

Dynamic Information Access Control:

MARKET MILESTONE REPORT



Going Beyond ECM Security

Carl Frappaolo and Dan Keldsen

Dynamic Information Access Control

There is great risk in assuming that content is in any deep sense “secured” simply because an Enterprise Content Management (ECM) solution is in place.

It is no longer reasonable to expect workers to be the watchful eye and only enforcement point in ensuring that information that should be private and/or protected remains in a secured state – between accidental content exposure and purposeful content leakage (eg. Selling credit reporting information to collections agencies). The problem of “who is watching the watchers” is one of many problems with pushing this responsibility down to individual workers. Scalability, simple awareness, and enforceability of security policies are just not reliable through a purely human effort.

Security Facets Throughout the Lifecycle

The answer to today’s information security requirements lies in a concept we label Dynamic Information Access Control (DIAC). DIAC is security that is specifically addressed – and in many cases embedded directly into – content throughout its lifecycle, from creation, modification, distribution, archiving and destruction, regardless of format or transmission method. This policy-driven capability is distinct from the realm of Information Security (InfoSec), which is primarily focused on securing infrastructure such as networks, servers, desktops, and operating systems.

DIAC includes securing not simply entire documents of any file format, but can also be extended down to “chunk” levels (such as chapters, paragraphs, indexes, etc.) as well as the metadata associated with this content, such as MS Office properties fields (author, title, summary, version number, internal reference number), tracked changes, forwarding history, etc. Every facet of content, from the macro to the chunk level, and metadata about or within content needs to be accounted for to have a reasonably comprehensive DIAC system.

Technologies that Enable DIAC

It is important to note however that DIAC is *not* a technology, but rather a strategy and system comprised of a many point technologies. The challenge is in orchestrating these point technologies to work as a cohesive lifecycle solution. ECM is a useful platform to orient content creation, distribution and re-use, but is not the end solution to all content problems. While an ECM repository is often secured, what is done with the content once it has left the virtual walls of the repository is essentially out of the realm of responsibility for ECM at this time.



DELPHI
GROUP

A Perot Systems Company

111 Huntington Avenue,
Boston, MA 02199

Before we discuss DIAC as an orchestrated solution, we need to understand the individual components that potentially comprise DIAC. The primary point technologies are:

- Records Management,
- Document Management,
- Web Content Management,
- Workflow,
- Business Process Management,
- Enterprise and/or Digital Rights Management,
- Identity Management,
- Content Authentication,
- e-Record Posting, and
- Contextual Information Filtering.

Records Management (RM) systems begin to hint at the overall lifecycle management of information, managing declared business records against the Records Retention schedules that an organization has established. RM addresses the “final resting place” or “life duration” of content, but does not address any other security aspects of content. This is often a critical component of DIAC, which an astonishingly large number of organizations continue to ignore. Content should not simply accumulate – lack of ownership and oversight of content impacts storage costs, manageability as a whole, and quite often, there is latent content that later becomes a “smoking gun” that should have long since disappeared – as long as they were legally, and disposed of in accordance to valid policies and procedures, and vice versa (disposed of in spite of retention schedules because they were **believed** to be problematic content).

Document Management (DM) systems are typically concerned with revision control (knowing the current version and ability to roll-back to prior versions to correct mistakes), document lifecycle audit trails (knowing the string of authorship, last modification date/time/author stamp), and rendition control (PDF versus MS Word copies of the same content – linking the two together). Frequently these are checkbox features for larger ECM solutions although DM can exist outside of ECM. DM is a core capability for DIAC, as integration into DM capabilities allow multiple points to apply policies, provide logging, and ensure that “splintered” versions of documents (Word vs. PDF from above) retain appropriate policies regardless of the machine format used.

Web Content Management (WCM) interwoven within a DIAC context extend policy-awareness to both internal and externally-facing sites/applications, to ensure that content managed and deployed via the Web remains in compliance with the policies established within the purview of DIAC.

