Gartner

Research

Publication Date: 16 July 2008 **ID Number: G00157816**

Hype Cycle for Governance, Risk and Compliance Technologies, 2008

Jay Heiser, Earl Perkins, Roberta J. Witty, Bradley Williams, Dan Miklovic, Richard J. De Lotto, Jeff Vining, John E. Van Decker, Ronni J. Colville, Mark Nicolett, Les Stevens, Douglas McKibben, David Furlonger, French Caldwell, Paul E. Proctor, Kenneth Chin, Debra Logan, Eric Ouellet, Jeffrey Wheatman, Carolyn DiCenzo, Neil MacDonald, John Bace, Rita E. Knox, Kristen Noakes-Fry, Ant Allan, Tom Eid, Gregg Kreizman, Carsten Casper, Kris Brittain, Sharon McNee

Although regulatory compliance continues to be a "hot button" issue for product sales, organizations are looking for solutions that can help them better manage multiple forms of risk.

TABLE OF CONTENTS

Gartner

LIST OF TABLES

LIST OF FIGURES

What You Need to Know

As corporations, government agencies and nonprofit organizations develop increasingly integrated and effective approaches to the overall management of risk, technology suppliers are repositioning themselves to meet evolving customer expectations. In some cases, this is merely a superficial change in the marketing message; however, it often means that buyers and sellers are converging on a realistic and useful understanding of the benefits of these products.

Many corporate roles can benefit from the products highlighted in this research. The products are relevant to IT risk managers, IT operations managers and those responsible for maintaining the configuration and integrity of the organizational information infrastructure. Although IT organizations must carefully govern their own activities, their greater contribution should be toward the management of risk at the enterprise level, providing and maintaining a growing variety of governance, risk and compliance (GRC) tools for use by strategic and operational business managers.

The Hype Cycle

In 2006 and 2007, this Hype Cycle was called "Compliance Technology." This year, we've renamed it. Although the umbrella term "GRC" is somewhat ambiguous (and more than a little overhyped), we're using it not only because the market identifies itself as such, but also because it provides a useful and holistic perspective.

During the past five years, corporations and government agencies have been concerned about meeting regulatory requirements, as well as the need to demonstrate that the requirements have been met. This has resulted in a huge — and arguably counterproductive — preoccupation with regulatory compliance. Corporate concerns about the negative effects of failed audits, as well as the potential for fines and negative publicity, were exploited by significant changes in product positioning, with thousands of software and service providers claiming that their offerings were not only beneficial, but mandatory for meeting regulatory requirements. Gartner has always maintained that "it is all about risk," and that the potential downside of not complying with a law is just one more risk that corporations need to consider, along with all the other risks confronting an organization.

Whether the acronym GRC remains a common umbrella designation or is supplanted remains to be seen, but, for the near future, it represents a useful conception of the nature of the problem that many products address. Essentially, the term is a more-abstract expression of what was meant to be described by "compliance management" or "risk management" — narrower terms that may have been adequate to describe the functionality of a particular automation product, but almost certainly did not address the overall corporate goal.

Governance is a popular term that most literally means "exercising authority." In practice, it's difficult to differentiate from the more mundane term "management." Governance is understood as referring to the quality of management, and it carries with it connotations of "appropriateness." However, it's defined, good governance is becoming a corporate imperative.

For organizations with relatively immature risk management infrastructures, taking an increasingly holistic and proactive approach to IT risk management provides relatively large benefits that far outweigh the cost of effort. However, only a limited number of risk events can be prevented or controlled, which suggests that an approach focused solely on preventing negative occurrences will eventually reach a point where further improvements are impractical. The logical evolution of

risk management is to apply the information gathered and governance processes in place to improve performance. Once this trend becomes recognized, the term "GRC" will become obsolete.

Point Products vs. Suites

Many of the product categories in this Hype Cycle continue to evolve as point products, while others morph into suites. Point products typically become incorporated into suites or evolve into platforms that can perform the tasks formerly handled by point solutions. The desire to break down risk management silos and provide a more-holistic view of risk across the enterprise is encouraging such transitions in many of the categories profiled in this Hype Cycle.

Specific Changes to This Year's Hype Cycle

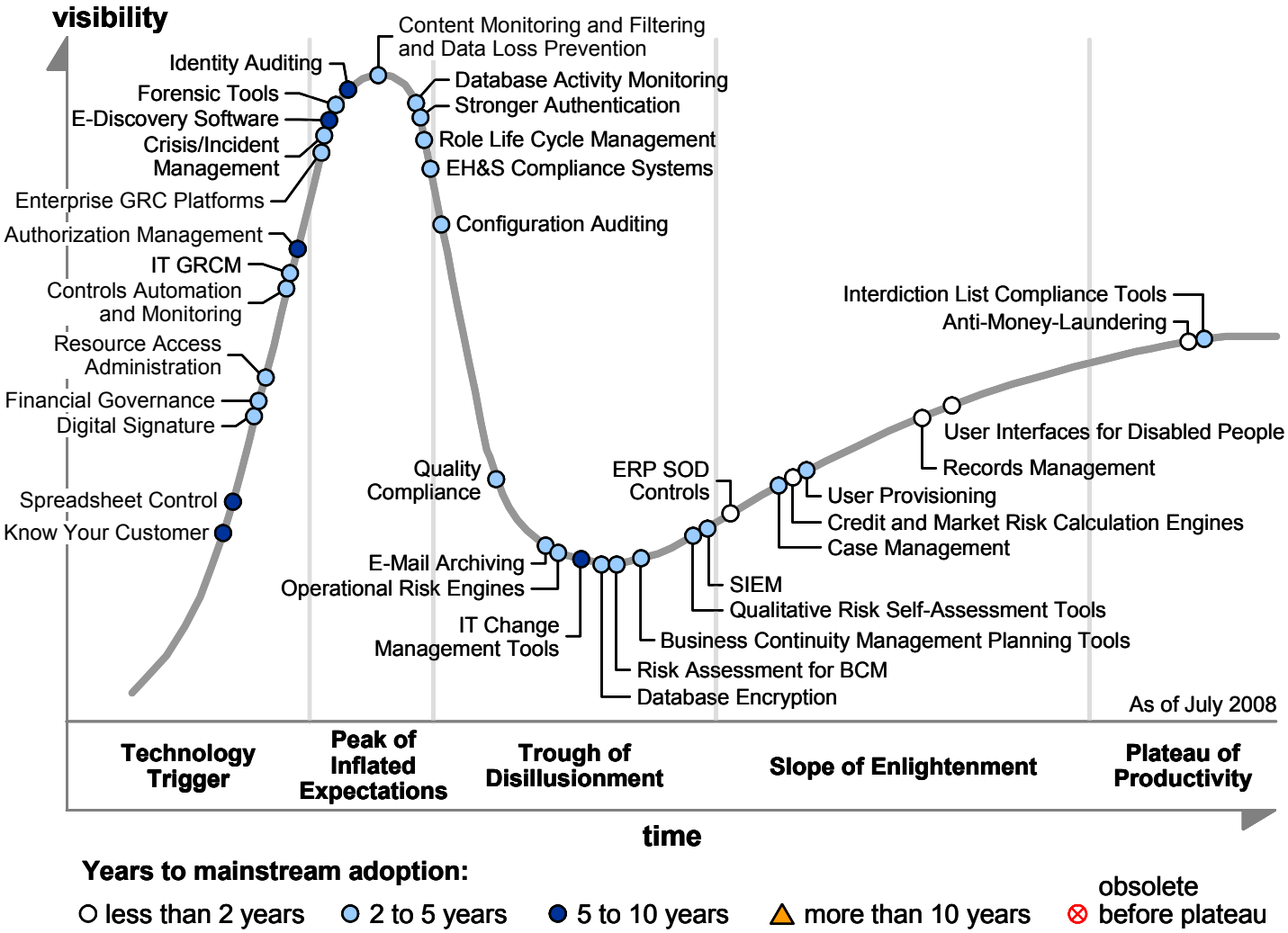
This third annual GRC Hype Cycle continues to see refinement in product categories. In comparison with other Hype Cycles, this one incorporates a relatively broad mix of product types. It emphasizes recognizable market categories, avoiding functional descriptions that don't readily map to discrete product types.

In addition to the name change, several technologies appearing in previous Hype Cycles have been renamed and repositioned on 2008's GRC Hype Cycle. CPM and Financial Controls have been renamed Financial Governance, a term being widely used in the market. Role Life Cycle Management is the new term for Role Management for Enterprises, which is no longer descriptive enough to include the recognition that multiple processes must be performed across the complete role life cycle. Cloud providers and other organizations that may not be considered enterprises also have role management issues, but were excluded by the old term. The product space referred to as Finance GRC Management has been renamed Enterprise GRC Platforms, reflecting the rapid evolution of this market, and the processes being automated with it by a growing number of corporate roles.

Several technologies have been added to this year's Hype Cycle. Environmental, Health and Safety (EH&S) Compliance Systems and Interdiction List Compliance Tools have been added to ensure that the Hype Cycle contains as comprehensive a list as possible of software being used for GRC tasks. Database Activity Monitoring is one of several forms of behavioral control that are increasingly being applied in the name of regulation. In recognition of the foundational role played by identity and access management (IAM), two new IAM technology profiles have been added to this year's Hype Cycle: Authorization Management and Resource Access Administration.

Know Your Customer (KYC) products, which are intended for use by financial service firms, represent a relatively new category of software that's related to interdiction list products. Although the latter is only used for compliance purposes, the newer category addresses a broader set of external relationships, including customers, partners and stockholders. KYC products are intended to address a larger number of potential risks, as well as offer the potential for performance improvements.

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



Source: Gartner (July 2008)

Gartner

The Priority Matrix

The technologies profiled represent categories that have demonstrated their usefulness in controlling IT risk and supporting a regulatory response effort. They differ in tactical and strategic significance.

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

benefit	years to mainstream adoption			
	less than 2 years	2 to 5 years	5 to 10 years	more than 10 years
transformational		**Operational Risk Engines**		
high	**Anti-Money-Laundering** **Credit and Market Risk Calculation Engines**	Controls Automation and Monitoring Crisis/Incident Management Financial Governance Qualitative Risk Self-Assessment Tools Risk Assessment for BCM Role Life Cycle Management User Provisioning	E-Discovery Software E-Mail Archiving Identity Auditing IT Change Management Tools	
moderate	ERP SOD Controls Records Management	Business Continuity Management Planning Tools Case Management Configuration Auditing Content Monitoring and Filtering and Data Loss Prevention Database Activity Monitoring Database Encryption Digital Signature EH&S Compliance Systems Enterprise GRC Platforms Forensic Tools Interdiction List Compliance Tools IT GRCM Quality Compliance Resource Access Administration SIEM Stronger Authentication	Authorization Management Know Your Customer Spreadsheet Control	
low	User Interfaces for Disabled People			

As of July 2008

Source: Gartner (July 2008)

Off the Hype Cycle

All the categories used for last year's Compliance Technology Hype Cycle can be found on the 2008 Hype Cycle for Governance, Risk and Compliance Technologies.

On the Rise

Know Your Customer

Analysis By: Richard DeLotto

Definition: KYC tools are a broad variety of products designed to help companies avoid initiating or maintaining commercial relationships with parties that are regulatory-inappropriate or otherwise undesirable. These tools facilitate the tracking of all parties that are potentially higher-than-acceptable risk, but are primarily applied in identifying and tracking those that might be interdicted by government regulatory agencies. While interdiction lists are freely available from the governments issuing them, in most instances they require extensive augmentation (ranging from simple spell checking through appending all known data) to be reliably usable.

Position and Adoption Speed Justification: Hype in this niche is driven by the spreading need to reduce both regulatory and reputation risk. KYC tools have already been widely proven in the financial services industry, but are now being deployed across a broad spectrum of companies where they had previously been unknown or underutilized. Hype for the tools rises and falls in particular industries based on how recent — and vivid, the stakeholder or customer's problem was. Speed to plateau is based on an increased lack of tolerance for reputation risk — demonstrated by the rise of corporate social responsibility (CSR). Examples of technologies and services include:

- Interdiction list screening of some sort is mandatory for most companies worldwide, though where and how it is done varies widely. Adoption is near universal in financial services. Current matching systems are adequate for all but the most sophisticated needs. Users are, however, likely to switch to find lower prices for lists and services, or incremental improvements in performance.
- "Heightened risk entity" data providers.
- Third-party certification for sensitive, CSR and CSR-like factors.

User Advice: Clients should keep their matching tools updated to take advantage of improving technology, adopt all available interdiction and heightened risk entity lists ("required" or not), and process all stakeholders through them as a general risk reduction procedure.

Business Impact: Aggressive use of KYC tools will enable firms to efficiently avoid risk and price correctly for it.

Benefit Rating: Moderate

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Sample Vendors: ChoicePoint; Experian; Factiva; World-Check

Spreadsheet Control

Analysis By: David Furlonger; Jay Heiser

Definition: Spreadsheet control is stand-alone software that provides additional controls over the use of spreadsheets without breaking backward compatibility with Excel. All products in this category improve process documentation by providing more-robust change tracking than native Excel. Most products also provide some unique mix of additional functionality, such as workflow, multiuser access to server-based spreadsheets, user roles and granular permissions, or output validation. Increasingly, products in this space also include functionality to locate spreadsheets and even analyze their content, providing reports that can help identify which ones are most important. Vendors are also improving their level of support for other user-developed application (UDA) platforms, such as Microsoft Access.

Position and Adoption Speed Justification: Numerous high-impact losses, both accidental and fraud-related, have occurred because spreadsheets lack the control mechanisms that are taken for granted in enterprise applications. Despite the wide use of business intelligence applications as a reporting front end to enterprise resource planning systems, their tremendous flexibility means that spreadsheets are virtually always on the critical path toward financial reporting. A growing number of companies, currently at least a dozen, offer products intended to reduce the risks associated with the use of spreadsheets. However, the sense of urgency associated with the control of spreadsheets is still relatively low, and neither IT nor spreadsheet users are widely aware of the potential benefits of these control products. Their use is most prevalent in the pharmaceutical and financial services industries, where U.S. Food and Drug Administration requirements for document validation have forced virtually all laboratories to implement additional Excel controls and where financial services providers are facing increased scrutiny over operational risk and compliance requirements — for example, for the Sarbanes-Oxley Act (SOX). Most publicly held companies are managing user-developed application risk through simple policies on manual workflow and approval. However, auditors are becoming more aggressive in identifying financially material spreadsheets as being highly relevant to SOX. In the U.K., the Financial Services Authority, along with the tax authorities, is putting more pressure on corporations to better manage the risks associated with UDAs. As a result, the expectation that companies should implement more-stringent controls over UDAs is growing slowly but steadily.

User Advice: To ensure that risk is kept within acceptable limits, all midsize and large organizations should develop a written strategy for the use of UDAs. In today's regulatory environment, undocumented ad hoc applications are no longer acceptable, so at a minimum, controls should include processes to identify, track and audit the use of spreadsheets supporting high-risk and regulated activities. If the analysis indicates that uncontrolled spreadsheets represent an unacceptably high level of risk, then some use of third-party compliance products should be part of the overall strategy. Organizations that have not yet started tracking their use of UDAs should also evaluate products that locate them, and analyze links and content. Because these products maintain backward compatibility with Excel, vendor lock-in and product obsolescence are not concerns. Financial institutions and enterprises should note that, while these spreadsheet control products help in "activity tracking" (for example, who changed a spreadsheet and when), most of these products lack the functionality to analyze quality of input data within the spreadsheet. It must be recognized that governance of spreadsheets (or any data) isn't just about what it is, where it is and who touches it. Good governance also requires understanding the need for specifying and maintaining the necessary level of data quality.

