The primary purpose of the EGRC platform is to automate GRC management activities — that is, much of the work associated with the documentation and reporting of the compliance activities that are associated most closely with corporate governance and activities for enterprise risk management (ERM; see "Introducing the ERM/GRC Blueprint for a Successful Risk Management and Compliance Program"). Most EGRC platforms are mature for this primary purpose, but Gartner sees opportunities for the broader GRC marketplace to evolve in other areas, such as business performance management and analytics, not just compliance. The evolving regulatory environment is putting pressure on vendors to expand their capabilities.

In the 2012 and 2013 Gartner survey of EGRC platform users, respondents indicated that the use for risk management activities exceeded the use for compliance activities. Few organizations are still buying solely for compliance, and enterprise risk management (ERM) is now a major element of

their decision making. In the 2013 Gartner CEO and senior business executive survey, respondents reported that regulatory risks ranked second behind economic uncertainty as the top business risk they face (see "CEO and Senior Executive Survey 2013: CIOs Must Help Their Companies Adapt to Regulatory Risks and Business Uncertainty"). To keep up with an onslaught of new regulations, regulatory change management has become a significant driver of EGRC platform adoption. Business performance is an emerging driver as well. While many vendors are touting their abilities to integrate their mature EGRC platforms with performance management suites and big data analytics, Gartner has not yet seen any successful demonstration of full-scale integration. However, in the 2013 Gartner survey of EGRC platform users, 29% of them reported that they are using the platform in some way to support business performance; the most common integrated performance and risk management use cases were evaluating the risks to strategic business objectives, and mapping key risk indicators to key performance indicators.

User Advice: Carefully weigh all your regulatory requirements and industry standards to avoid procuring a platform simply for automating the compliance activities of only a small set of regulations:

- Consider using an EGRC platform to integrate controls over the general ledger and other business applications, business intelligence, enterprise content management, and continuous controls monitoring, but evaluate the specific integration issues with your in-house systems as part of your purchase decision.
- Despite vendor claims regarding EGRC platform functionality, organizations often are better off purchasing best-of-breed offerings to address specific requirements in finance, IT, legal and operations. When evaluating best-of-breed versus an EGRC platform, consider the following:
    - For organizations that are moving to an ERM strategy, the EGRC platform must support the roll-up of relevant risk and compliance information from a broad range of applications, including other point GRC solutions that may have been purchased by various entities; business applications; IT GRC; GRC solutions for environmental, health and safety; quality management; sustainability; and controls solutions for IT, finance and operations. Keep in mind that, in this scenario, consulting and implementation services will outweigh software costs, and a phased approach starting with the highest priority inputs can help to keep the initial costs down.
    - If the IT organization must perform IT asset risk assessments and/or tight integration of reporting from automated general computer controls, then an IT GRC solution also is appropriate (see "Technology Overview for IT GRC: Clarifying IT GRC to Match Technology to Need") and should be integrated into the EGRC platform.

Business Impact: Regulatory risks and greater awareness of other business performance risks worldwide are driving the high-profile business and IT activities of financial compliance, corporate governance and risk management. When organizations take a project-by-project approach to compliance and risk management, the costs are much higher than a programmatic approach. The first business benefit is to get all the various initiatives into a common application — a common system of record — instead of volumes of spreadsheets and Word documents that are difficult to manage and problematic in supporting an enterprisewide program.

The greater benefit is that a programmatic approach enables a reduction in the complexity supporting the ability to apply common controls objectives and risk management principles across multiple initiatives. The ideal is to enable a common set of compliance controls testing and risk assessments to support multiple reporting requirements. Although it is not possible to get to that perfect ideal, many organizations have reduced their compliance costs by 30% or more through reduction in complexity and redundancy. For ERM initiatives, improved business performance is still a stretch goal for many organizations.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: ACL; BWise; Chase Cooper; CMO; Covalent Software; Cura Technologies; C&F; Enablon; IBM; LogicManager; Mega; MetricStream; Oracle; ProcessUnity; Protiviti; Resolver; RSA The Security Division of EMC; SAI Global; SAP; SAS; Software AG; Sword Group; Thomson Reuters