Ultimately, DIAC allows content to be security aware within unique contexts – such as who is accessing the content, where the user is currently located, whether the user is connected or off-line, how many times viewers are allowed to open the document, whether cut/copy/paste of content is allowable, whether rights to forward to another user are available, etc.. This particular set of capabilities is most fully embodied within Enterprise or Digital Rights Management (ERM/DRM) solutions, which literally embed security policies within documents themselves, enforcing policy even when outside the boundaries of ECM repositories, or even organizational perimeters (such as behind the firewall).

Workflow (WF) and Business Process Management (BPM) are integral to full-fledged DIAC. WF and BPM technologies ensure that content creating, modifying, distributing, archiving and destroying systems and processes are in fact applying the policies that the organization intends is **key** to the policy-driven and policy-enforced nature of DIAC. Without automated processes to assist and enforce these policies, DIAC is greatly vulnerable to human error, oversight and/or sabotage.

Identity Management (IdM) is used to ensure that Authentication, Access and Audit controls feed from authoritative, current, and fully correct identity stores. Policies need to be connected to both higher-level groupings, and have fine-grained control down to each unique individual. While standard access control repositories such as Active Directory (AD) are typical end repositories of this information, they do not in and of themselves contain the “intelligence” to ensure that this information is verified and up-to-date. Regulatory compliance and general corporate governance standards state explicitly that access privileges need to be certified and audited, much as the generation of financial statements are required for Sarbanes Oxley (SarBox) compliance. Individuals should have the appropriate level of access to information that they need to do their stated jobs, but **no more than that**. All too often, employees who have been within the organization for a number of years, transferring through various divisions and departments, accumulate privileges that are no longer relevant, and more often than not, completely inappropriate to retain – organizations should be wary of “rights creep” as that can completely undermine any useful implementation of DIACs.

e-Record Posting (e-RP) is technology that works in concert with RM or DM systems to certify outside of the RM/DM system that a record, when submitted to the managing system is the same record as when it is later recalled/retrieved – in order to prove that the record has not been modified and beyond repudiation. This is also known as Data Integrity, and is in some cases provided as a service by a third party to further separate the possibility of internal collusion.

Contextual Information Filtering (CIF) is the intelligent filtering component of DIAC that allows policies to be automatically enforced with as little human intervention as possible. This capability is able to “read” content and discern whether there is protected, private data (such as social security numbers, credit card numbers, medical history), intent to divulge information

indirectly (rephrasing protected content to bypass keyword filters – known also as advanced content filtering or linguistic content filtering) or in preventing certain parties (such as buy-side and sell-side workers in a brokerage house) from being able to communicate due to the issues of internal collusion.

Lastly, Content Authentication plays a key role within DIAC in ensuring that content accessed is exactly the content that it claims to be – this includes digital signing, hashing, watermarks and similar techniques to allow verification of the content to the level of scrutiny that is appropriate.

The sum total of these technologies into a DIAC assures the enterprise trustworthiness (via Content Authentication) of content, to ensure that employees are operating from the latest version (DM) and not an expired copy (RM) of their policies, that they can find the original author or owner of the content (IdM), to ensure that the process (WF and BPM) they are involved in, and their understanding of the relevant content. For customer-facing applications of content, having content publishing processes that certify the authenticity of content (tracing the chain of authorship and approval), can help to prevent faulty content from ever being seen by customers, side-stepping the sort of mess that several airlines have encountered recently in inadvertently offering airfares for far less than their operating costs. Content Authentication coupled with suitably intelligent publishing rules (e.g. Flights should cost no less than \$X) would ensure that such mistakes are prevented.