Business Impact: Spreadsheet control products are commonly used to aid in tracking, auditing and reporting data that directly impacts the financial statements of the firm. In many cases, this includes the ancillary benefit of improving the efficiency of process in managing large, user-defined sets of information that would otherwise be isolated to individual employee environments. In the U.S. and, increasingly, in other countries, products to supplement Excel have become virtually mandatory in the pharmaceutical and financial services industries. Several years of lessons learned in adding rigor to the reporting of laboratory results can now be productively applied to the creation of controls over financial reporting. Spreadsheet controls are also highly

desirable for operational uses of spreadsheets that involve high-value transactions, such as derivative trading, which typically relies heavily on Excel. In all cases, change tracking can be performed with virtually no negative impact on the spreadsheet user, although it may also be necessary to apply workflow or access controls that would reduce user flexibility. However, supplemental technical controls for UDAs have significant potential to prevent multimillion-dollar losses, providing a high level of protection at a relatively low cost.

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: Cimcon Software; ClusterSeven; Compassoft; Finsbury Solutions; Prodiance

Recommended Reading: "MarketScope for Spreadsheet Control Products, 2008"

"Bank Controls Runaway Use of Microsoft Excel, Improves Risk Management"

"Developing a Strategy to Control Spreadsheets"

"Recognize the Risks of Uncontrolled Spreadsheets"

Digital Signature

Analysis By: Gregg Kreizman; Carsten Casper; Kristen Noakes-Fry

Definition: Digital signature is a specific type of electronic signature (e-signature) that relies on public-key cryptography to support identity authentication and provide record integrity through a pair of mathematically related keys — the public key and the private key. It is used toward a goal of providing irrefutable evidence that a specific digital object originated with a specific individual and has not been altered.

Position and Adoption Speed Justification: Digital signature has been widely anticipated for more than 10 years, but the level of effort to implement a digital signature infrastructure has usually exceeded the benefit. Early projects with e-signature made use of public-key infrastructure (PKI), and involved the private-key (the signing key) generation and placement on users' workstations or on smart tokens. Adding smart tokens improved protection for the private keys but also drove up costs. Many simple commercial e-signature processes avoid the use of digital signature technology. A number of U.S. regulations theoretically indicate a need, or at least an option, for some form of digital signature. Only a few of these regulations, such as the Food and Drug Administration (FDA) 21 Code of Federal Regulations (21 CFR Part 11), have led to a change in corporate practices, and those involve only small numbers of people.

The European Union (EU) Directive 1999/93/EC on e-signature has been in force since 2000, but has not brought the intended uptake due to diverging interpretations of the directive and inconsistent guidance on technical standards from the EU. This has caused differences in national legislation and implementations, such as leading to rather strong technical solutions in Germany and a comparatively pragmatic approach in Italy. This confines investments to national markets, making them even less profitable. In parallel to smart cards issued by banks but not being used for digital signatures, some EU countries such as Belgium and Estonia have started to issue electronic identity cards that also contain keys for use in digital signature applications, but application demand remains low. High-value transactions of citizens occur rarely (buying a house, renewing a passport) and usually justify the effort of a physical presence for a signature, whereas low-value transactions (buying books, filing taxes), which citizens prefer to conduct online, do not justify the cost of a digital signature infrastructure. Auditable business records such as invoices

are used by commercial organizations to substantiate their tax returns. EU tax authorities are increasingly concerned that some commercial organizations using electronic invoices will commit tax fraud by manipulating those business records after the fact. Because of these concerns and because business-to-business (B2B) and government-to-business (G2B) invoice applications don't require widespread distribution and management of certificates and private keys on consumer end-point machines, digital signatures will likely and increasingly be used for e-invoice applications to provide record integrity and support transaction non-repudiation.

Overall, the number of pilot projects continues to increase slowly, yet the feasibility of supporting personal signature keys on a widespread consumer use-case basis remains to be proved. Internal enterprise use cases for digital signatures are growing when smart cards or common access cards are being deployed (see the Smart Token and Common Access Card profiles/sections in the Identity and Access Management Hype Cycle).

User Advice: Because the signature is based on a protected private key known only to the user, the primary risk to a digital signature is the compromise of the private key. Thus, maintaining the security of the key should be an essential concern for companies considering this signature solution. Enterprises interested in experimenting with digital signature should look to the EU countries that are providing citizen smart cards and promulgating the use of compliant applications. Tax authorities and e-invoicing applications will also provide proving grounds for digital signatures.

Most benefits attributed to any form of e-signature are really a result of automating a business process, and the signature is a small but important step in the process. When the signature is automated as part of the process, it's important to consider whether you need the same degree of security as you had with "wet" signatures or if you need a much-higher level of security. Many organizations — when the primary motivation is to reduce the expense and delay of obtaining wet signatures for a transaction — may conclude that a cryptographic-based digital signature is not necessary.

Other less-expensive methods of e-signature, such as using a user ID and password, as well as acknowledging a text prompt, may suffice — particularly in applications that require a signature but have low-impact consequences of fraud or repudiation.

Business Impact: E-signatures, including digital signatures, add efficiencies to formerly paper-based processes, enabling them to be put online for B2B and business-to-consumer (B2C), as well as e-government applications. Cryptographic-based digital signatures add the assurance of making the signature and the document in which it is embedded virtually tamper-proof — enabling organizations to comply with a higher level of security requirements.

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Sample Vendors: Adobe; Algorithmic Research; CIC; Entrust; Gemalto; Giesecke & Devrient; Oberthur Card Systems; OpenTrust; Silanis Technology; VeriSign; Verizon; XYZMO

Recommended Reading: "Electronic Signature Suites and Services Mature"

"A Quick Look at E-Signature Vendors and Products"

"Tutorial: Understanding Electronic and Digital Signatures"

"Case Study: Loan Company Uses E-Signatures to Cut Costs and Save Time"

"IBM-Led Team to Create E-Forms Solution for U.S. Army"

"Time's Running Out to Prove the Value of Government PKI"

"No 'Big Bang': HSPD 12 Smart-Card Implementations Will Be Evolutionary"

Financial Governance

Analysis By: John Van Decker

Definition: Financial governance offerings will be targeted directly to the needs of the CFO and finance function. We define the components of a broad financial governance solution as:

- Financial consolidation: Typically found in corporate performance management (CPM) suites, these applications enable organizations to reconcile, consolidate, summarize and aggregate financial data based on different accounting standards and federal regulations across multiple legal entities. They also provide reporting tools to support the production of financial statements that represent the overall financial performance of the organization.
- Intercompany transaction management: This provides acceptance, rejection and reconciliation of intercompany transactions, ideally at the transaction level (as opposed to the overall account balance level).
- Reconciliation management: Numerous accounts in the trial balance need to be reconciled during the financial close process, as well as during predetermined periods throughout the month.
- Financial controls and compliance: This covers solutions intended to document the organization's Committee of Sponsoring Organizations (COSO) control response to specific financial compliance process initiatives, such as the Sarbanes-Oxley Act. Many of these control-monitoring solutions are rooted in auditing applications and have been refocused to provide continuous control monitoring by comparing information as it moves through various financial processes.
- Financial close management ("the last mile of finance"): Many activities that are part of the financial close need to be managed and automated. Although ERP and financial consolidation systems can manage these processes through their workflow and reporting capabilities, the delivered functionality usually is limited and requires users to build the required capabilities by using the vendor's tools.
- Access and segregation of duties controls: These controls typically are found in ERP solutions, but may need to be augmented with additional security controls to ensure that appropriate security measures are in place.
- Financial risk management: This refers to solutions that project an organization's tolerance for financial risk, given a series of parameters. This area is not currently well-served, but we anticipate solutions during the next three to five years.
- Financial analytics: These solutions are used to understand in-period, as well as period-to-period, analysis of financial information. This includes drill-down into transactional data to understand varying results. Unlike CPM, financial analytics is concerned with detailed analysis primarily of in-process measurements, although it also can be used to augment CPM reporting.

Position and Adoption Speed Justification: Financial governance is a new market that will mature during the next three to five years, combining elements of ERP, financial governance, risk and compliance management (GRCM), and CPM suites. It will build additional process controls around financial consolidation to support financial close processes and the production of periodic financial statements for regulators. It will augment the compliance controls in financial GRCM solutions with broader controls that monitor capabilities, When delivered as a comprehensive solution, it will enable CFOs to better manage financial risk. While financial governance solutions mature, a variety of point solutions will emerge, challenging CFOs who have to address pressing governance issues.

User Advice: Although users may have to wait for vendors to bring integrated financial governance suites 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 are overwhelmed with manual processes. Where there is a tactical need for a point solution, users should not defer evaluations. Instead, they should evaluate the appropriate point solutions. However, they should view such evaluations in two ways: First, the investment should be considered on a five-year basis, the time frame in which more-comprehensive financial governance solutions will become available. Second, users should give preference to point solutions from CPM, ERP or finance, and audit GRCM vendors with whom they 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 (BI) and CPM vendors.

Business Impact: The typical enterprise response to compliance initiatives, such as Sarbanes-Oxley, was to add more manual controls to system processes while the technology investment went to security and other IT initiatives. The biggest investment made in the finance area for compliance has been in the proliferation of Microsoft Excel in the financial organization. To avoid material weaknesses during audits, companies built up an arsenal of Excel solutions in addition to ancillary manual processes to document and prove financial controls. Many companies continue to report material weaknesses and significant deficiencies in internal controls.

Many CFOs wrestle with the issue of improving governance of financial processes. To improve governance, they have to deploy and integrate disparate applications, usually from different vendors. These typically include elements of the ERP systems, CPM suites, and finance and audit GRCM products that address specific tactical needs, but do not provide an overall optimal solution. Gartner originally anticipated that CPM suite vendors would extend their financial consolidation systems to address this need; however, this has not happened because compliance is less of a driver for CPM suite purchases, and CPM vendors are more focused on providing broader performance management solutions, often integrating their applications with BI platforms. Consequently, we anticipate that a new market will emerge during the next three to five years to address financial governance in a comprehensive manner.

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: Oracle; SAP; Trintech

Recommended Reading: "Q&A on Financial Governance Market Trends"

"Financial Governance Will Emerge to Enhance Financial Controls and Regulatory Reporting"

Resource Access Administration

Analysis By: Earl Perkins

Definition: Resource access administration manages access by IT resource (that is, for a particular resource, who has access to it), whereas user-provisioning solutions manage access to IT resources by user (that is, who has access to the resources). Resource access administration products (or the features of some user-provisioning products) manage IT resources in two ways:

- They administer and report on IT resources and the users who have access to each.
- They provide users a view of only the resources to which they have access.

Some user-provisioning products create and administer roles/groups at the target system level or explicitly assign privileges (for example, read, write and delete) to a user outside the role/group structure. Most user-provisioning products provision users only to roles/groups in a supported system. Microsoft-centric platforms are especially problematic, given the number of folders, files, printers and other system objects that are shared among groups of end users and require management.

Position and Adoption Speed Justification: Microsoft Windows is the dominant platform for server infrastructure roles. Management needs are complex, and Microsoft does not yet provide this natively in Windows; therefore, Microsoft partners and other unaffiliated vendors provide this capability. Obstacles for these vendors include:

- Integration with heterogeneous user-provisioning products, because many products are Windows-centric
- Coordination with Microsoft so that the products are well-integrated with Windows infrastructures, including Active Directory, Systems Management Server, Microsoft System Center Operations Manager
- Seeking and obtaining Microsoft's endorsement of the solution
- Storage vendor coordination for product alignment

User Advice: Consider resource access administration products when you need to:

- Manage resources in a delegated model; that is, allow the end user or branch or store manager to manage resources specific to them
- Audit or report on object ownership (or access) from a group or end-user perspective
- Have a restricted view of network-available resources
- Use identity-auditing products for reporting needs by resource

Business Impact: Resource access administration products benefit any organization that must manage Microsoft groups or that wants to leverage its user-provisioning tool to create and manage roles and groups on supported IT target systems.

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: Aveksa; Beta Systems; BMC Software; Brocade; Hitachi; nCipher; NetIQ; Quest Software; SailPoint; UpperVision

Recommended Reading: "Magic Quadrant for User Provisioning, 2H07"

"Identity and Access Management Technologies Defined, 2008"

Controls Automation and Monitoring

Analysis By: French Caldwell; Paul Proctor

Definition: Controls automation and monitoring tools act proactively to implement controls through business rules or reactively to monitor controls through analysis of processes, transactions and events. Controls automation and monitoring can take many forms and operate at several levels of the enterprise architecture. At the infrastructure level, controls automation and monitoring focuses on configuration management and network access. At the system level, it focuses on identification and access. At the application level, it focuses on segregation of duties and, most recently, on rules governing transactions and behavior.

Position and Adoption Speed Justification: There is a high demand to reduce the amount of labor associated with compliance. These tools automate process controls and their monitoring, particularly as related to financial processes, and as related to automation of the analysis of the proper functioning of IT general computer controls.

Enterprises that have implemented Sarbanes-Oxley or SOX-like requirements, whether in response to regulations or as a self-directed initiative, will adopt controls automation and monitoring as a means to improve the reliability of controls and to lower audit costs. For enterprises that must report to the U.S. Securities and Exchange Commission, changes made by the Public Company Accounting Oversight Board in mid-2007 in the SOX internal controls audit standard AS5 strongly encourage controls automation and will accelerate investment to reduce audit costs.

User Advice: One of the more-common solutions for controls automation and monitoring that enterprises acquire is ERP transaction monitoring for segregation of duties violations. Additionally, there are tools called "continuous controls monitoring" that perform analysis of financial transactions and monitor for patterns of behavior. Business rule engines (BREs) are also used to automate controls, especially when business process management is implemented to standardize and automate critical regulated processes. Other controls automation and monitoring tools analyze changes to configurations, and still others analyze content on the network or on the client as it is created. Consider any of these various categories of tools when there can be considerable savings in labor from automation or improved reliability from continuous monitoring. While many of these tools are represented by other points on this Hype Cycle (for example, separation of duties, content monitoring and filtering, and security information and event management), many are best represented by the description of the business rule engine on the business process management Hype Cycle.

Business Impact: Controls automation and monitoring improve the reliability of controls and potentially reduce the cost of compliance by reducing the labor component of compliance activities. As enterprises automate and standardize more regulated processes, the application of controls automation and monitoring will increase.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: 170 Systems; ACL Services; Approva; Oracle; Oversight Systems; Reliant Solutions; SAP

Recommended Reading: "Best Practices for Role-Based Separation of Duties in ERP"

"Sarbanes-Oxley Update: How to Best Support the CFO"

IT GRCM

Analysis By: Paul Proctor; Mark Nicolett; French Caldwell

Definition: IT GRCM technology supports the management, measurement and reporting of IT controls, and the distribution and attestation of policies, compliance reporting and risk assessment. IT GRCM solutions have policy and asset repositories, basic document management, workflow, survey and reporting functionality, and dashboarding. IT GRCM solutions also provide policy content that is specific to IT controls, as well as support for automated measurement and reporting. The products may take input from controls automation and monitoring tools, such as vulnerability assessment, configuration auditing, identity and access management, and security information and event monitoring. IT GRCM does not unify everything. It is directed toward a defined subset of functions to manage, measure, and report on risk and security controls.

Position and Adoption Speed Justification: IT GRCM is an emerging market. Product installed bases are small, and adoption has been limited to more-mature organizations that have (or are investing in the development of) the process and policy foundation needed to capitalize on the technology. Adoption will be driven by a need to operationalize compliance activities and the implementation of mature risk-oriented security programs. Many vendors that have technology in adjacent markets will enter the IT GRCM market during 2008 and 2009. In particular, vendors that have capabilities in technical controls data gathering infrastructure (vulnerability assessment and configuration auditing) will create overarching management and reporting functions. Also, vendors that support finance and operations GRCM functions will improve capabilities in IT GRCM to provide comprehensive controls management functions.