Recommended Reading: "A Comparison Model for the GRC Marketplace, 2011 to 2013"

"Magic Quadrant for Enterprise Governance, Risk and Compliance Platforms"

"Introducing the ERM/GRC Blueprint for a Successful Risk Management and Compliance Program"

"Technology Overview for IT GRC: Clarifying IT GRC to Match Technology to Need"

SOD Controls Monitoring

Analysis By: Brian Iverson; Anmol Singh

Definition: Separation (or segregation) of duties (SOD) controls monitoring tools help detect and remediate conflicting entitlements within transactional systems like ERP, financial planning, and electronic medical record and health record applications. Tools in this category provide basic risk analysis, along with some of the following features:

- Role design and management
- Access certification for role assignments
- Compliant provisioning (access requests and workflows)
- Emergency privileged access
- Transaction monitoring for exceptional access

Position and Adoption Speed Justification: The market for SOD controls monitoring experienced slow but steady growth over the past 12 months, based on a continued need in organizations to address related audit findings and auditor concerns based on compliance requirements. The ability to support multiple applications and detect conflicts (that is, the ability to create a vendor record in

one ERP instance and pay that same vendor in another instance) has grown in importance and is now supported by most vendors.

Auditors and audit findings continue to drive client need. Many organizations start to address SOD control requirements through homegrown processes driven by spreadsheets or consultants, but such processes can be expensive and difficult to sustain. The move to SOD controls monitoring tools usually is driven by a need to manage costs and provide more-comprehensive control over the SOD and access policy.

User Advice: For larger organizations, manual analysis and removal of SOD conflicts will be costly and will not prevent SOD violations from being introduced. Purchasing an automated tool alone won't solve what is fundamentally a process problem.

While automated SOD controls monitoring has business benefits to reduce risk with less effort, few organizations engage in SOD projects without auditor pressure. Gartner recommends auditor engagement as early as possible to confirm that the chosen solution will meet compliance requirements for SOD analysis.

Start by designing a process to eliminate SOD conflicts in critical enterprise applications, beginning with financial transactions. Then evaluate the tools that help to automate the process, and make it more scalable and consistent (see "Enhance Monitoring of SOD Controls for Applications With Complex, Role-Based Authorization Models"). Smaller enterprises may continue to use manual processes and tools. However, the pricing of third-party point solutions can be quite competitive, so evaluate the cost-benefit of continuing to perform SOD controls monitoring manually.

Business Impact: Investments are typically made to address a specific control deficiency identified by an external audit, and regulatory compliance remains the major driver of investments in this area. In the longer term, SOD conflict detection and remediation should become part of a broader IT governance, risk and compliance framework and strategy. Automated SOD controls monitoring should be integrated into the automated provisioning of users and roles within identity governance and administration systems, reducing the cost of future audits and remediation efforts.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Sample Vendors: ControlPanelGRC; CSI tools; ERP Maestro; Fastpath; Greenlight Technologies; Infor; Oracle; SAP; Security Weaver; wikima4