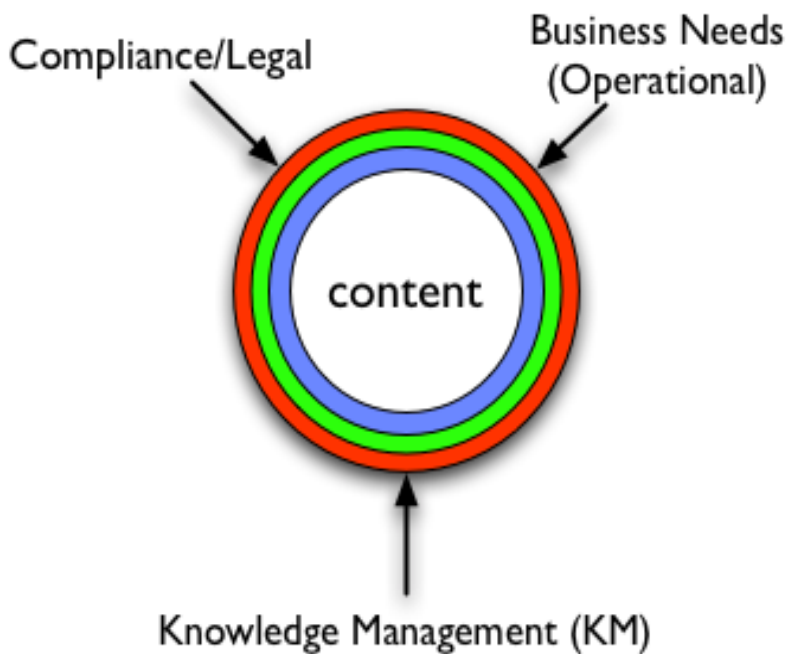
Technology in Itself, is Not the Solution

Orchestration of these technologies into a cohesive DIAC system comes through the policies, procedures, and disciplines created by the organization that apply business rules on and within content, providing intelligent assistance that allow employees to automatically “do the right thing” (auto-correction or prevention as warranted) or inform them of the corrective actions that they need to implement to safely create, use, disseminate, modify or destroy content in a business setting. While it is possible to buy/obtain generic “compliance policies” for many current regulatory concerns, organizations should be wary of simply consuming those rule sets whole. Make certain that the technical interpretation of these rules agrees with your organization’s legal interpretation, or you will be automating your way into legal snafus.

The Business Drivers Behind DIAC

Like many other technical genres that have emerged over the last several years, Dynamic information access control (DIAC) is not a technology in search of a business problem, but rather one that is directly in response to new business challenges emerging in the 21st century. At the root of these emerging business requirements is the growing rate at which the global business community creates, stores and shares its business content in elec-

tronic format. Word processing, e-mail (and attachments), instant messaging, web sites and online collaboration are among the more popular approaches to creating and storing business content. It is not the objective of this study, however, to add redundant statistics regarding the amount of business content that is created and stored electronically – we have all accepted this as fact by now. Nor is it the focus of this study to state that the online content itself is responsible for the need for dynamic information access control. Rather, the existence of the online content has given way to evolving business challenges and opportunities. Indeed, In the case of dynamic information access control, there is not one business challenge or set of issues, but three. This triumvirate convergence of need is a strong force behind the rate at which dynamic information access control is likely to be embraced.



As the figure to the left illustrates, the need for DIAC is driven by: 1) the need for increased control in the form of compliance/legal issues, 2) evolving business models or operational business needs that leverage digital intellectual property in unprecedented ways and 3) knowledge management initiatives to drive innovation and collaboration . Each of these forces is a separate and distinct challenge in today's business setting. Each has associated with it, schools of thought, established user communities, and niche solution players. Each of these is a separate and distinct opportunity and challenge. In fact, It is not a foregone conclusion that every organization will require functionality that addresses each of these situations – at least initially. Similarly, the component technologies, as introduced above, that comprise DIAC are not required in each of these situations. That is why it is good business sense to determine which of these business forces are relevant to your current practices and then, in turn, to determine which technology components are required.

Intelligent Information Processing

Compliance/legal has received the greatest attention of late. Industry dynamics such as increased regulation, lawsuits, identity theft – to name but a few, are requiring that organizations protect online content and employ policies, procedures and processes that control how content is accessed, by whom, and how long it is maintained. The need to know the who, what and when associated with content mandates the application of workflow and document management with their associated audit trails. The need to establish valid content that is beyond repudiation requires application of records management, e-record filing, data integrity and content authenticity technologies. ERM and DRM software enable organizations to prohibit access to content not just by user, but by business context. For example, limiting access to sensitive content to certain users, *only* when they are establishing access from certain (controlled) IP addresses. Data loss prevention technology, content filtering, ERM and DRM technology prohibit intentional and accidental shipping of content to unauthorized users and/or to unauthorized media (e.g. inability to print certain content). This functionality protects the organization not only from the overt content, but from the “hidden content” (e.g. meta data) in many electronic files, as described above. Content filtering also allows the organization to control incoming and outgoing content for inappropriate statements and subjects. This is a proactive application of DIAC, that can seriously and positively impact risk reduction.