User Advice: Organizations were not ready for this type of automation three years ago. Program maturity has reached a tipping point, where many organizations can take advantage of this type of automation to make this level of management a viable vision for some organizations.

Organizations that want to deploy IT GRCM technology must understand that the labor associated with policy development is significant and buy-in is unavoidable. There is wide variation in the scope and functional capabilities in the current set of solutions. An organization that has implemented good vulnerability management is well-positioned to implement IT GRCM technology. Three primary use cases exist: Support for audit workflow, automating the collection and analysis of general computer controls, and managing control self-assessments. Organizations may lead with one of these use cases but should consider their eventual need for all three when developing tool-selection criteria.

IT GRCM products usually are produced 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 you do 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: IT GRCM can improve an organization's external audit capability, reduce compliance-reporting costs and improve an organization's ability to analyze IT risk. Organizations can reduce compliance-reporting costs by applying IT GRCM 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 ingrate 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: Emerging

Sample Vendors: Agiliance; Archer Technologies; Brabeion; Modulo Security; NetIQ; Symantec

Recommended Reading: "IT GRCM Functions Defined"

"MarketScope for IT Governance, Risk and Compliance Management, 2008"

"Critical Capabilities for IT GRCM Tools"

Authorization Management

Analysis By: Earl Perkins

Definition: Authorization management grants and enforces fine-grained authorization policies (also referred to as entitlements, privileges, access rights, permissions and rules) across heterogeneous IT infrastructures, which includes structured/unstructured data, devices and services. Authorization management is delivered by disparate technologies based on specific platforms, applications, network components and devices. None of these, by themselves, create a solution. A more comprehensive/cohesive approach to the problem is occurring with the next generation of authorization management technologies. These are still early in evolution, requiring enterprises to develop a strategy for authorization. An optimum strategy externalizes authorization from applications, enabling application developers to use a common, fine-grained framework to evoke authorization decisions. This allows a centralized and enterprise approach not only to authorization management policies in response to business needs, but to streamline IT infrastructure.

Position and Adoption Speed Justification: Enterprises have sought to address IAM needs through steps such as the centralization of authentication, automation of security administration and reporting, and enforcement of segregation of duties for ERP applications. Addressing "siloed" and fractured approaches to authorization management is a logical next step and will take different, although complementary, forms, depending on data and application type.

User provisioning attempts to administer and report authorization management policies across all platforms and applications. However, more is needed, because it often only administers to one role or group level and doesn't address unstructured data. Other solutions, such as identity auditing and role life cycle management, are required to administer and report on authorization management policies.

Entitlement management is a related function that performs all three actions of authorization management (administer, decide and enforce) in an externalized framework for heterogeneous IT infrastructures. Entitlement management has some role life cycle management and reporting capabilities, but not as much as pure role life cycle management and identity auditing tools.

Entitlement management products are delivered by pure-play vendors and some application development platform vendors.

Some Web access management (WAM) vendors are extending their products to provide authorization management capabilities. These vendors are improving their role life cycle management and identity auditing capabilities beyond just Web-enabled applications to address broader heterogeneous IT infrastructure needs. Early WAM products began as authorization management engines, but few enterprises used that capability because of application requirements. The products became primarily single sign-on solutions for Web-enabled applications, delivering the user to the networked application but performing modest application-level authorization management. This was often referred to as "coarse-grained" authorization.

As service-oriented architecture (SOA)-enabled application development and Web services use grows, authorization management is critical. Web Services Policy Framework (WS-Policy) is a standard used to encode the policies of how a service should be invoked. WS-Policy does not yet substantially define how the service will manage authorization management policies. Authorization management for Web services combines entitlement management and Web services management (WSM).

Interest in identifying unstructured data for electronic discovery (e-discovery) and access control is increasing, as are tools for managing thousands of documents across the enterprise. Few user-provisioning products map users to files. Three important markets for unstructured data management are: 1) metadata management; 2) indexing content and monitoring; and 3) information life cycle management. However, these tools have nascent capabilities for delivering file-based authorization management.

Most authorization management implementations use entitlement management products based on the Organization for the Advancement of Structured Information Standards (OASIS) Extensible Access Control Markup Language (XACML) standard. This is a standard that provides an externalized technical framework for three authorization management actions: administer (through a policy administration point [PAP]), decide (through a policy decision point [PDP]) and enforce (through a policy enforcement point [PEP]). XACML-based implementations have occurred in large financial investment firms, banking and other vertical industries with strong business and regulatory compliance access control needs that must be met across many business applications to mitigate risk.

Some authorization management maturity has occurred in the 2008 IAM Hype Cycle because of the growing pace of implementations for authorization management and movement by major vendors to address the need. The overlap between markets of entitlement management, WAM, identity auditing, application development platforms, WSM, metadata management, indexing content and monitoring, and information life cycle management will continue for the next few years. The markets of entitlement management and WAM are merging into a single authorization management product by 2009, with role life cycle management becoming a tightly coupled capability with the merged authorization management product. Data-focused markets (such as metadata management, indexing content and monitoring, and information life cycle management) will remain separate from authorization management products because of different requirements and audiences.

User Advice: Enterprises need different solutions for authorization management, depending on data and application type. Centralize authorization management administration (PAP) and decision making (PDP), but keep enforcement (PEP) at the platform, application, network and device level to avoid performance bottlenecks at enforcement time. Authorization management enforcement (the PEP) can also be collocated with the Web services management or gateway products. Authorization management requires little to no application modification if done from the outset of a new application development process. Retrofitting legacy applications usually requires

application-level changes to externalize the authorization policy administration and decision making. Apply authorization management to new application development efforts and retrofit authorization management to legacy applications only if urgently required.

Authorization management products can be found from pure-play vendors (such as Cisco-Securent), application development platform vendors (such as IBM, Oracle and SAP) and as an extension of WAM (from CA). Authorization management enforcement for unstructured data is still done at the individual platform level. Authorization management policy reporting of those files can be done by identity auditing tools (such as those from Aveksa or SailPoint). Limited authorization management for Web services support is available from vendors such as AmberPoint, Cisco (formerly Reactivity), Forum Systems, IBM (formerly Webify Solutions), Layer 7 Technologies, Progress Software (formerly Actional), Red Hat (formerly MetaMatrix) and SOA Software.

Business Impact: Removing authorization decisions from application development and centralizing them in a standards-based framework provides significant savings in application development time and IAM infrastructure costs, and addresses information security/regulatory compliance requirements.

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: Bayshore Networks; Bhold; Bitkoo; CA; Cisco; IBM; Jericho Systems; Oracle; SAP

Recommended Reading: "Yesterday's Cool Vendors in Secure Business Enablement: Where Are They Now?"

"Cool Vendors in Secure Business Enablement, 2007"

"Identity and Access Management Technologies Defined, 2008"

At the Peak

Enterprise GRC Platforms

Analysis By: French Caldwell; Thomas Eid

Definition: To assist organizations in making good decisions regarding their GRC requirements, Gartner has developed a model that bundles common areas of requirements across IT, finance and operations (see "A Comparison Model for the GRC Marketplace, 2008 to 2010"). As aligned with this GRC market model, the enterprise GRC platform offers cross-functional capability for integrating and managing a variety of compliance and risk management programs. An enterprise GRC platform must solve an immediate need (such as regulatory compliance) and enable the enterprise to pursue consolidation and integration of additional GRC activities (such as operational risk management and mapping multiple regulations, corporate policies and standards to a common control set). The GRC platform should provide the integration foundations of an overall enterprise GRC architecture by integrating effectively with business applications, and control automation and monitoring solutions. Although it will not contain all the GRC architecture elements in one box, the platform should provide functionality for the primary GRC activities: audit management, compliance management, risk management and policy management, and key supporting functionality — such as reporting, certification, policy mapping and analytics,

integration with business applications and controls, and the ability to collect and aggregate automated controls information.

Position and Adoption Speed Justification: No single vendor provides all the capabilities for an enterprisewide approach to GRC activities. Gartner does not foresee GRC platforms fulfilling all necessary forms of control. The primary purpose of the enterprise GRC platform is to automate GRCM activities — that is, much of the work associated with the documentation and reporting of the risk management and compliance activities that are associated most closely with corporate governance. GRCM is defined as the automation of the management, measurement, remediation and reporting of controls and risks against objectives, and in accordance with rules, regulations, standards and policies.

There is still a need for greater embedding of controls in business applications, host platforms and networks. Enterprise GRC platforms must evolve to collect, correlate, analyze and assess information from this growing set of GRC data sources. It will take several years for enterprise GRC platform vendors to develop and integrate their applications effectively with this growing set of automated controls, and to integrate with other enterprise applications that manage processes and performance.

User Advice: Vendors that offer specialized control products but market them as GRC solutions do the market a disservice, because every possible control is not a requirement for every enterprise. Good GRCM functions, however, are requirements for every enterprise and have the potential to be applied broadly. Only vendors that offer control-independent GRCM solutions should be considered "true" GRCM vendors. Do not be fooled into believing that a vendor that presents itself as a GRC vendor will actually help you with your core GRCM requirements.

Develop comprehensive GRCM requirements. The availability of features for a vendor to support finance, IT or operations requirements does not imply credibility in the production deployment of those functions. For example, many of the enterprise GRC platform vendors historically supported finance and audit GRC requirements in the wake of the Sarbanes-Oxley Act. The addition of features to support operations for IT requirements does not mean that they can address organizations' needs effectively. An enterprise GRC platform is just that, a platform. Carefully weigh your requirements against the platform's ability to support and execute those specific requirements.

Implement a GRC platform to provide a common workplace for a cross-enterprise team approach to compliance and risk management. Consider using an enterprise GRC platform to integrate controls over the general ledger and other business applications, business intelligence, enterprise content management, and control automation and monitoring, but evaluate the specific integration issues with your in-house systems as part of your purchase decision.

Despite vendor claims regarding enterprise GRC platform functionality, we recommend that organizations purchase best-of-breed offerings to address specific requirements in finance, IT and operations GRCM:

- If the enterprise has established a cross-business-unit compliance and/or risk management program, then an enterprise GRC platform will support the management and reporting for that program.
- If the IT organization must perform IT asset risk assessments and/or tight integration of reporting from automated general computer controls, then an IT GRCM solution also is appropriate.
- If organizations use enterprise GRC platform and IT GRCM solutions, then the reporting function of IT GRCM should be integrated into the enterprise GRC platform.

Business Impact: Compliance regulations and greater awareness of business risks worldwide are driving the high-profile business and IT activities of financial compliance, corporate governance and risk management. The requirements and market opportunity are worldwide in scope because companies registered with the U.S. Securities and Exchange Commission must comply with the Sarbanes-Oxley Act, regardless of where their headquarters are located. In response, some countries, such as Canada and Japan, have aligned their financial reporting rules with the Sarbanes-Oxley Act. Furthermore, in an emerging trend, many organizations that are not required by law to comply with the Sarbanes-Oxley Act have implemented many of the requirements for internal controls in response to perceived business advantages and external auditors' higher standards. As enterprises' compliance activities mature and incorporate risk assessment, the awareness of the business value of risk management has become a board-level initiative.

Most companies are organizationally, functionally and technically disaggregated, which can impede business success and make it more difficult for a company to comply with governmental regulations. As organizations take a more holistic approach to GRCM, there will be stronger links among compliance initiatives, risk management and corporate business strategies, which should, in turn, develop better alignment among people, processes and technologies. However, there will continue to be multiple buying centers for GRC offerings for some time because of the fragmented use of too many technologies that have been purchased, deployed and managed separately, as well as a similarly fragmented IT and line-of-business management structure.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: 80-20 Software; Achiever (Sword Group); Archer Technologies; Axentis; BI International; BWise; Compliance 360; Cura; DoubleCheck; IDS Scheer; List S.p.A.; Mega International; Methodware (Jade); MetricStream; OpenPages; Oracle; Paisley; Protiviti; Qumas

Recommended Reading: "The Enterprise Governance, Risk and Compliance Platform Defined"

"Dataquest Insight: The Finance and Audit GRC Software Markets Are Evolving in Support of Broader GRC Management"

"A Comparison Model for the GRC Marketplace, 2008 to 2010"

Crisis/Incident Management

Analysis By: Roberta Witty; Bradley Williams; Daniel Miklovic; Richard DeLotto; Jeff Vining

Definition: Incidents such as earthquakes, fires, floods, collapsing bridges, severe weather conditions, terrorist attacks, chemical spills and so forth affect individuals, localities, businesses and public agencies, all of which desire a return to normalcy after the event. Incident management is the process of managing multiple group/subgroup responses to a particular incident, with a consistent approach to respond quickly and appropriately to minimize damage to an organization's reputation and business operations or a government's ability to reduce adverse impacts on public safety.

In recent years, we've seen the commercialization of specialized incident management software tools designed for government, utility and private-enterprise use. These tools are used to manage relationships with all organization stakeholders and the press, manage incident/situation recovery and restoration actions, manage expenses incurred during the recovery effort, communicate information internally (as well as externally) and provide reports for post-mortem reviews of the

incident for business continuity management (BCM) process improvement efforts. Solutions may be:

- Specialized to the operations of one industry, for example electric utilities or oil and gas.
- Generalized for management of any type of incident normally found in a BCM plan.
- Part of a larger solution, such as an environmental, health and safety (EH&S) application

The incident management capability may be part of a case management tool. Many of these products are evolving into centralized "systems of record" and general risk management tools.

Position and Adoption Speed Justification: Many organizations, particularly governments, are tasked with creating ways to better protect the public and business operations, and improving the efficiency of incident command and related emergency responses. The St. Louis Area Regional Response System and New York State's Emergency Management Office NY-Alert and NY-Delivers are examples of public-private efforts. Government and other industries, such as electric utilities and gas and oil, have for years embraced incident management processes and their supporting technologies to continually communicate and assess progress when responding to a disaster, especially events such as natural disasters and power failures that interrupt the delivery of goods and services, or a pipeline break or biohazard accident that affects the environment. The financial services industry, primarily as a result of 9/11, has started to mature its incident and crisis management processes and has adopted the use of incident management software.

However, in most organizations (even some electric utilities and gas and oil companies), no alignment has been made between managing an operational disruption, such as an electric utility responding to an ice storm, resulting in power failure, and an incident normally covered under a BCM plan, such a fire at the data center. Only since Hurricane Katrina have organizations considered how a supply chain interruption affects their ability to recover and continue business services. Therefore, as institutional crisis/incident management maturity grows, Gartner projects that once-disparate crisis/incident management solutions will begin to show convergence of features, form and functionality. Regional and national-scope disasters increasingly will require enterprise-based crisis/incident management for the critical structure sectors to interact, at least at the level of status reporting and communicating with each other and the government.

User Advice: Incident management functionality should include emergency response planning, incident response and tracking capabilities, community interaction support, and embedded functionality for formalized incident command reporting and processes. Develop an incident command process as a series of steps and components. Each of these, while not mutually exclusive, must be evaluated or tested as independently of the other components as possible, with at least one annual end-to-end test.

Match the type of incident management solution deployed to the most likely and critical types of 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 IT or financial crime management, while a heavy industry manufacturing entity might chose one with functionality tailored for response to environmental or safety-related incidents.

Ensure that the chosen solution adheres to public-sector incident protocols relevant in the geographic regions in which the solution is deployed. For example, in the U.S., any solution targeted to respond to physical incidents, such as environmental mishaps, safety issues or natural disasters affecting health and safety, should adhere to the Incident Command System as

mandated by the U.S. Department of Homeland Security. This will ensure interoperability with public-sector response agencies.

Consult with corporate counsel for jurisdictional issues relating to privacy and rules of evidence.