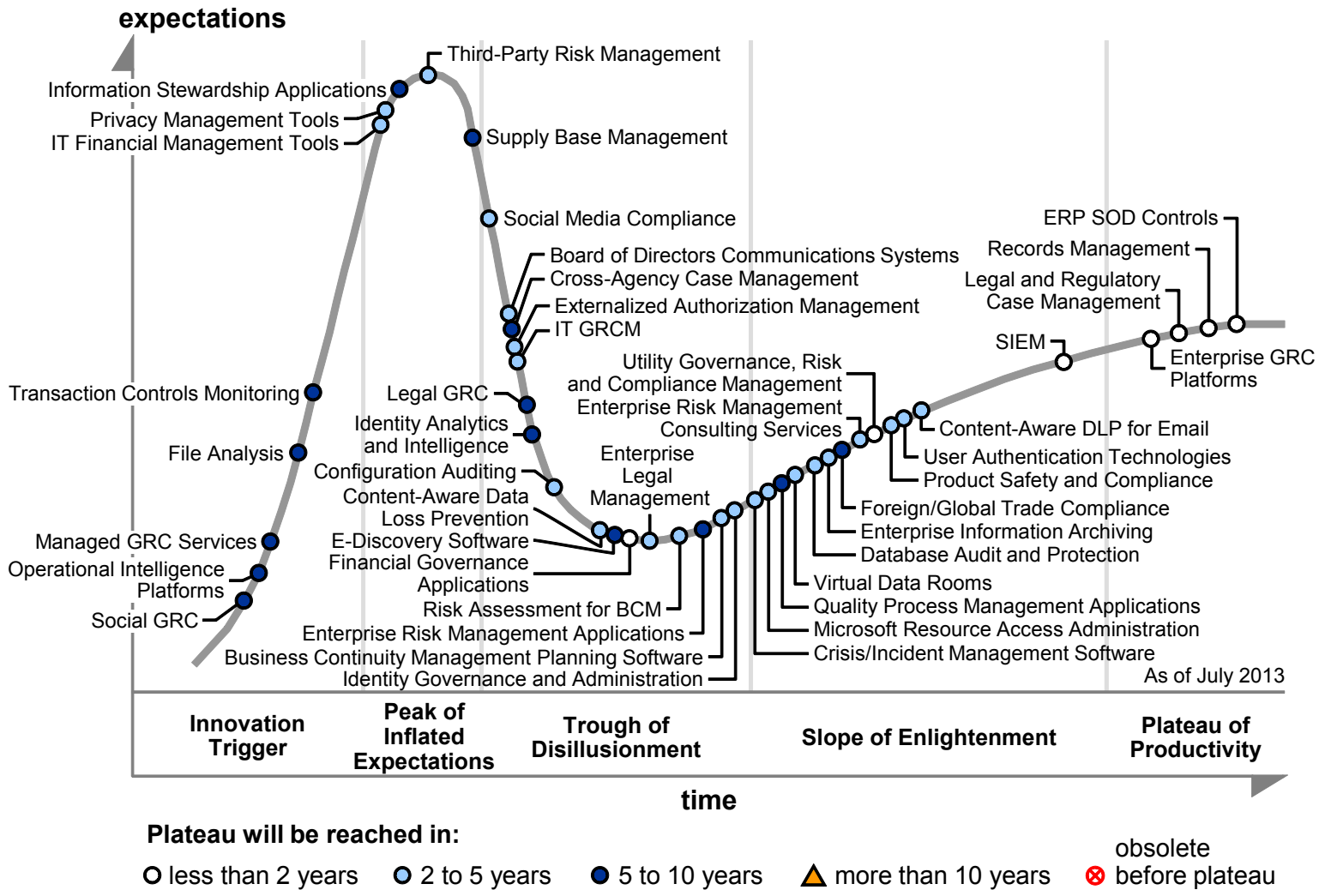
Recommended Reading: "MarketScope for Segregation of Duty Controls Within ERP and Financial Applications"

"Automate Segregation of Duties in ERP to Reduce Compliance Costs"

"Enhance Monitoring of SOD Controls for Applications With Complex, Role-Based Authorization Models"

Appendixes

Figure 3. Hype Cycle for Governance, Risk and Compliance Technologies, 2013



Source: Gartner (July 2013)

Hype Cycle Phases, Benefit Ratings and Maturity Levels

Table 1. Hype Cycle Phases

Phase	Definition
Innovation Trigger	A breakthrough, public demonstration, product launch or other event generates significant press 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 technology is pushed to its limits. The only enterprises making money are conference organizers and magazine publishers.
Trough of Disillusionment	Because the technology 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 technology'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 technology 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 technology to reach the Plateau of Productivity.

Source: Gartner (July 2014)

Table 2. 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 2014)

Table 3. Maturity Levels

Maturity Level	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 2014)

Gartner Recommended Reading

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

"Understanding Gartner's Hype Cycles"

"The 2014 Gartner CEO and Senior Executive Survey: 'Risk-On' Attitudes Will Accelerate Digital Business"

"How to Use Pace Layering to Build a GRC Application Strategy"

"Predicts 2014: Advances in Risk Management Technology Will Improve Corporate Performance and Public Policy"

"Definition: Governance, Risk and Compliance"

More on This Topic

This is part of an in-depth collection of research. See the collection:

- Gartner's Hype Cycle Special Report for 2014

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