With the advent of electronic content, new models of using content have emerged. The web, for example represents an entirely new channel for business communication, marketing and sales. But, these opportunities require DIAC, lest the organization stumble into unfortunate situations. As previously cited, recently, both United Airlines and USAir have had erroneous flight prices posted to their respective websites, resulting in the need to honor tickets issued at prices that were less than 10% the “actual” fare. E-business requires that processes be established, that use workflow and BPM software to control the creation, approval and posting of content. WCM and DM can be leveraged to ensure content does not become dated, yet still accessible. Potential piracy and plagiarism can be thwarted via content authentication and e-record filing software. ERM and DRM can enable access to intellectual property without whole scale loss of access control. This in turn enables e-based approaches to “paid for” access to content, in a controlled environment, that inhibits the rightful purchaser of the content from sharing the content with others, or having that content modified or stolen from a subscribers less than protected site. In an intra-organizational setting, ERM prohibits employees from sharing content with other departments or product lines that should not have

that access for a variety of reasons. Multi-discipline, multi-national organizations can control how and when internal content is shared within the organization, without infringing any national or industry specific breaches of confidentiality. Data Loss Prevention can inhibit the accidental (or intentional) release of content (both overt and hidden) that perhaps is not subjected to legal/regulatory restrictions, but nonetheless can cause harm to an organization (e.g. the release of marketing plans, recipes and future product development). DIAC technologies such as ERM, DRM, user authenticity and data loss prevention also enable the establishment of *secure* online collaborative environments to support business situations such as product development and M&A negotiations.

Knowledge management is the most tenured of the three business drivers behind DIAC. Despite this momentum, however, DIAC is often not focused on in a knowledge management setting. The technologies that enable and support knowledge management are vast and go well beyond the DIAC genre. DIAC technologies (i.e. content authentication, user authentication, WCM, ERM, workflow and, to a lesser degree, DM), nonetheless offer potential benefit in a knowledge management setting. Appropriately applied, these technologies ensure that relevant and valuable explicit knowledge is properly captured, maintained and shared in an online environment that prohibits the proliferation of unqualified, unofficial and/or unsubstantiated sources of knowledge. Although the direct business value associated with DIAC in knowledge management is not always overtly apparent, organizations should not overlook this need. Accessing and relying on content that has not been approved, is not deemed official or qualified can be very costly – albeit different than doing so in a legal setting or customer facing setting.

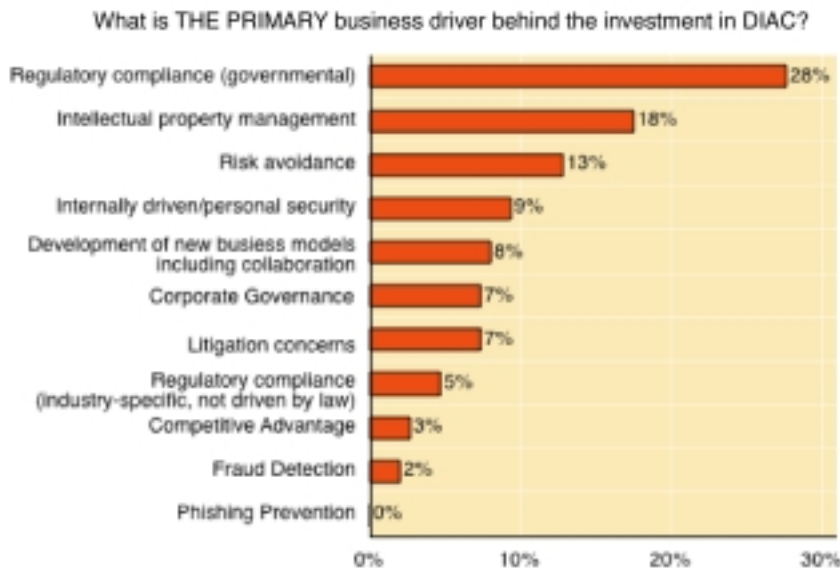
The categorization of DIAC technologies within each business driver setting presented here is of course somewhat generalized. In each case, a detailed business requirement is necessary to explicitly determine which drivers are relevant to the organization, and what facets are behind each driver. This is the topic of the last section of this paper. The point to be made here is that a plethora of point technologies directly address each of the business drivers behind DIAC. There is overlap between the technologies applicable to the different business drivers. Thus, a business case or ROI can be developed not based on a single driver, but across these three drivers.