Business Impact: Incident management processes and solutions help organizations manage all the actions taken in response to a disaster and, therefore, improve the organization's ability to protect public safety; restore business, utility and government services as quickly as possible; ensure recovery of expenses incurred during the disaster from business interruption insurance policies; and protect the reputation of the organization in the eyes of all stakeholders — employees, customers, citizens, partners/suppliers, auditors and regulators. Using a system that imposes a standardized "best" or leading practices model extends uniform managerial controls across the organization, 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: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Crisis Commander; Dell; Electro Scientific Industries; ESRI; ESS; Global AlertLink; IBM; Intergraph; IntraPoint; MissionMode Solutions; Pier Systems; Previstar; Send Word Now; Strategic BCP; Strohl Systems; The National Center for Crisis and Continuity Coordination

Recommended Reading: "Turning EH&S Challenges Into Benefits"

"How to Understand and Select Business Continuity Management Software"

E-Discovery Software

Analysis By: Debra Logan; John Bace; Rita E. Knox

Definition: Electronic discovery (or E-discovery) software facilitates the collection, processing and review of large amounts of electronically-stored information (ESI) within an enterprise 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. An independent group of consultants, legal scholars and vendors have created and put into the public domain an "E-Discovery Reference Model" ([EDRM]; www.edrm.net) that maps traditional common-law discovery into a six-step, nine-process framework for technology. There are hundreds of vendors that have products that fit within the EDRM framework that do everything from policy management and search and analysis, to production and presentation. When Gartner focuses on the e-discovery software market, we are concentrating on the technology providers who work at the nexus of where IT and the legal staff meet: the preservation and collection of relevant ESI from the technologist point of view, and the search, review, and analysis of its content for the legal professional.

Position and Adoption Speed Justification: End users are increasingly doing legal discovery in-house. End-user companies are most interested in the information management, identification, preservation and collection phases of the EDRM. Because of the number of vendors in the market and the remaining uncertainty around what the U.S. courts are expecting companies to do, firms remain confused about what the best practices are should they become involved in litigation.

User Advice: The move to acquire e-discovery software is driven by efforts to reduce risk and drive cost efficiencies.

Evaluate products that can aid in the identification, preservation and collection of potential evidence. The second most important area around e-discovery software is the ability of these tools to create, communicate, enforce and document compliance with litigation hold orders.

Finally, can these tools provide the in-house legal staff with the technology to query custodian repositories in early-case assessment to determine things like cause, motive and action.

Business Impact: Major enterprises undergo dozens, or even hundreds, of investigations per year, resulting in high costs to specialized litigation support companies 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.

The market is just emerging, with point products that handle part of the process being the norm in the market space. There are hundreds of vendors that claim e-discovery functionality in some form or another. The tools have emerged from several adjacent and related areas, like forensic investigations, records and document management, e-mail archiving and search and information access. There is also a large, stand-alone review and analytics market, which focused on providing review and analysis tools for legal personnel. Although the market has already begun to consolidate around a set of tools to handle information management, identification, collection, preservation and processing, we do not consider that there to be complete end-to-end e-discovery suites yet on the market. Aspects of the problem remain difficult, particularly those relating to information access and finding relevant data in the masses of content that most enterprises have.

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: Anacomp; Attenex; Autonomy; AXS-One; Catalyst; CA; Clearwell; CommVault; EMC; FTI Ringtail; Guidance Software; IBM; Kazeon; Mimosa Systems; Oracle; PSS Systems; Recommind; Seagate Technology; StoredIQ; Symantec; ZyLAB

Recommended Reading: "MarketScope for E-Discovery and Litigation Support Vendors"

Forensic Tools

Analysis By: Jay Heiser

Definition: Forensic software is used by investigators for the legally defensible collection of raw data from digital storage devices, the restoration of hidden and deleted files, and the search for potentially incriminating information. Case management functionality maintains and links the collected digital evidence, facilitating the sorting and collation of file data and metadata to determine event sequences and the preparation of legally defensible reports.

Position and Adoption Speed Justification: Regulations addressing hostile workplaces, pornography, privacy, whistle-blowing and insider information leaks are increasing the rate of internally conducted digital investigations. Combined with the growing volume of e-discovery requests and a demand for forensic skills that exceeds the supply, many organizations are building the capabilities to perform forensic tasks in-house, and an increasing number of corporate information security practitioners are choosing investigation as a specialty focus.

Core forensic technology is relatively mature, and its use is well-understood by digital investigator specialists. A relatively new and rapidly growing functionality is "remote forensics" — the location and legally defensible collection of evidence across the network using software agents installed on the PCs being investigated. Useful in analyzing host attacks in progress, remote forensic tools are also being used in support of e-discovery. Forensic technology vendors are being applied as the "front end" for discovery requests, making initial keyword-based searches remotely on personal computers, and preserving the located files and metadata in secure repositories.

The use of forensic tools and techniques are sometimes used in e-discovery to prove the digital integrity of items that have been produced and placed into evidence. This reduces the potential of legal challenges on the part of opposing lawyers who are more often than not trying to win their cases on technicalities, such as suggesting the discovered material has been tampered with.

User Advice: Organizations that find themselves conducting a relatively large number of costly digital investigations should consider organizing an in-house forensic function to gain more control over investigations and reduce costs. Such a step should not be undertaken without ensuring that the investigation staff is sufficiently skilled. Part-time forensic investigators can cause more harm than good, and cases have been lost by inexperienced investigators using forensic tools inappropriately. Organizations that want to have an internal capability must find ways to ensure that their investigative staff can keep their skills strong through drills and actual investigations.

Business Impact: Internal investigative capabilities allow corporate investigators to quickly and inexpensively respond to allegations of inappropriate activities within the IT infrastructure, enabling organizations to effectively enforce their policies and control illegal activities. Only the largest organizations can realistically expect to maintain in-house staff that can perform investigations with the level of rigor as a service provider.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Sample Vendors: AccessData; Guidance Software; Paraben; Technology Pathways

Recommended Reading: "What Every IT Manager Should Know About Digital Forensics"

"Introduction to Investigative Case Management Products"

"Proper Preparation Crucial in Digital Investigations"

"Prepare Your Organization for Effective Computer Forensics"

Identity Auditing

Analysis By: Earl Perkins

Definition: Identity auditing is a technology that documents, reviews and approves access controls — roles, rules, entitlements (also referred to as privileges or permissions). It enables the enforcement of segregation of duties for business applications and IT infrastructures. Identity auditing can be conducted from identity (user) and resource (application, operating system, database and others) perspectives. It answers the following questions:

- Who has access to what?
- Who should have access to what?

- Who reviewed and approved what (that is, the attestation process)?
- Who did what?

Producing identity-audit reports and performing management reviews are labor-intensive and expensive. Depending on regulatory compliance requirements (for example, the U.S. Sarbanes-Oxley Act and Basel bank capital accords), these activities could be performed monthly, quarterly or yearly, as security officers and IT auditors require.

Position and Adoption Speed Justification: IAM governance activities (that is, identity auditing, role life cycle management, access request initiation and security administration approval and workflow) have matured. Identity auditing was created to address gaps between identity management features and customer requirements, such as identity/resource views for users, roles, fine-grained entitlements and approvals. Role life cycle management provides reports and attestation capabilities, but it lacks front-end IAM governance features. The identity-auditing and role life cycle management markets will evolve into full-fledged IAM governance tools from 2008 to 2009.

Historically, basic identity auditing occurred through a number of other IAM technologies, including:

- User-provisioning or stand-alone auditing modules associated with user-provisioning products for "who has access to what" and sometimes the "who should have access to what" reports
- Role life cycle management products from vendors such as Beta Systems (a user-provisioning vendor), Bhold, Courion, Engiweb Security, Eurekify, Oracle (Role Manager), Prodigen, Siemens, Sun Microsystems (Sun Role Manager) and Voelcker Informatik for "who has access to what reports"
- Some identity-based network access control (NAC) products for "who has access to what" and a limited view of "who accessed what" reports (review the 2008 infrastructure protection Hype Cycle to see the NAC vendors)
- Security information and event management (SIEM) products for "who accessed what" reports (review the 2008 SIEM Hype Cycle to see the vendor list)

Identity auditing (also known as identity management compliance reporting) is part of the normal security administration process that organizations have been practicing for years. Regulatory-compliance pressures are forcing most enterprises to write applications to work with a strong access control infrastructure. This infrastructure delivers business-level ownership of access request approvals, permits regular reviews of entitlements/privileges and monitors real-time access events. Access reports of users and applications remain a requirement in information security and compliance/risk management programs, and products are needed to address these requirements.

Clarifying and strengthening customer IAM governance needs, the failure of user-provisioning vendors to address elements of identity auditing and role life cycle management, and growing market requirements for identity auditing all have resulted in a marginal increase in identity auditing on the Hype Cycle. This growth is due to:

- Market maturity as a distinct set of requirements that are separate but related to user provisioning, which increasingly is viewed to application development as "plumbing," with transport pipes and connectors to perform core security administration activities on target systems

- Potential acquisition targets by IAM suite vendors as identity auditing addresses key governance concerns and general IAM feature sets mature as part of a governance architecture for identity

User Advice: If your enterprise needs to respond to auditor requests for reports, or if it needs to start IAM projects with strategic identity governance as a top priority, then a pure-play, identity-auditing product is a good choice.

If developing and managing roles to manage access (regardless of user provisioning to those roles) without strategic governance is a priority, then role life cycle management products are a good choice.

If your enterprise is automating the security administration process as a prerequisite to a user-provisioning initiative, then seek a user-provisioning product with strong reporting and attestation capabilities.

If your organization is implementing network-based access controls categorized by identity, then identity-based NAC products may be useful for NAC reporting. Plan for SIEM products to report on "who did what" across heterogeneous IT infrastructures.

Business Impact: Chief information security officers, compliance officers, IT risk management officers, application developers, IT infrastructure managers and identity management project managers in regulated industries should consider implementing a repeatable process to deliver identity-auditing and governance reports. The cost savings to the enterprise of automating this process can be high.

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: Aveksa; Bhold; CA; Courion; Eurekify; Hitachi; HP; Oracle; Prodigen; SailPoint; Sun Microsystems; Trusted Network Technologies; UpperVision

Recommended Reading: "Identity and Access Management Technologies Defined, 2008"

"Magic Quadrant for User Provisioning, 2H07"

Content Monitoring and Filtering and Data Loss Prevention

Analysis By: Eric Ouellet; Jay Heiser

Definition: Gartner defines content monitoring and filtering (CMF)/data loss prevention (DLP) solutions as the set of content-aware tools used to prevent inadvertent or accidental leaks or exposure of sensitive enterprise information outside authorized channels using monitoring, filtering, blocking and remediation features. 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, and they 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). DLP products maintain detailed logs that can be used to support investigations.

Position and Adoption Speed Justification: This market continues to experience rapid growth, but Gartner still considers it to be in its "adolescent" phase. The market's total value was an estimated $50 million in 2006 and $120 million in 2007. Gartner believes it will reach $200 million to $250 million in 2008. A key factor in the ongoing maturation of solution and technology

offerings has continued to be the infusion of significant amounts of venture capital into relatively small vendors in 2006 and 2007. Many of these vendors have fewer than 100 employees and received funding in the $30 million to $40 million range. During 2006 through 2007, several of these vendors were acquired by incumbent security players (including Symantec, McAfee, Trend Micro, Websense, RSA and Raytheon) with solid positions in the larger security market. We expect further consolidation through 2008 with the remaining independents.

A key driver of this market continues to be the need to address regulatory requirements, including those of the Payment Card Industry (PCI) Initiative and the U.S. Health Insurance Portability and Accountability Act (HIPAA), among other compliance requirements. Another form of market maturation is the increasing appearance of DLP functionality within products such as e-mail security boundary, endpoint monitoring solutions and planned offerings around EDRM.

User Advice: This technology is commonly perceived as being an effective way of preventing theft of intellectual property and for preventing accidental disclosure of regulated information. In practice, it has proved much more useful in helping identify and correct faulty business processes and accidental disclosures. The inadvertent data leakage actually represents the lion's share of the problem, so these automated controls are proving useful. However, motivated insiders will always find ways to steal data, and no technology will ever be able to fully control this. As the technology matures, network-only mechanisms will evolve to a more comprehensive model that also addresses host protection. However, only the network components are mature enough for enterprise use.

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.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Fidelis Security Systems; Orchestria; Reconnex; Tablus; Vericept; Vontu; Websense

Recommended Reading: "Content Monitoring and Filtering Helps Find Faulty Business Process, Accidental Disclosures"

"Market Trends: Content Monitoring and Filtering and Data Loss Prevention, Worldwide, 2008"

"Develop an Enterprise Strategy for Content Monitoring and Filtering/Data Loss Prevention"

"Tips for Midsize Businesses Considering Data Leakage Prevention"

Database Activity Monitoring

Analysis By: Jeffrey Wheatman

Definition: Database activity monitoring (DAM) is a type of governance, risk and compliance (GRC) control that transparently monitors database activity to identify fraudulent, illegal or other undesirable behavior. DAM monitors and analyzes database activity. It operates independently of the database management system (DBMS) audit functionality or as an extension of it. DAM contains embedded knowledge about database structures and access to analytics and reporting. There are two primary use cases for DAM:

- Monitoring of privileged users (for example, database administrators [DBAs] and root or system administrators) offers the ability to read and update all data in the DBMS. DBAs also can modify database structures using data definition language and can manage access controls using data control language. DAM is used to identify and, in some cases, prevent privileged users from accessing data, making modifications to schema or table structure, or creating or modifying user accounts or permissions.

- Application user monitoring focuses primarily on database access that results from transaction activity from the end users and applications that connect to the database. The primary purpose of this monitoring is to detect fraud and other abuses of legitimate access privileges.

Some auditors and security teams are evaluating or implementing DAM technologies to fulfill legal and regulatory requirements, enhance overall risk management, and achieve data governance goals.

Position and Adoption Speed Justification: Auditors are increasingly requiring tighter controls around data stores to preserve confidentiality and integrity of data while limiting access to privileged users and identifying fraudulent activities. Preventative controls, such as encryption, are not effective against authorized user threats. DAM, as a real-time detective control, provides a "last stop" that can be helpful in closing the gaps arising despite the use of preventative controls, such as identity and access management and encryption. DAM is still a young market, with much opportunity for growth. Gartner saw close to 100% growth, year over year, in 2007, and we expect similar growth through 2008.

Although some DAM products come from vendors with a wide variety of offerings, most of the vendors are focused on database and application security. The relatively young age of the market has resulted in rapid change, and the addition of product functions and high levels of responsiveness to customer requests and requirements. Tremendous interest has been spurred by increased focus on legal and regulatory compliance needs.

DAM products are improving and adding new functionality at a rapid pace; on average, we are seeing incremental upgrades quarterly and full upgrades every nine months. Some of the extended functions are dynamic and static discovery of data types (for example, credit card numbers or Social Security numbers), tight integration with SIEM, and vulnerability scanning, as well as future DLP-type functions.

User Advice: Although some clients use native DBMS auditing, there are limitations and constraints to its efficiency and effectiveness:

- Native logging can add significant overhead to the database server CPU.

- A lack of granularity in capturing and reporting makes it more difficult to extract relevant data.

- Clients with heterogeneous environments need to manage multiple logging and reporting platforms.

Clients should:

- Implement DAM functionality to mitigate the high levels of risk resulting from database vulnerabilities and to address audit findings in areas such as database segregation of duties and change management.

- Use DAM technology when there is a need for granular monitoring, or when the overhead of database audit functions is unacceptable.