But, before we look at how such a strategy is developed, our focus shifts to the reality of today's market.

Theory and Practice - In Sync? Or Sunk?

While we may be pontificating on the model of DIAC as a strategic method to address overall content control and management, it is not simply our opinion. Respondents to our 2005 survey (comprised of 458 individuals responding to 22 questions) substantiate the views on DIAC reported here, and lend insight into current and real issues being faced in today's businesses.

With the increase in regulation and legislation of recent years, such as the Sarbanes-Oxley Act of 2002 (SOX) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA), it is no surprise that Regulatory Compliance (governmental) was the top choice amongst the primary business driver choices.



However, while Regulatory Compliance tops the list, with a 28% response rate, it is greatly encouraging to see that “Intellectual Property Management” (IPM) ranked as the second highest response, at 18% and that “Development of new business models including collaboration” was within the top 5 responses at 8% - reflecting what we had previously stated, that the primary drivers for DIAC are compliance/legal, collaboration, and knowledge management. In fact, while many organizations hyper-focus on compliance as a stand-alone issue, we have found that organizations that address the larger issues of IPM and new business opportunities are capable of swiftly (and

with minor modification to existing systems/policies), implementing regulation-specific policies - and this in turn leads to even further strategic thinking around this set of capabilities.

It is worth acknowledging that Knowledge Management was not explicitly identified, nor in the responses hinted at within other choices to this question, and this also harkens to our findings with consulting clients that KM is quite frequently seen as the complete opposite of “being secure” due to the focus on capturing and sharing knowledge/information – although this is a mistaken belief, as we have already discussed.

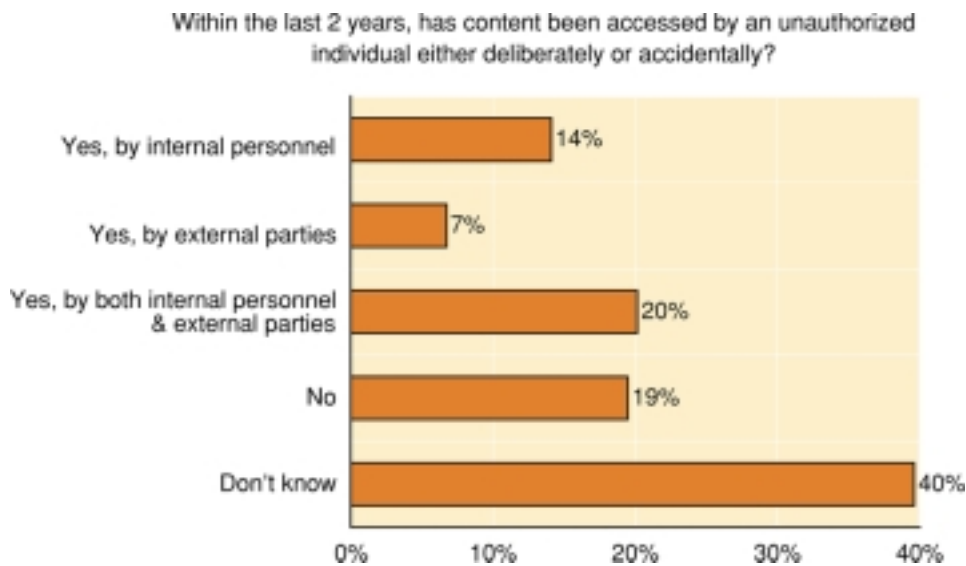
While some feel that, in theory, compliance stands clearly and distinctly alone from all other business concerns, the reality is that the work involved in identifying the content and processes related to compliance efforts is

inexplicably intertwined with other areas for both cost reduction and revenue improvement in nearly any organization.