As with any technology, there are always caveats. Although there have been a few large implementations, enterprises with large installed bases should take a cautious approach and focus on a pilot group of servers to iron out any issues. Pay careful attention to using the "blocking" or prevention functions; application-database interaction can be complicated and great care must be taken to avoid blocking of what may prove to be false positives. Support for certain database and operating system platforms is sometimes incomplete or partial; assemble a full requirements list before talking to vendors, and recognize that your enterprise might need to wait on certain platform support.

Business Impact: Although DAM has not reached its full potential, it is a worthwhile investment for clients with databases containing confidential data, intellectual property or any data that must be protected according to legal and regulatory requirements. DAM will continue to grow in maturity, function and usability.

In addition to helping clients with compliance, DAM is a beneficial addition to risk management programs. Many installations start small and grow rapidly over time as enterprises see increased value and benefit from their investments.

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Sample Vendors: Application Security; Guardium; Imperva; Lumigent; MENTISoftware; Oracle; Secerno; Sentrigo; Tizor

Recommended Reading: "DAM Technology Provides Monitoring and Analytics With Less Overhead"

Stronger Authentication

Analysis By: Ant Allan

Definition: Stronger authentication encompasses a broad variety of technologies that provide greater confidence in a user's claimed identity than simple passwords do. These range from improved password methods, through methods that exploit other things (such as images or patterns) known to only the user or any of many kinds of "token" held by the user, to biometric authentication methods based on biological characteristics or behavioral traits inherent to the user (see "A Taxonomy of Authentication Methods"). Gartner has defined "strong authentication" as authentication that combines two or more methods of different types — known, held or inherent — which significantly increases resistance to attack and, thus, authentication strength. (Such a combination is commonly called two-factor authentication or multifactor authentication.) But even "single-factor" methods can be stronger than simple passwords, and may provide an appropriate level of confidence in some use cases. Each distinct method or combination of methods offers different trade-offs between authentication strength, total cost of ownership and user convenience.

Position and Adoption Speed Justification: Concerns about unauthorized access, especially to financial systems and databases containing private data, are increasing the interest in strengthening authentication. Although commonly implemented at the behest of auditors in the name of regulatory compliance, neither increasing password length and complexity nor forcing periodic changes is effective against deliberate attack or accidental leakage. Yet, much of the focus is still on these ultimately futile efforts to wring as much strength out of simple passwords as possible. Relatively few regulations explicitly demand migration to authentication stronger than simple passwords. Even so, it is increasingly evident that stronger authentication can make a

significant contribution to a broader range of compliance initiatives (adding value to improved controls, monitoring and reporting). Moreover, compliance hype has highlighted the weaknesses of simple passwords, and many enterprises are independently evaluating — and implementing — stronger authentication as a way of mitigating the risks relating to access control and accountability.

Some vendors are aggressively cutting the prices of traditional strong authentication methods, such as hardware tokens, and many are offering lower-cost alternatives, such as phone-based authentication methods and innovative knowledge-based authentication methods. These dynamics mean that many more enterprises will implement stronger authentication during the next few years.

User Advice: Authentication is a foundational service that supports many information security and compliance functions. It is crucial to authorization and auditing services. If users' identities are not properly authenticated, an enterprise has no assurance that access to resources and services is properly controlled. No matter how well-managed a company's authorization services, everything hinges on the true identity of the user. If a person can easily log on with another's user ID, segregation of duties controls provide no benefit. Similarly, without properly authenticated identities, audit trails and other activity logs, however complete and well-monitored, it will be unreliable and provide no accountability. This is pertinent beyond obvious information security usage. In change management, workflow in business processes, records and document management, and so on, there is the same need to know with confidence who did what.

Like any other security service, authentication must be appropriate to the risks. Simple passwords are vulnerable to many attacks and abuses, such as password-capturing spyware, network sniffing, social engineering and unauthorized sharing. In some situations, a simple password might provide an appropriate level of security, but with increased exposure of corporate systems to external users and more-sophisticated threats, the convenience of staying with passwords is increasingly outweighed by the risks. All enterprises should already be using stronger authentication in high-risk situations, and planning wider deployment over the coming years according to a risk-based timetable (see "The Twilight of the Passwords: A Timetable for Migrating to Stronger Authentication"). In many cases, the timetable may be dictated by regulations. This may be explicit, as in online banking where several countries' regulators have demanded "two-factor authentication" or at least something better than simple passwords. But it may also be implicit — enterprises that have regulated content, especially in the areas of privacy or insider trading, and those required to record internal activities through mechanisms such as logging and records and document management systems, should migrate early.

But authentication strength (concomitant with risk) is not the only consideration. When selecting stronger authentication methods, an enterprise should evaluate the impact on users (a particularly difficult issue for consumer-facing applications), ease of integration with its established technology architecture and total cost of ownership (TCO). Fully implementing stronger authentication for all users across an enterprise remains a challenge (see "Ways of Integrating New Authentication Methods Within a Heterogeneous Environment"). However, it is relatively straightforward to deploy stronger authentication for remote or extranet access, or for discrete critical applications.

Enterprises should not overlook complementary safeguards, such as fraud detection and monitoring, transaction verification, and network access control. We see this as particularly appropriate for online consumer security, where we see an increasing incidence of attacks that bypass authentication and so can succeed however strongly users are authenticated (and such compensating controls are allowed by some banking regulations). However, such complementary safeguards have value in other use cases too.

Business Impact: Stronger authentication provides increased confidence in the identity of users accessing enterprises' systems and data, strengthening the bond between users and their online activities. Thus, it adds considerable value to other security and compliance initiatives, such as improved access controls (including enforcement of segregation of duties), monitoring and reporting. Stronger authentication not only will reduce the risk of unauthorized access to regulated and other sensitive data, but can also significantly improve individual accountability and the forensic value of audit trails in support of a variety of internal investigations.

Nevertheless, authentication cannot mitigate all kinds of identity-based attack. Malware-based attacks, for example, can succeed however strongly users are authenticated. Enterprises must also invest in complementary safeguards.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Sample Vendors: AdmitOne Security; Authentify; DigitalPersona; Entrust; PortWise; RSA; Swivel Secure; Vasco Data Security International; VeriSign

Recommended Reading: "A Taxonomy of Authentication Methods"

"Defining Authentication Strength Is Not as Easy as 1, 2, 3"

"The Twilight of the Passwords: A Timetable for Migrating to Stronger Authentication"

Role Life Cycle Management

Analysis By: Earl Perkins

Definition: Role life cycle management mines, defines, maps, manages and reports on the complex relationships of users, business rules, roles and entitlements assigned to them within the IT infrastructure. A generic framework is required to address role life cycle management needs. Enterprises enhance their identity administration processes to:

- Define existing roles through business analysis and role mining automation.
- Manage formal and informal business-level roles for enterprise views (such as location, department, country and functional responsibility), and provide input into user-provisioning products to link business roles and associated IT roles. It also ensures proper entitlements are provisioned for the user.
- Manage the role through its entire life cycle — role owner, role changes, role review, role assignment and role retirement.
- Establish a process by which new business and application roles use the same management process as existing roles, and tie those new roles to role life cycle management processes.

Position and Adoption Speed Justification: Regulatory compliance pressures (such as those from the Sarbanes-Oxley Act and Health Insurance Portability and Accountability Act in the U.S.) drive role life cycle management into many identity administration initiatives. As a result, the role becomes a key control point for mapping authorization entitlements that enterprises need to manage as life cycles, just as they do an identity. Financial services companies lead in this effort, but are being joined by other vertical markets, such as retail, telecommunications and

manufacturing. Role life cycle management has matured past the Peak of Inflated Expectations on the Hype Cycle for the following reasons:

- It plays a critical role for most enterprises in streamlining the user-provisioning initiative by standardizing role and entitlement use in those initiatives.
- Enterprises are becoming aware that managing roles and entitlements can help in other areas of identity and access management, including identity auditing, compliance reporting and authorization management.

User Advice: Establish a role framework that matches the culture and operations of your business. Using HR titles, roles or job codes is not reliable for most enterprises because they are not detailed enough to map the specific and varied authorization entitlements used for access control for business applications. It is not uncommon to have many roles assigned to each user; this approach enables flexibility in role management, but more so in aligning authorization entitlements to the different business functions that the user performs.

Use a top-down and bottom-up approach to role development. One approach does not work — you will end up with theoretical roles that don't correspond to reality (top-down only), or with roles that have limited or excessive access (bottom-up only). Don't try for 100% assignment of users to roles — 80% is "good enough." The expense of getting that final 20% isn't worth the investment.

Business Impact: Role life cycle management is recognized as an important part of identity and access management deployments, particularly for large, multinational enterprises and other organizations with complex reporting and management relationships that need authorization entitlements managed consistently. Role life cycle management is aligned with business process management. It determines the correct approver based on the current business policies of the enterprise. Some user-provisioning vendors offer this functionality as part of their core product; others are developing the capability themselves or acquiring companies that provide the capability.

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Sample Vendors: Aveksa; Beta Systems; Bhold; Courion; Engiweb Security; Eurekify; Novell; Oracle; Prodigen; Quest Software; SailPoint; Siemens; Sun Microsystems; Voelcker Informatik

Recommended Reading: "Magic Quadrant for User Provisioning, 2H07"

"Identity and Access Management Technologies Defined, 2008"

EH&S Compliance Systems

Analysis By: Daniel Miklovic

Definition: EH&S compliance systems capture product or process data according to a regulatory authority's standards, forms and procedures for compliance with laws related to occupational health and safety; hazardous materials management and product genealogy/content; and environmental management. Compliance management applications provide richer functionality such as tracking processes or rolling up the status of multiple compliance activities. This provides management with an accounting that can help manage risks in a more holistic fashion. The greater the use/production of hazardous materials and the more dangerous the industry is, the greater or richer the functionality required and the stronger the impetus to use commercial off-the-shelf products.

Position and Adoption Speed Justification: Despite legislation mandating compliance, typical deployed solutions are fraught with departmental biases, legacy applications (often point solutions), and a lack of end-to-end information definitions and flows across regulated business processes. Suites that mitigate these problems are just beginning to gain acceptance in the industry. Most deployments are along a single branch of Gartner's EH&S model.

User Advice: CIOs must assemble holistic views of the various regulatory requirements crossing individual departments. Once that is done, compliance teams may identify department-specific needs and common needs, planning architectures, and systems to maximize the business impact of end-to-end compliance goals. Organizations must be sure to properly weight reporting and notification functions in their evaluation of vendors against the "to be" compliance environment. The advantages of a platform approach using a content-rich solution set can provide the maximum benefit.

Business Impact: These systems affect corporate and manufacturing strategic business unit compliance programs. As such, they enable continued operation but do not directly contribute to enhanced performance. However, if leveraged to provide the basis for carbon accounting, for many industries, these applications can contribute to revenue generation through selling of carbon credits, or can indicate the need for offsets. Additionally, when deployed across all aspects of EH&S, they can contribute to much higher employee satisfaction, customer brand loyalty (assuming improved performance) and stakeholder value.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Enviance; ESS; Hitec (Laboratories); Paradigm Software; Perillon; Synapsis Technology

Recommended Reading: "Turning EH&S Challenges Into Benefits"

Sliding Into the Trough

Configuration Auditing

Analysis By: Ronni Colville; Mark Nicolett

Definition: Configuration auditing tools provide change detection and reconciliation against pre-established policies and standards (such as operational, regulatory and security), and the record of approved changes. Broad configuration change detection capability is needed to guarantee system integrity by ensuring that all unauthorized changes are discovered (and potentially remediated). Discovered changes need to be matched to the approved and documented records for change (RFCs) that are governed in the IT change management system. Configuration settings are assessed against industry-recognized security best practices (such as NIST and CIS) or company-specific policies (for example, "golden image") for operating systems, network components, applications and databases. Exception reports can be generated, and some tools can automatically return the settings to their desired values or can block changes based on approvals or specific change windows.

Position and Adoption Speed Justification: Configuration audit has a major external driver (regulatory compliance) and an internal driver (improved availability). Implementation of the technology is gaited by the process maturity of the organization. Prerequisites include a functional change management process, as well as the ability to define and implement configuration standards.

User Advice: Develop sound configuration and change management processes within your organization before introducing configuration auditing technology. Process development and technology deployment should focus on the systems that are material to the compliance issue being solved. Define the specific audit controls that are required before configuration auditing technology is selected, because each configuration auditing tool has a different focus and breadth — for example, security regulation, system hardening, application consistency and operating system consistency. IT system administrators, network administrators or system engineers should evaluate configuration auditing tools to maintain operational configuration standards and provide a reporting mechanism for change activity. Security officers should evaluate configuration auditing tools to implement system-hardening standards and provide an automated control audit trail that enables internal and external auditors to address regulatory requirements.

Business Impact: Regulations do not provide a clear definition of what constitutes compliance for IT operations and production support, so businesses must select reasonable and appropriate controls, based on reasonably anticipated risks, and build a case that their controls are correct for their situation. Reducing unauthorized change is part of a good control environment.

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 the broader configuration management capabilities) will ensure reliable and predictable configuration changes and offer policy-based compliance with audit reporting.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Sample Vendors: BMC/Bladelogic; Solidcore Systems; Tripwire

Recommended Reading: "Configuration Auditing Is an Overlapping Market Segment"

"Answering Some Frequently Asked Questions About Configuration Auditing"

"Using Configuration Auditing for Compliance Control"

"Server Provisioning and Configuration Management Vendors Differ in Functional Focus"

Quality Compliance

Analysis By: Daniel Miklovic

Definition: Quality compliance is either a stand-alone application or a functional subset of a larger compliance application that provides for the management of compliance with International Organization for Standardization (ISO) standards or other quality standards, which may be internationally required, self-mandated or customer-mandated (see Quality Standards ISO 9000 and Related Standards for other typical quality standards). Quality compliance functionality ensures that proper workflow — frequently associated with ISO 9000 series standards — occurs and that a document trail is created that validates that the workflow has been followed. It also generally has functionality that allows products or services that do not meet certain quality specifications to be moved from a work-in-process state to a finished-goods state, making it available for shipment. Other functionality may be provided to ensure that only trained or certified employees are involved in the production of certain products and that product safety standards, such as those of the U.S. FDA and the U.S. Department of Agriculture (USDA), as well as other quasi-quality standards, are met, depending on the product category.

Position and Adoption Speed Justification: Quality control tools have been available for years, and statistical process/quality control applications are well-established; they are endpoint-focused solutions that address either adherence to specifications or process improvement. The addition of workflow management features is what expands the solution set into a quality compliance technology, and as such, the deployment footprint is just now approaching the 20% mark, especially in manufacturing. The pre-Trough position reflects the integration of the Slope position of pure statistical process control or statistical quality control (SPC/SQC) functionality coupled with the near-the-Peak hype of specific track-and-trace/genealogy solutions as well as the Trough position of pure quality workflow solutions.

In reality, point functionality is still sometimes deployed, but there is an increasing trend toward either full-function compliance solutions or overall GRC solutions that have full-function quality compliance capabilities. Quality management has been an area dominated by specialists, frequently from a statistics background. However, it is moving into a mainstream technology area, which must be supported by IT functions.

User Advice: Enterprises in all industries — especially those in consumer-facing industries and particularly those delivering products targeted for use by children or for consumption, such as food or pharmaceuticals — should deploy quality compliance functionality. The choice of a point quality compliance solution or leveraging of quality compliance capabilities provided by broader GRC suites will depend on individual circumstances.

Generally, as long as specific quality compliance requirements can be met using the broader GRC solution, it makes more sense to use the broader package. However, where the FDA, the USDA or other regulatory quality compliance standards need to be met and the functionality is not available in a generic GRC application, a specific solution should be deployed. In those cases, maximize the use of the point solution, because the integration of the workflow is generally an essential element of regulatory compliance.

Business Impact: Any business that delivers products and services should have a quality compliance program. Even in commodity-based industries, quality remains a differentiating factor. Quality compliance touches all aspects of product delivery from the original design (for example, evaluating its eventual fitness for use or application), to manufacturing, to delivery and, finally, after-the-sale service.

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, poor quality in automobile tires, or contaminated food or medical products. A stringent quality compliance program supported by robust tools can prevent unsafe, dangerous or shoddy products from reaching the market. More importantly, for quality compliance (such as with ISO 9000, for contractual reasons), the best practice is to use compliance automation solutions.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: IBS; IQS; MetricStream; Qumas; Sparta Systems

Recommended Reading: "Best-in-Class Lean Manufacturing Leverages IT"

"Manufacturers Miss Point on Shop-Floor-to-Top-Floor Projects"

"Key Issues and Research Agenda for the Manufacturing Industry, 1H08"

E-Mail Archiving

Analysis By: Carolyn DiCenzo; Kenneth Chin

Definition: Leading e-mail archiving solutions provide tools for capturing all, or selected, e-mail messages in a central repository for efficient storage and access. These tools can also prune messages from the active e-mail system data stores, leaving stubs that redirect users to the archive for viewing or retrieval. This activity is designed to keep the active message system data stores lean, to improve application performance and reduce recovery times. The need for users to maintain personal stores is eliminated and established stores can be migrated to the archive. Quotas can be used to trigger archiving or can be eliminated totally, with the stubbing being driven by a policy that usually is based on age and/or size of the message and related attachments. Legal discovery and content retention and search are used to meet discovery and compliance requirements. They also provide a way to export data for use with special purpose or more robust e-discovery tools. Tools for sampling and reviewing messages are available with many e-mail archiving products, in response to requirements specifically for the regulated portion of the financial industry. With the increase in the use of laptops for mobile workers, it is becoming increasingly important to provide users with the option to have a copy of their portion of the archive on their local disk.

Position and Adoption Speed Justification: The number of vendors offering e-mail archiving solutions continues to increase, with most offering archiving and mailbox management solutions appropriate for the markets that they target. The ability to put messages on legal hold has improved, but largely remain untested because many users have yet to set a time frame for deletion or, if one was set, refuse to approve the deletion. As more features within installed products are tested, or as company archiving requirements change, some companies will look to replace their initial product with another. A choice of products is available for all the major mail systems, and providers of mail solutions are continuing to provide better links within their mail systems for archiving vendors to leverage. Companies with large volumes of e-mail and long retention periods are putting stress on the scalability and reliability of current solutions, requiring improved index methods and, in some cases, major architectural changes. The need to support more than just e-mail and attachments, such as documents or presentations, is also causing vendors to redesign their offerings. Enterprises that bought tactical solutions or overbought and are unable to deal with the complexity are preparing to change to more-appropriate products. An increasing number of companies have implemented e-mail archiving for some part of their mail users. For those that have implemented archiving for all users, the opportunity still exists to sell more capabilities to existing customers to extend the archive access to users or to provide more robust legal discovery support.

User Advice: As requirements to search and recover old e-mail messages grow, and in the face of increased demand for higher user quotas as users struggle to keep up with increased numbers of messages and larger messages, companies should implement an e-mail archiving solution now. Consolidating all archived messages into regional repositories or a centralized repository will support a quick response to inquiry and will enable a quick implementation of the official retention policy when it is ready. Migrating personal stores to the archive should be part of the deployment of an archive system. Look for archiving solutions that provide the additional option to archive files and other content types that also may be needed in the future.

Business Impact: E-mail archiving improves e-mail application performance, delivers improved service to users, and enables timely response to legal discovery and business requests for historical information. Archived data can be stored on less expensive storage technology, with the opportunity to even take some of the data offline or to delete it. Removing old data to an archive will also reduce backup and recovery time.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Atempo; Autonomy; AXS-One; Barracuda Networks; C2C Systems; CA; CommVault; EMC; Estorian; GFI; GFT inboxx; GWAVA; HP; H&S Software; IBM; Jatheon Technologies; MessageSolution; Messaging Architects; Mimosa Systems; Open Text; Quest Software; Sherpa Software; Symantec; Waterford Technologies; ZL Technologies

Recommended Reading: "What Is E-mail Active Archiving?"

"E-Mail Active Archiving Market Update, 2008"

"Magic Quadrant for E-Mail Active Archiving, 2008"

Operational Risk Engines

Analysis By: Doug McKibben; David Furlonger

Definition: An operational risk engine is a tool for the measurement of potential loss that is due to the inadequate management of operations. It supports event reporting, calculates the risk capital (economic and regulatory) to be allocated to operational risk, runs scenarios against operational risk exposures (such as value at risk, loss frequency, loss severity or loss from a given event) to quantify operational risk, fits statistical distributions to internal and external loss data, links cause and effect to determine key risk indicators (KRIs), conducts fault tree analysis, and creates qualitative rankings and balanced scorecards for operational risk.

Position and Adoption Speed Justification: Much operational risk management (ORM) is still focused on process standardization and monitoring, rather than on allocation of capital as the result of risk-based performance and economic analysis. In addition, there is a lack of consistently defined and recorded operational risk information within institutions and across the industry. This precludes best practice or enterprisewide modeling of operational risks in the near term.

In this environment, many vendors based their operational risk applications on pre-existing and usually non-industry-specific software for qualitative assessment of operational risk processes and controls, and assessment policy management. Generalized, qualitative offerings have been acceptable to many financial institutions that have not yet recognized the competitive value of quantifying operational risk information to advance performance management, and have not been pushed in that direction by regulators. At this point, many banks falling under the Basel II Capital Accord employ the basic indicator or standardized approaches to operational risk that base regulatory capital for operational risk on measures of gross income rather than on internal process or activity-specific measurements.

However, the influence of Basel II and the necessity to link risk assessment to corporate performance will continue to push adoption of a more-blended quantitative/qualitative approach. In addition to qualitative assessment functions, this approach will include quantitative functionality for capital calculation and scenario analysis where exposures are continually examined and adjusted as additional data becomes available. Regulatory pressure and the competitive value of improved performance management will increase the attractiveness of this blended approach and will drive the broader adoption of operational risk engines to support risk-based performance measurement and capital allocation.

User Advice: Avoid vendors of generic (nonindustry), qualitative operational risk tools in favor of applications that combine self-assessment capabilities to monitor and measure KRIs and business process. Preferred applications will also facilitate the quantification of operational risk for calculating and allocating risk, regulator and economic capital. Quantification is essential for corporate performance management. Evaluate vendor offerings in the context of an overall risk management and governance strategy to share data and process workflows across the enterprise. Avoid building a heavily customized solution that cannot be readily assimilated into that architectural blueprint.

Business Impact: Beyond regulatory compliance for such initiatives as Sarbanes-Oxley or Basel II, standardized definition, quantification and reporting of operational risk data are essential for managing corporate performance. Process effectiveness is a core element of quality customer service, which will drive customer retention, organic growth and competitive differentiation. Focusing on the process level will also enable the clearer definition and monitoring of line-of-business processes. This will be increasingly important as organizations move toward a services approach with reusable subprocesses. The inability to understand and successfully manage operational risks will also substantially expose businesses to negative operational risk events and impair the potential for long-term business viability.

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Sample Vendors: Algorithmics; eFront; Mega International; Oracle Financial Services; SAS

IT Change Management Tools

Analysis By: Kris Brittain

Definition: IT change management (ITCM) tool functionality governs documentation, review, approval, coordination, scheduling, monitoring and reporting of RFCs. The basic functional requirements begin in the area of case documentation, with industry-standard assignment capabilities of classification and categorization (such as risk and priority). The tool must include a solid workflow engine to manage embedded workflows (such as standard RFC life cycle), as well as provide escalation and notification capability, which can be executed manually or be automated via business rules. RFC workflows are presented graphically and are capable of managing assessment and segmented approval with the ability to adjust automatically, based on alterations and multitask change records. To assist with managing the large volume of RFC activity, ITCM tools enable workload assignment, scheduling and calendar functionality, as well as the reporting analysis of service-level agreements and production metrics. Critical integrations with configuration, release and configuration management database (CMDB) technologies are required for change management tool success. For example, the categorization of a configuration item within the case log in the ITCM tools will improve risk, impact and collision assessment capabilities through the integration with a CMDB. Integration with release management tools provides improved quality and efficiency when IT change management workflow policy automates RFC handoffs to release. Other critical integrations include configuration audit tools and governance, risk and compliance tools. The majority of ITCM tools are a module offered within IT service desk suites offering integration with incident and problem management.

Position and Adoption Speed Justification: Nearly 60% of enterprise-scale companies use ITCM tools to support their ability to govern ITCM process policies. Overall industry adoption has been slow, resulting from years of IT technical silo or department-specific processes which represent configuration and release (such as application development and server management)

change execution procedures, not IT change management. However, pressure is growing based on 24/7 demands, operational efficiency, recent compliance demands and emerging technologies (such as service-oriented architecture and virtualization). The adoption of industry standards, such as ITIL v.3 and CobiT 4.0, is also accelerating the adoption of ITCM tools.

User Advice: The ITCM tool should be the sole source for governing and managing the RFC life cycle. IT organizations looking for closed-loop change management will require the change tool to be integrated with configuration and release management tools used to build, test, package and push the change into the production environment, such as server provisioning and configuration management, as well as software change and configuration management (SCCM). Initiatives to address compliance demands, such as the Sarbanes-Oxley Act, can be addressed by ITCM tools to support control procedural documentation and the integration with configuration auditing tools to produce a complete view of compliance and noncompliance reporting. Tool adoption will require new responsibilities in the IT organization, such as adding IT change manager and change coordinator roles. As well, growing service complexity and compliance (demand to adhere to governmental and industry regulations) will influence the ITCM tool implementation and depth of integrations (such as configuration auditing to support compliance reporting).

Business Impact: An ITCM process that is implemented across all IT departments will deliver discernible benefits in terms of service quality, IT agility, cost reductions and risk management. The implementation of ITCM tools will improve communications within the IT organization as well as between the IT organization and its business constituents. By managing all RFCs in a common repository, IT organizations achieve improved insight into the service-level effects resulting from changes, as well as better coordination of changes based on the ability to manage the change schedule. With an ITCM tool in production, compliance and business risk rules can be established, which will improve the overall analysis, authorization and reporting of IT changes.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: BMC Software (Remedy); CA; HP-Peregrine Systems; IBM Maximo

Recommended Reading: "Poll Indicates IT Change Management Improving Slowly"

"The ITCM Market Presents a Confusing Vendor Landscape"

Database Encryption

Analysis By: Eric Ouellet

Definition: Database encryption software is used to protect data within relational database management systems (RDBMSs) at the table or column levels.

Position and Adoption Speed Justification: This technology has been available for some years, but has been plagued with performance and technical problems. Current products work well on databases designed initially with provisions for the support of encryption functionality integration, but can be difficult to implement on legacy systems. Use of encryption on certain fields results in a fundamental level of impact, altering the behavior and usability of the RDBMS when indexing or performing wild-card searches. Existing offerings require significant schema changes to support encryption. Portability of encrypted fields from one application to another remains difficult under most scenarios, as does centralized key management. Export of large encrypted datasets to third-party partners for external processing remains problematic. RDBMS vendors are improving native encryption capabilities, but most continue to fail in protecting data

from database administrators. Third-party vendors will be seriously challenged if RDBMS vendors resolve this problem.

User Advice: Despite the difficulty involved, enterprises should plan to encrypt all credit card numbers, Social Security numbers, bank account numbers and other information that is deemed sensitive in databases within two to three years. Begin planning, testing and integrating cryptographic functions in projects today, even though they may take two to three years to complete due to internal political sensitivity, application testing, and workflow or database use modifications.

Business Impact: Arguably, encryption offers the most certain form of control against unauthorized access to data. Consequently, concerns about privacy, and especially payment card industry standards, are putting pressure on enterprises to make greater use of cryptographic mechanisms to protect person-related information. Although it remains difficult to implement and use, database encryption is increasingly perceived as desirable and even mandatory. Enterprises with a business need to demonstrate the highest level of practice in the protection of personal data will have no alternative to the use of database encryption software.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Application Security; IBM; Ingrian; Microsoft; NetLib; Oracle; Protegrity; Valyd; Yantra

Recommended Reading: "When and How to Use Database Encryption"

Risk Assessment for BCM

Analysis By: Les Stevens; Roberta Witty

Definition: Risk assessment in the BCM context is the process of identifying and treating risks to business continuity. It is an essential step in the overall BCM process necessary to reduce the frequency and effect of business interruptions, addressing risks related to technology, location, geopolitical, regulatory and industry.

Position and Adoption Speed Justification: Unfortunately, BCM planning is often conducted with a superficial level of risk assessment, or none at all. Although it has been well-understood that risk assessments are a necessary component of BCM planning, the line of business often considers them to be time-consuming and too resource-intensive. This opinion has been justified given the general lack of efficient risk assessment methods and tools. Expectations of better levels of practice are increasing though, encouraged to some extent by standards such as ITIL, CobiT and ISO/IEC 27001. Today, risk assessments are recommended in almost every BCM framework, and risk assessment tools are being included as integrated or stand-alone modules in BCM toolsets. Using these tools requires specific BCM skills and time, which are often not available, but this situation is improving.

User Advice: Make formal risk assessments that identify key control weaknesses and single points of failure a mandatory component of your BCM program. Define the extent to which risk assessments will be performed based on BCM project scope, and resource and time availability. If existing processes are not effective, then change them. Improve efficiency and reduce time demands on business managers by leveraging risk assessments performed by operational or IT risk teams. Work with those teams to ensure that their data is sufficiently granular-level to meet BCM needs. As you become more mature at BCM risk assessment, make the transition to a

continuous process accommodating BCM and IT and security risks. This will ensure that BCM teams are included and kept apprised of new or changing threats. Use a standard terminology and process to ensure consistency in assessment and risk prioritization. Investigate the use of software tools. They will not eliminate the need for an experienced risk assessor, but they can simplify the risk assessment process. Additionally, they provide an important repository for risk information, tracking assessment and treatment activities, providing documentation for auditors and an aid to program improvement.

Business Impact: Implementing BCM plans can be expensive and disruptive. Risk assessments are essential for pre-emptive action to reduce threat occurrences and constrain the effect of a disaster so that the need to implement BCM plans is diminished.

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Sample Vendors: eBRP Solutions; Linus; Office-Shadow; RiskWatch; Siemens Enterprise Communications

Business Continuity Management Planning Tools

Analysis By: Kristen Noakes-Fry; Les Stevens; Roberta Witty

Definition: Business continuity management planning (BCMP) software automates the collaborative research, analysis and writing needed to create a recovery plan for critical business and IT operations that can be published and distributed to the recovery teams.

A BCMP software package will typically include the following components:

- Business impact analysis
- Risk assessment for BCM
- Business process and IT dependency mapping
- Information libraries of common equipment, procedures and so forth
- Plan builder

Position and Adoption Speed Justification: BCMP products have been in the market for more than 20 years, and have grown from word-processing templates to sophisticated interactive decision support tools. The past decade has seen increased awareness of the need for a usable recovery plan, as well as a consistent and repeatable plan development process, and has resulted in increased sophistication in the products. In addition, they are more likely than in the past to integrate with other BCM tools, such as emergency notification and incident management. However, even with the growing awareness, the added sophistication has resulted in very complex tools, and this complexity has limited the uptake of these tools in the marketplace. Few organizations use them to their fullest potential; rather, they are often used as a master repository for recovery plans stored in Word, Excel, Visio or other documents. The newer BCMP products introduced in the marketplace during the past three years have been built from the ground up, using modern technology, and have focused on end-user usability and streamlined BCM process implementation. Most BCMP products are based on proprietary methodologies, and therefore do not align with any particular BCM standard or framework — for example, BS25999, ITIL v.3, Singapore TR19, PAS 77, DRII, BCI and so forth.