Are the Threats real? Is a Solution Necessary?

To further discover what was driving interest in DIAC solutions, we examined our survey responses to identify whether there was a discrepancy in how content was being secured against the potential threats, and whether their existing policies and systems were serving them well.

Fully 40% of respondents' companies had no idea whether content had been accessed by an unauthorized person (or person abusing their existing access rights), which is a more honest assessment than most organizations would typically concede to, opting instead for "optimism" or outright denial. 41% of respondents said that internal, external or both internal and external parties had accessed content without authorization. Further, as many classic surveys (such as the oft-cited CSI/FBI surveys) have revealed over the years, the "insider threat" is again being cited twice as often (14%) as the external threat (7%) - such as hackers or crackers.



In total, 81% of respondents have had issues around information leakage/exposure, or have reason to be concerned, not the least of which, because they simply have no idea (such as via an audit trail) what their level of exposure to this threat is, nor confidence in their ability to prevent, detect or react to these issues. Hope, luck or ignorance of a problem cannot really be used as strategies for managing information leakage – clearly there is much work to be done.

In concert with the lack of awareness of whether content has previously been accessed inappropriately, the vast majority of respondents (63%) state that there is no appreciation of the dollar value **risk** associated with unsecured content. In the absence then of a compliance mandate or any other externally required spend to address this area of risk, the tendency on the part of budget holders for these organizations would opt to minimize, and perhaps not spend a single dime on DIAC capabilities – as it would clearly be difficult to balance Return on Investment (ROI) against the range of possibilities of zero risk to infinite risk. Risk Management (Risk Identification and Quantification being the first steps to Managing Risk) continues to play a fairly low role in organizations from our survey respondents point of view, as well as our experiences in directly working with our consulting

clients. As insurance companies and other risk assessors lend their business acumen and actuarial tables to assessing risk of content and content-oriented systems, we should quickly see the appreciation of the dollars associated to this avenue of risk becomes nicely quantified, and as insurers begin to impose standards and financial penalties for lack of compliance with their guidelines, no doubt risk thinking will come into focus with very specifically quantified boundaries.

Unfortunately, lack of understanding of a hard-dollar cost associated with risks that organizations face makes pro-active thinking a rare commodity.

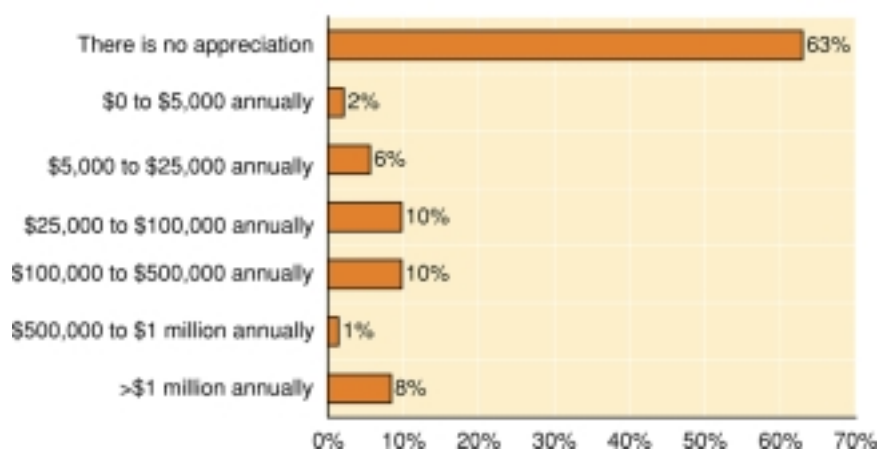
Inevitably, it is not until after a (frequently public) incident arises that money spontaneously appears to solve an incident, and a risk is then quantified, such as US Air, United Airlines, Iron Mountain, Enron, WorldCom, and more every week. Fire fighting is **not** the same as fire prevention, and rebuilding is always more costly than building soundly to begin with.