Most offerings today are available as a hosted service by the vendor. Perpetual licensing is available if needed in some cases. Although various types of tools are on the market, the Web-based products facilitate multiple departments, divisions and locations, providing input to the plan and enabling the plan itself to be managed consistently from a central location.

User Advice: Consider BCMP tools when:

- You are faced with audit results that have uncovered gaps in your preparedness to deal with an emergency.
- You need to integrate plans and partial plans from a number of departments and business units into one consistent, accessible, easily updated plan.
- 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 minimum assistance from outside consultants.

Choose a tool that matches your organization's complexity — do not overbuy.

Without continuous process improvement procedures in place for periodic plan review and event-triggered plan reviews (such as changes in the organizational processes or changes in related regulations), even the best recovery plan can rapidly become obsolete. Like your other policies and procedures, the recovery plan will need to be a living document, as flexible enough to be changed as the business and technology. Of all your company documents, this is the one most likely to result in lost revenue or damaged reputation if it is not current.

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 to have in place an up-to-date, accessible plan to facilitate recovery. If used to its fullest potential, a BCMP tool can be used to enhance business resilience in areas such as human resource management, business re-engineering, mergers and acquisitions, and so forth.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Sample Vendors: COOP Systems; eBRP Solutions; EverGreen Data Continuity; Paradigm Solutions International; Strategic BCP; Strohl Systems; SunGard Data Systems

Recommended Reading: "Best Practices for Conducting a Business Impact Analysis"

"How to Understand and Select Business Continuity Management Software"

Qualitative Risk Self-Assessment Tools

Analysis By: Doug McKibben; David Furlonger

Definition: Risk self-assessment tools are software applications that provide the ability to identify operational risk exposures, and link controls, risks, audit findings and losses to those exposures. Usually as an alternative to decentralized, spreadsheet-based approaches, these applications are employed to provide greater control and access to risk and control data in a consistent manner across the institution to detect changes in the operation's risk profile and to assess the effectiveness of risk management and performance controls. These software packages typically

support risk policy definition and controls, including an organizational framework, business process identification, and mapping, evaluation, audit and certification functions. Information related to loss events, near misses and key risk indicators is captured and reported, and workflow functions support the alerting and escalation of risk events to the appropriate level of management for regulatory reporting. Risk self-assessment tools focus on qualitative, process-based management of operational risk, but typically do not include quantitative risk measurement and calculation capabilities.

Position and Adoption Speed Justification: With regard to technical applications, the lack of an organizationwide view and risk management program plan, and often the treatment of operational risk as a series of disjointed tasks or projects as opposed to a holistic strategy, have resulted in an inconsistent and many times incompatible approach to data management and reporting across the organization. From a management perspective, this means that the context concerning the nature of the risk event or loss is often lost or hidden. Effective enterprise data governance, including metadata management as well as the movement to real-time workflow management and alerting necessary for enterprise-level management and control, is not possible with an ad hoc approach. Many vendors with a limited offering support and even encourage compartmentalized or piecemeal tactics to gain a foothold in the institution with a promise of building out the solution over time, even though they have not previously demonstrated such capabilities with others. It is acceptable to maintain such functionality and extend it, but only in the context of a broader enterprise strategy and solution architecture. Functional extension should be evaluated in the context of a risk management methodology blueprint or framework to avoid redundancy and to facilitate integration and data sharing across the enterprise. The software market for operational risk software, while immature, continues to evolve rapidly. However, various vendors contend that they provide software for managing operational risk, but most address only elements of an institution's portfolio of operational risk exposures and frequently provide generic, non-industry-specific solutions that focus on a rudimentary compliance and reporting regime typical of GRC initiatives. Qualitative risk self-assessment is only part of the operational risk management process.

User Advice: There are no shortcuts. Pursuing multiple project initiatives without working out interdependencies and conflicts will complicate and delay implementation, as well as escalate costs and potential losses.

While some financial services providers (FSPs) have found vendors capable of addressing flexible and integrated architectures required to address Basel II and talk about service orientation, organizations must not be lured into vendor offerings that lack fundamental, pre-existing capabilities and that have not achieved a level of market acceptance and scale in live installations. Moreover, most risk management services have not received sufficient treatment to be widely developed or deployed. Financial institutions must avoid building, under vendor influence, a heavily customized solution that cannot be readily assimilated into the buyer's broader IT architecture, and must still pay close attention to the long-term viability of many of the vendors offering operational risk management solutions. Moreover, many of the larger, seemingly viable vendors that perhaps lack sufficient stand-alone functional capabilities may encourage custom code generation as a tactic to inhibit any future vendor replacement due to the mission-criticality of this type of application**.**

This duality can challenge IT departments, which tend to view risk management, incorrectly, as only the reduction or elimination of IT risk. The challenge for IT groups is to determine which risk software and technical processes offer the capability to detect and capitalize on risk events significant to corporate performance, as well as measure and report on, and potentially reduce risk, through automation and standardization.

Financial institutions that purchase applications that only support qualitative self-assessment solutions run the risk of having to replace them with those that also support quantitative functionality, if they want to leverage operational risk management for improved performance or if they are forced by regulators to move to an advanced measurement approach.

Business Impact: Operational risk management, in general, has traditionally focused on system failure, not process. Merely continuing the traditional method of internal and regulatory audits ignores the forward-looking requirements of managing operational risk and the broader implications of operational risk beyond what can be observed or experienced directly by an institution. This requires extending the focus of operational risk management beyond the rudimentary compliance and reporting regime of the typical GRC initiative. While an appropriate emphasis on the competitive value of effective governance is necessary, decisions on how to run your business should not be linked exclusively to regulatory action. This includes taking a holistic approach to risk management across the enterprise, which delivers consistent operational risk data across the institution, as well as addresses its interdependencies and correlations with market and credit risks to capitalize on the positive potential of properly managed risk. Rather than focusing only on preventing or reporting losses and risk events, the objective of operational risk management is performance improvement to deliver maximum return to the organization.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

SIEM

Analysis By: Mark Nicolett

Definition: SIEM technology provides two main capabilities. Security event management (SEM) analyzes security event data in real time (for threat management, primarily in network events). Security information management (SIM) analyzes and reports on log data (for privileged user and resource access monitoring and compliance reporting, primarily in host and application events).

Position and Adoption Speed Justification: Early adoption of the technology was limited to very large companies, and the focus was SEM. Many smaller companies are now adopting this technology. Application of the technology is trending more toward the SIM use case, driven by regulatory compliance reporting requirements and the rise in targeted attacks.

User Advice: Product selection decisions should be driven by organization-specific requirements in areas such as the relative importance of SIM vs. SEM capabilities, speed of deployment requirements, acquisition cost and the IT organization's support capabilities, and integration with established system and application infrastructures.

Business Impact: SEM helps IT security operations personnel be more effective in responding to external and internal threats. SIM provides reporting and analysis of data to support regulatory compliance initiatives, internal threat management and security policy compliance management.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: ArcSight; CA; Cisco; eIQnetworks; ExaProtect; High Tower; IBM; Intellitactics; LogLogic; LogRhythm; netForensics; NetIQ; NitroSecurity; Novell; OpenService; Prism

Microsystems; Q1 Labs; Quest Software; RSA (EMC); SenSage; Symantec; Tenable Network Security; TriGeo

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

"Critical Capabilities for Security Information and Event Management Technology, 2008"

"Select the Right Monitoring and Fraud Detection Technology"

Climbing the Slope

ERP SOD Controls

Analysis By: Neil MacDonald

Definition: Largely driven by regulatory compliance requirements, organizations are looking to address segregation of duties (SOD) issues in their enterprise applications. These projects typically start with resolving SOD issues in financial transactions that are embodied in ERP applications, such as those offered by SAP and Oracle. Technology controls to address the problem include detection and remediation of existing conflicts, modeling to detect potential conflicts at the time of provisioning and transaction monitoring for SOD violations.

Position and Adoption Speed Justification: Addressing SOD issues that surround financial transactions is increasingly required by auditors and is driven primarily by the U.S. Sarbanes-Oxley Act and similar legislation worldwide. This process can be addressed manually, but it is complex and resource-intensive. Automated SOD analysis tools provide immediate value in the automation and consistency of the SOD remediation process. These tools are entering the mainstream (as evidenced by SAP's 2006 acquisition of Virsa Systems and Oracle's 2007 acquisition of LogicalApps, which had acquired Applimation), but they remain expensive and complex to maintain. We have seen cases in which these tools were purchased and were later shelved because process deficiencies weren't addressed first. In many cases, organizations will look to their ERP platform vendors for this capability, which will pressure smaller, stand-alone vendors in this space to provide sufficient differentiation.

User Advice: If you are a larger organization, then manual analysis and removal of SOD conflicts will be costly and don't solve the root cause — preventing SOD violations from being introduced to begin with. Purchasing an automated tool alone won't solve what, fundamentally, is a process problem. Start by designing a process for eliminating SOD conflicts in all enterprise applications, beginning with financial transactions. Then evaluate the tools that help to automate the process and make it more scalable and consistent.

Transaction monitoring helps to quickly identify SOD violations that have occurred and can provide controls for other types of violations or risks beyond SOD conflicts (for example, fraud and collusion). Oracle and SAP's solutions can be expensive, so do not overlook alternative third-party solutions from Approva, Security Weaver and others that are substantially less expensive.

Business Impact: Investments are typically made to address a specific control deficiency by an external audit. Regulatory compliance is the major driver of investments in this area. Longer term, SOD conflict detection and remediation should become part of a broader controls management framework and strategy, and automated SOD analysis should be integrated into the automated provisioning of users and roles within identity and access management role management systems.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: ACL Services; Approva; D2C Solutions; FoxT; Oracle; Oversight Systems; SAP (xEM/GRC); Security Weaver

Recommended Reading: "Best Practices for Role-Based Separation of Duties in ERP"

"MarketScope for Segregation of Duties Controls Within ERP, 2007"

Case Management

Analysis By: Jay Heiser

Definition: Investigative case management products are workflow tools used by investigators to track the occurrence and resolution of person-related incidents, completely documenting ongoing and historical investigations into regulated activities. Case management tools are typically intended for the support of specific types of investigations, including HR, money laundering, fraud and computer forensics. Anonymous reporting (whistle-blowing) capabilities are increasingly being added to corporate case management tools.

Position and Adoption Speed Justification: Case management is an essential part of any compliance, anti-fraud or anti-money-laundering effort, automating data correlation and workflow, and providing legally defensible documentation for specific cases and historical records on loss events. The whistle-blowing requirements in Sections 301 and 302 of the Sarbanes-Oxley Act have encouraged public companies to include anonymous reporting capabilities as part of their case management workflow. Revisions to the Federal Rules of Civil Procedure and the rigorous focus they require on issues dealing with e-discovery are encouraging growing interest in software to help guide the litigation life span. The corporate legal departments using these products often refer to them as "matter management." Although the market remains fractured, with different tools being purchased by different corporate departments and relatively little sharing of case data among corporate functions, this somewhat sleepy market is starting to wake up. The past 18 months have seen several vendors change hands, and a growing number of products are being positioned as "enterprise case management," suggesting the benefit of using a common platform to support multiple corporate departments. Although use of these products does vary according to vertical industry, virtually all Fortune 500 and heavily regulated organizations are making some use of case management products somewhere. However, many corporate departments that would benefit from them have yet to seriously consider the purchase of a purpose-built product.

User Advice: Although many organizations create and use their own database or just rely on spreadsheets, organizations that have purchased purpose-built tools find they enhance their productivity, providing features that they would not have included in a system built in-house. Any corporate function conducting regular investigations should consider the use of a commercial case management system purpose-built for their needs. IT can improve investigative efficiency and reduce overall costs by encouraging different corporate departments (such as security, HR and corporate counsel) to share a common case management platform.

Business Impact: Virtually all regulated organizations require case management tools for the use of HR, compliance, legal, corporate security and corporate counsel. Loss tracking and reporting, as well as whistle-blowing support, are mandatory activities for publicly held companies, and suspicious-activity reporting is required of a growing number of companies. These activities cannot be adequately performed without automation.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Sample Vendors: D3 Security Management Systems; EthicsPoint; Guidance Software; PPM 2000; Syfact; Vantos

Recommended Reading: "Introduction to Investigative Case Management Products"

"Ease Financial Crime Compliance Efforts With Case Management Tools"

"Improve Operational Risk Management With Syfact Investigator"

Credit and Market Risk Calculation Engines

Analysis By: Doug McKibben; David Furlonger

Definition: Credit and market risk calculation engines for banks are used to quantify and analyze risk exposures, as well as the likelihood and effect of potential default. To be effective, they should include at least these components: capital computation, capital adequacy reporting, probability of default (PD)/loss given default (LGD) calculation, economic calculation, risk-adjusted return on capital (RAROC), collateral management, stress testing, scenario analysis, value at risk and Monte Carlo simulations.

Position and Adoption Speed Justification: Unlike operational risk, credit and market risk functionality is well-established in the majority of banks. Institutions already have developed or obtained applications for calculating and managing these exposures within the context of their legacy environments. As required, the majority are modifying and expanding established functionality to meet demands of newer regulations for additional calculations and analysis (such as risk-weighted assets [RWAs], PD and LGD calculations) rather than replacing existing applications. In terms of modeling these exposures, there is not yet a single best practice developed for modeling risk. Risk engines themselves are nearing mainstream maturity and are built to accommodate any modeling approach that an institution may currently use or that may evolve.

User Advice: It is acceptable to maintain existing applications or to consider replacements, but they should not be stand-alone, and their acquisition should be evaluated in the context of, and mapped to, a risk management technology blueprint for the enterprise — to avoid redundancy and facilitate integration and data sharing across the enterprise. Avoid build-to-order solutions, given the complex functional requirements of enterprise risk management (ERM) and Basel II, as well as the cost and uncertain performance of custom-built or prototype offerings. Consider vendors with established applications, subject matter expertise in risk, industry experience and an installed customer base.

Business Impact: Demonstrating effective risk governance and control extends beyond regulatory compliance. Quality service and corporate performance management hinge on having a "single version of the truth" to support decision making, which can only be achieved from a holistic view of risk across customer and business portfolios. This includes the employment of common internal risk methodologies, as well as the consistent use of risk calculations and retention of the associated data across the institutions.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Sample Vendors: Algorithmics; Fermat; Fernbach; Oracle Financial Services; SAS; SunGard

User Provisioning

Analysis By: Earl Perkins

Definition: User provisioning is the act of creating, modifying, disabling and deleting user accounts (of, for example, employees, contractors or consumers) and the profiles linked to each person across IT infrastructure and business applications. Using approaches such as cloning, roles and business rules, user provisioning enables the business to support all onboarding and off-boarding activities for the workforce — for example, new hires, transfers, promotions, terminations and dismissals for cause. User provisioning also automatically correlates data from HR, CRM, e-mail systems and other "identity stores." Fulfillment is handled by self-service requests, a line management request or an HR system change. Regulatory compliance and security efficiencies continue to drive most user-provisioning implementations to date.

Position and Adoption Speed Justification: Security administration hasn't worked in many enterprises because of the complexity of identity information locations and needs. Enterprises continue to implement user provisioning to address this complexity, driven by the business to establish regulatory reporting and reduce that complexity. These enterprises seek to automate data entry for security administration. However, these same business drivers and their user-provisioning responses underline weaknesses and gaps in delivery. To correct this, user provisioning is increasingly augmented by role life cycle management and resource access administration capabilities. Although user-provisioning technology is improving, it remains a slow process because of complexity and integration needs. Therefore, its time to plateau in maturity will increase to two to five years from 2008.

User Advice: Implementing user provisioning is often complex and lengthy because of inadequate planning between the enterprise and integrator — product features appear adequate. However, not all products meet the identity administration needs for users. Some products show considerable business process capabilities. Best practices highlight the need to understand and document the "as is" processes for fulfilling user access requests, then design and agree on a new access fulfillment process.

Choosing a product that aligns with enterprise architecture and administrative needs is critical. Choosing the right integrator to deploy and manage the effort is also key. Easily implemented and maintained products (such as Web-services-architected products, a minimal hardware presence, modular functionality and those with excellent connector management) are desirable for Day 1 deployments (the first day of work for a new user). Day 2 and Day 3 processing (such as changes to existing users, systems and business practices) is more complex than Day 1 processing. Avoid technology selection at the outset — a decision framework that identifies, prioritizes and organizes resources for the initiative is best.

Business Impact: User provisioning can offer significant return on investment over manual methods when aligned with an enterprise's mission-critical applications and can become a mission-critical application itself. Customers seldom report a return to manual processes once automated. If the deployment accurately reflects the role of people in business operations, then streamlining many business processes can be done, especially those that involve fast turnaround for changing business needs on a daily basis.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Sample Vendors: Avatier; Beta Systems; BMC Software; CA; Courion; Evidian; Fischer International; Hitachi; IBM; Microsoft; NetPro; Novell; Omada A/S; Oracle; Quest Software; SAP (MaXware); Sentillion; Siemens; Sun Microsystems; Voelcker Informatik

Recommended Reading: "Magic Quadrant for User Provisioning, 2H07"

"Identity and Access Management Technologies Defined, 2008"

Records Management

Analysis By: Kenneth Chin; Debra Logan

Definition: Records management (RM) technologies enable organizations to enforce the policies and rules for the retention and disposition of content required for documenting business transactions, and automate the management of their record-retention policies. These technologies, implemented with well-formulated and consistently enforced RM strategy and policies, form an essential part of organization-wide life cycle management of records. Records management principles and technology apply to any media, including non-electronic media.

Position and Adoption Speed Justification: RM was introduced 10 years ago, but focused mainly on paper documents and, until recently, lacked impetus for adoption. Legislation and regulations are driving organizations to meet similar compliance requirements for electronic content. RM has become a core component of enterprise content management (ECM) product suites and is being deployed as part of an overall ECM strategy. Integrated content archiving platforms are also including varying levels of retention management capabilities. Major drivers in the U.S. federal government include the eGovernment Act of 2002, the Office of Management and Budget Circular A-123 (Sarbanes-Oxley-type requirements for financial management and access controls) and the President's Management Agenda initiative (e-records management), which address correspondence management, e-records management and permanent records archiving. More recently, the Federal Rules of Civil Procedures has driven the demand for RM, and we expect RM will move from departmental deployment to organization-wide implementations.

User Advice: All public companies and government sector organizations should implement and maintain a comprehensive RM program, supported by appropriate technology and processes. Your records management program should be part of a broader enterprise content management strategy. Records management programs are necessary if organizations want to manage the amount of content they have over time, because a life cycle approach ensures that content is managed, archived, stored and deleted as appropriate.

Business Impact: Global companies will adopt RM to comply with regulations, mitigate the risk of litigation and liability, and meet legal discovery requirements. Many government organizations worldwide are also implementing RM solutions. In most cases, this is being driven by compliance with local RM legislation and regulation.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: ASG; Autonomy; CA; EMC; IBM; Iron Mountain; Objective; Open Text; Oracle; Tower Software; Vignette; ZyLAB

Recommended Reading: "Toolkit: Seven Key Criteria for Evaluating Records Management Solutions"

"MarketScope for Records Management, 2007"

User Interfaces for Disabled People

Analysis By: Sharon Mcnee

Definition: Some copiers, printers and multifunction products (MFPs) are designed or modified with user interfaces or are compatible with remote user interfaces to enable visually, aurally or physically impaired individuals to use them as required by law.

Position and Adoption Speed Justification: In November 2000, the European Union undertook to prohibit discrimination of people with disabilities and others in the labor market. Its aims were set out in an EC directive that introduced the concept of reasonable accommodation. This directive means that an employer must do what is reasonable to adapt a workplace or working routines to the capabilities and needs of a person with disabilities. A prerequisite for this is that the person is the best candidate for the job once these adaptations have been made. In the United States, the policy was taken a step further. Section 508 of the Rehabilitation Act of 1998 requires that electronic and information technology developed, procured, maintained or used by the federal government is accessible to people with disabilities.

Section 508 has been in effect in the U.S. federal government since 2001, so the full impact of this legislation has already been felt in these environments. However, demand exists and may continue to exist for easy-access user interfaces to extend beyond federal government offices into all offices and to countries outside the United States, or even into environments in which ease of use is key regardless of whether the user is disabled. Major vendors, such as Canon, Konica Minolta, Ricoh and Xerox, are integrating accessible technology for all.

User Advice: Ensure that your copier, printer and MFP fleets are easy to use and comply with local legislation on technology accessibility for all. Failure to comply will rule you out of many tender situations and disadvantage you where there is no legal requirement but where compliance is a box to tick. Monitor progress in voice recognition technology because it can bring benefits to all users — regardless of abilities — and it has the potential to improve document workflow and applications.

Business Impact: Office printing, copying and document processing will be affected. Aging consumer populations may also increase future demand for devices that can be used from a wheelchair or by people with diminished vision or manual dexterity. Advances in technology, particularly voice recognition, may increase future demand. Another advance, which may increase future demand, has been the development of a remote personal user interface by Select Technology, a U.K. company. The interface can be viewed in the Web browser of a PC or PDA and can be used to remotely operate MFP functions, such as manipulation, printing, copying, scanning, sending and sharing of documents. The new user interface takes advantage of existing and future assistive technology available on the host device (such as magnifiers and screen readers).

Benefit Rating: Low

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Sample Vendors: Canon; Konica Minolta; Ricoh; Select Technology; Xerox

Recommended Reading: "Cool Vendors in Printing Markets, 2007"

"Vendors Must Make Printers and Copiers Everyone Can Access"

Entering the Plateau

Anti-Money-Laundering

Analysis By: Richard DeLotto

Definition: These products help entities covered by anti-money-laundering (AML) regulations to:

- Verify the identity of any person seeking to open an account, determine the source and destination of their funding, and check the account opener's name against any government-provided lists of known or suspected terrorists or terrorist organizations.
- Understand their customers' and stakeholders' behaviors well enough to detect and report suspicious activities. This is done through comparing the client to profiles of expected, projected and suspect behaviors, and through direct tracking of behavior violating regulations.

Systems run the gamut from simple rule engines (such as flagging deposits over a certain amount) to complex profile generators that detect changes in risk profile (such as the subject suddenly having multiple phone numbers, or having limited means of support yet traveling extensively to high-intensity financial crime areas and wiring money to noncooperating countries).

Position and Adoption Speed Justification: AML compliance is an ever-shifting target for the financial services community worldwide. Although initially required for U.S. banks since the 1970 passage of the Bank Secrecy Act, the components of compliance, business processes affected and institutions covered have steadily grown to include institutions as diverse as casinos, check printers, transportation dealerships and jewelers. All are required to detect and report behavior that might be related to criminal activities or activities that "make no sense" based on their understanding of the client. Although the same law applies to all, individual regulators' expectations and requirements may vary. Many banks, in particular, face detailed AML compliance responsibilities for each jurisdiction in which they operate, and they must balance the sometimes conflicting needs for data privacy, financial crime detection and cost containment. Requirements will spread to other industries over time. Regulations and response technologies are based on the Organisation for Economic Co-operation and Development's (OECD's) Financial Action Task Force's "40 Recommendations" and are similar worldwide. Hype in this niche is driven largely by the need to show continual adjustments to external conditions and changes to the bank's internal technical and product environments, though heavy local effects can be seen due to new regulations. Almost all financial services providers will have some form of AML technology in place, though types will vary from simple rule engines to advanced neural networks; no method can fairly be said to be dominant. The focus is shifting worldwide from anti-terror and organized-crime issues (where the technologies are quite mature) to one of enhancing governmental collection of revenue and increasing control of tax evasion, requiring additional detection methods and data sources.

User Advice: Systems must be upgraded to reflect changes in criminal behavior, customers served, new products or processes, shifts in enforcement emphasis, and ever-tightening regulations. "Test, patch and test again" remains the best operational policy.

Business Impact: The information and insights on customer behavior required for AML compliance are substantively the same as those required for successful sales and marketing: Covered entities are required to understand their customers' behaviors well enough to detect suspicious activities. Emphasis will shift from purely compliance-oriented tools to a more refined business intelligence approach. Increased understanding of customer behavior may be transformational to banks.

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Early mainstream

Sample Vendors: Bankers Systems; GIFTS Software; Mantas; NetEconomy; SAS

Recommended Reading: "Client Issues 2005: Risk and Regulation in Banking"

"Use Gartner's COMPARE Cycle to Guide Anti-Money-Laundering Efforts"

Interdiction List Compliance Tools

Analysis By: Richard DeLotto

Definition: Known in the U.S. as Office of Foreign Assets Control (OFAC) tools, interdiction list compliance tools are a broad variety of matching and record-keeping systems designed to detect and prevent companies worldwide from initiating or maintaining commercial relationships with parties interdicted by government regulatory agencies, as well as the seizing/freezing/disposing of foreign-owned or controlled assets in accordance with government policy.

Position and Adoption Speed Justification: Hype in this niche is driven largely by two factors: 1) the ongoing regulatory need to adjust improvements in compliance technology to hit a "moving target"; and 2) the industry need to reduce costs and improve operating efficiency. Interdiction list screening of some sort is mandatory for most financial services providers worldwide, though where and how it is done vary widely. Although tool use is nearly universal in financial services, their uptake lags elsewhere; interdiction list management tools wobble in popularity, based on the changing needs of the regulatory and enforcement communities, whose actions drive user purchasing and the willingness of users to spend for risk reduction beyond minimum compliance requirements. Enforcement and severity of penalties seem to shift with the political climate. Current matching systems are adequate for all but the most sophisticated needs. Users are, however, likely to switch to find lower prices for lists and services, or incremental improvements in performance. Weaknesses are centered on customer data quality and integration issues (an issue far beyond the remediation of the interdiction tool vendors), intensified by the reluctance of many users to subscribe to nonmandated lists, neither of which is likely to be overcome in the near term.

User Advice: Gartner urges clients to keep their matching tools updated to take advantage of improving technology, adopt all available interdiction and heightened risk entity lists ("required" or not), and process all stakeholders through them as a general risk reduction procedure.

Business Impact: All businesses operating in the U.S. are required to verify contacts against certain interdiction lists, though few seem to comply. The sole positive business effect of these technologies is the reduction of compliance and reputation risk. Failure to comply can result in heavy fines and (rarely) incarceration for willfully noncompliant managers. Online services are now available for as little as $250 per year. Good software for smaller firms can be had for less than $5,000, with ongoing license fees based on usage.

Benefit Rating: Moderate

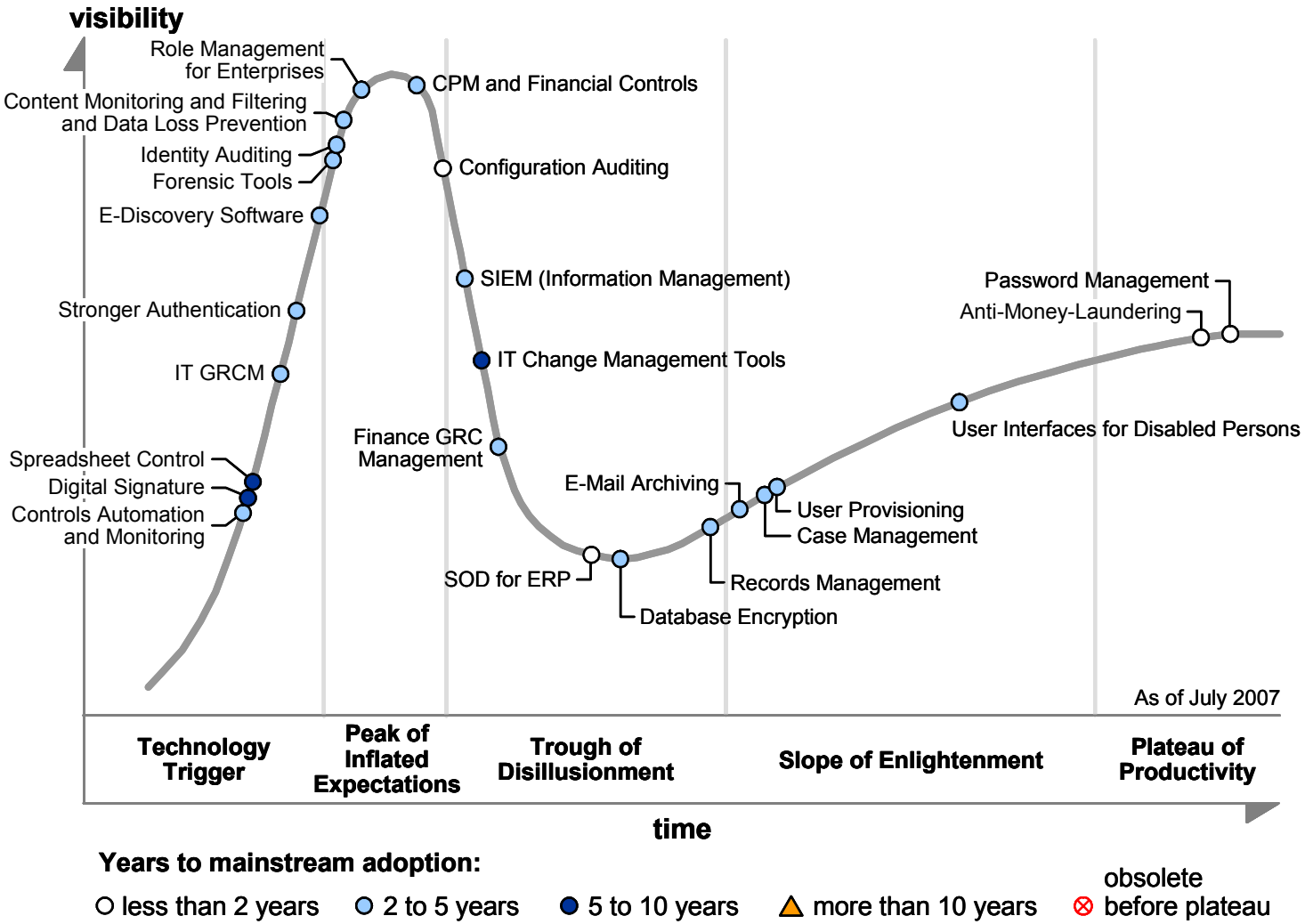
Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Sample Vendors: ChoicePoint; LexisNexis; Metavante; World-Check

Appendixes

Figure 3. Hype Cycle for Compliance Technology, 2007



Source: Gartner (July 2007)

Hype Cycle Phases, Benefit Ratings and Maturity Levels

Table 1. Hype Cycle Phases

Phase	Definition
Technology 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 2008)

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

Benefit Rating	Definition
Low	Slightly improves processes (for example, improved user experience) that will be difficult to translate into increased revenue or cost savings

Source: Gartner (July 2008)

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 2008)

RECOMMENDED READING

"Magic Quadrant for Operational Risk Management Software for Financial Services"

"Key Issues for the Risk and Security Roles, 2008"

"Top Five Issues and Research Agenda, 2008: The IT Risk Manager"

"Understanding Gartner's Hype Cycles, 2008"

"Is SaaS Safe for Financial Governance, Risk and Compliance Solutions?"

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters
Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509

Gartner