Building a Business Strategy

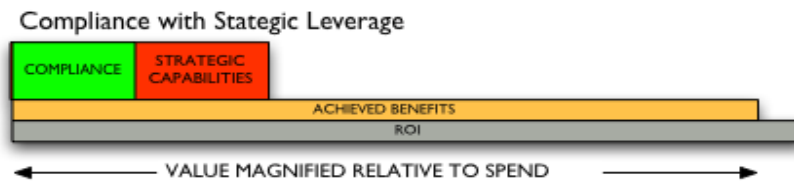
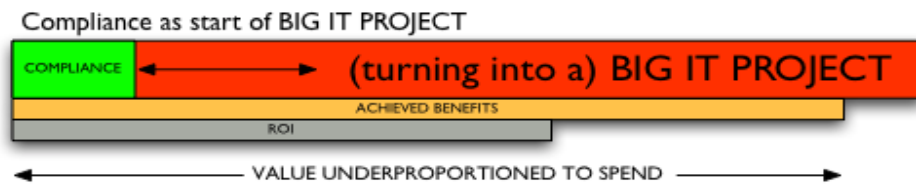
But to simply state that the need for a DIAC program within an organization is a clear and present requirement is not enough. How does an organization get

started? How is such an investment justified? As has been stated throughout this paper, the best approach warrants the formation of a specific strategy that looks at the needs across all user types, content types and business drivers. It has been our experience that when this is done, an investment made in one area can be highly leveraged across other areas, and therein will lie a powerful ROI. The approach taken to meet compliance issues can be leveraged to create new business opportunities, which in turn can fuel the capture and sharing of internal knowledge. If, on the other hand, DIAC is viewed individually – as a way to address compliance, a way to address internal business issues or a way to augment knowledge management, not only will the ROI be seriously diminished, but the resulting solutions will be siloed. The potential for redundant efforts increases and holes in the content control between separate systems becomes a very real threat. This is why we termed the phrase dynamic information access control. The combination of multiple point technologies, used in tandem in an coordinated effort provides more than just a single business solution – more than just security of content. DIAC is lifecycle approach to not only protecting content, but maximizing the value derived from that content, in a manner that exploits the investment in technology across multiple business settings.

Is there an appreciation for the cost associated with the risk of unsecured content in your organization? If so, how great?



Alternative views of strategy around compliance issues



No one answer, the choice for your organization is in the grey area, but compliance is heavy lifting, why not make it do more?



This approach to the development of a DIAC strategy requires a diligent needs assessment across all sources of content across the entire organization. The matrix illustrated to the left is an example of the type of thought process and investigation that should be undertaken. Each content source should be evaluated as to the degree of risk it poses to the organization if it is inappropriately accessed, and/or made available without qualification and tracking. You must determine if the threat this represents is well articulated, understood and if there are current approaches to managing the threat and if these are valid approaches.

		Controls in Place	
		Know	Don't Know
Level of Risk	High Risk		
	Low Risk		
	No Risk		

Moreover, the potential risk posed by access to the content needs to be weighed against the cost and validity of the approach to security and the cost to inhibiting access. Security spending and the degree of security needs to be balanced against the needs of the business to function, not strictly to serve the needs of compliance – overtightening security will merely threaten workers, and by the sheer pressure to “do their job” they will find workarounds to overly zealous security. Ideally, security should transparently support both the worker and the organization, to function in accordance with the overall governing principles of the organization.

The Governance Document and Content Resource Department

The strategy that develops should be viewed as a foundational element to your organization. It must be stressed that the solution goes far beyond investments in technology. Technology is no alternative for sound practices, strong business ethics and a well developed records policy. This requires discipline. DIAC goes beyond records management, although records management is a part of it. Indeed, the real power behind DIAC is the establishment of a clear set of corporate policies and procedures that are augmented and enforced by specific and calculated deployment of appropriate DIAC technology.

The DIAC strategy, including the policies, procedures and technologies deployed should be clearly documented. A Corporate Information Management Governance Document should be authored. This document should be signed by each employee in acknowledgment of awareness and compliance. The governance document should clearly lay out which forms of content are covered by the governance model, the approaches taken for each form of content (i.e. from authoring, to sharing, to destruction), search and discovery models, approaches to rights management, filters that are used, standards being enforced, responsible parties for each facet of the governance and the ramifications of any violation of the governance model.

If the suggested tone of the governance document sounds most serious and foundational – it should. DIAC should not be taken lightly. In fact, we have advised our clients of late that it may warrant the creation of a new department within the organization, a Content Resources Department. For several years businesses have touted the opinion that next to employees, business content/documents are the single greatest asset of the organization. Content embodies a corporation's explicit knowledge and history. Content can be sold or leveraged as a resource (e.g. patents). Content, if mismanaged or ignored can be the demise of the organization. In recognition of this reality, organizations need to establish a Content Resource Department similar in scope and purpose to its Human Resources Department. Similar to a HR department, the CR department should be a centralized entity that sets policy and guidelines regarding how resources are obtained, managed and leveraged across the organization. Similar to HR, CR does not own the resource (in this case content), it is not responsible for its acquisition (authoring), it does not explicitly manage the day-to-day use of the resource, but it sets the policy for acquisition and disposal, sets guidelines for proper handling and serves as a source of authority regarding these centralized policies and procedures.

DIAC is not About Security but Opportunity

In conclusion, with all of this said, it is most important to realize that the proposition being made here is not about security, at least not in the traditional sense. The focus is not just on control in the end but protection, leverage, sharing and increased opportunity.

Traditional approaches to security are founded in a direct relationship between security and access. Under this approach security is a black and white issue. The basic tenet of the perspective is that risk reduction comes at the price of increased security, which by definition limits accessibility. Higher degrees of security (lower risk) are only achieved through decreased sharing or accessible of content.

The Modern Perspective on Security/DIAC is a new perspective on security and access to content. With increased granularity on the levels of security and the ability to have security travel with the content, as the levels of control are increased, so too is the ability to securely share or collaborate in creative new ways. Understanding this new paradigm represents a new realm of opportunities for deriving value from content without compromising the organization or putting it at risk.

About the Authors

Carl Frappaolo is co-founder of Delphi Group and heads up its business consulting practice. Carl has over 23 years of experience working with a broad array of technologies including knowledge and content management, search engines, document management, workflow, imaging, intranets and portals. Valued for his technical, practical and market expertise, he has consulted with a variety of organizations spanning multiple industries including: The City of San Diego, Pfizer, The City of Boston, Lockheed Martin, ING, Affinity Insurance Group, Las Vegas Valley Water Authority, American Express, Apple Computer, CoreStates Bank, the State of Washington, The Clorox Company, IBM, AT&T, Air France, Perkins Coie, Federal Reserve Bank of New York, Nabisco and The World Bank. He serves on the board of the Electronic Document Systems Foundation. Mr. Frappaolo has been recognized by AIIM International (the Association for Information and Image Management) as a *Master of Information Technology* and as an *Information Systems Laureate*, and in 2000, was bestowed the *Distinguished Service Award* by AIIM.

Mr. Dan Keldsen is a Senior Analyst/Consultant as well as Delphi's Chief Technology Officer. He evaluates and directs the implementation of new technologies to streamline Delphi's efforts in fulfilling client and employee information technology needs. Dan has consulted with organizations such as ProMutual, Fannie Mae, Pfizer, Alcoa, Stratify, Teragram, Great West Life and Parent McLaughlin & Nagle CPAs. Mr. Keldsen is well versed in the issues associated with web content management, security systems (encryption, filtering, firewalls, intrusion, detection prevention, managed services), content creation/posting, performance measurement methodology, web and network analytics, content distribution and syndication networks and tagging/classification. Dan serves on the Advisory Board for the SANS GSEC (GIAC Security Essentials Certification) program and is a member of the Usability Professionals' Association (UPA) and AIFIA (Asilomar Institute for Information Architecture).