

## **Compliance Integrated Infrastructure**

by Thomas Bookwalter, CEO FMDC

### **What Is Compliance Integrated Infrastructure<sup>SM</sup>?**

Compliance Integrated Infrastructure<sup>SM</sup> (CII<sup>SM</sup>) is an integrated solution to enterprise storage and information management requirements. CII is a combination of storage, information security systems, regulatory profiling and records management policies and procedures designed to protect enterprise value. CII meets the need to minimize storage costs while addressing the requirements for regulatory records management, litigation support and the protection of enterprise information assets. CII is implemented in a way that eliminates the need for costly and disruptive “compliance point solutions” that exist outside the standard operating environment of the enterprise.

### **Why Is Compliance Integrated Infrastructure<sup>SM</sup> Important?**

CII is important because it reduces the cost and operational impact of protecting enterprise records and meeting the information management requirements of security, regulatory compliance and litigation readiness.

The volume of electronically stored information is increasing at a startling pace. Additionally, the percentage of a company’s overall records that are stored electronically increases steadily. At the same time, both the courts and the regulators are establishing new standards for information access and integrity. Companies are faced with new requirements for scalability, security and access.

So far, most attempts to meet these requirements have focused on isolated stand-alone or point solutions. These solutions are not only costly, but also temporary at best. They create extra work. They require separate skills to support. Many require their own back-up solution. They operate outside the general day-to-day IT operational framework. Some are stopgap measures that do not scale well and will have to be re-engineered. Many were implemented in a “compliance panic” created by regulations such as Sarbanes-Oxley and SEC Rule 17a-4. These solutions do not mitigate costs they exacerbate them.

Compliance Integrated Infrastructure<sup>SM</sup> addresses the problem head-on. The final solution incorporates:

- Disaster recovery to support business continuity;
- Information Life Cycle Management (ILM) to maximize storage cost savings;
- Scalable storage architecture to meet growing data storage requirements;
- Information Security to protect corporate information assets and sensitive customer data;
- Tamperproof storage to ensure data integrity;
- Regulatory records management for enterprise-wide compliance;
- Compliance review of IT Change to ensure continuing regulatory integrity

## PROTECTING ENTERPRISE VALUE

### #2. Compliance Integrated Infrastructure

- Intelligent archiving to facilitate record retrieval and reduce the cost of litigation support and regulatory inquiry

#### **How is Compliance Integrated Infrastructure<sup>SM</sup> Different from Disaster Recovery?**

Disaster Recovery is just one aspect of CII<sup>SM</sup>. It addresses the need to make sure that the enterprise can quickly recover from interruptions to its IT operations. Disaster Recovery solutions are focused on a very specific function, systems continuity. Disaster Recovery is an overly expensive solution for long-term data retention and regulatory compliance. Companies have been fined millions of dollars for using DR tapes to meet regulatory retention requirements. The failure of DR as a data retention and retrieval strategy is its inability to implement additional data management functionality required by regulators.

CII incorporates Disaster Recovery as a critical element in the overall infrastructure. The difference is that CII relies on DR for disaster recovery and not for regulatory records management. Other elements of CII are integrated in the overall solution in order meet the needs of the business to protect its information assets and to meet its regulatory and legal obligations.

#### **How Is Compliance Integrated Infrastructure<sup>SM</sup> Implemented?**

Compliance Integrated Infrastructure<sup>SM</sup> is implemented through a structured methodology that follows six steps:

- Assess regulatory jurisdictions to determine the regulations that apply to your company in all of its business units and locations
- Define the IT functional specifications necessary to meet both regulatory and business requirements
- Design the infrastructure that integrates necessary network, hardware and software to protect your data and your company
- Deploy solutions that leverage existing systems, minimizes future costs and streamlines operations
- Enable organizations and their people to use the solutions to best advantage
- Optimize and refine the solutions to improve economy and performance and adapt to ever changing requirements

#### *Regulatory Assessment*

CII begins with the Regulatory Profile<sup>SM</sup> of the enterprise. The profile defines the regulatory records management requirements of the enterprise. In the days of physical records management when documents were kept in boxes in storage rooms and warehouses, individual departments and offices were responsible for their own document retention. General enterprise guidelines were created and people at each location were expected to adapt those guidelines to their own specific needs and manage their own records. It made no sense to consolidate those records.

## PROTECTING ENTERPRISE VALUE

### #2. Compliance Integrated Infrastructure

The proliferation of electronically stored data and the trend to electronic data discovery has changed that. Central data stores reduce the cost of access and increase the ability of the enterprise to protect its data and itself from the careless and selfish acts of misguided employees. Further, the central storage of the information enables the enterprise to respond to litigation and investigation quickly and at minimal cost.

The starting point for enterprise-wide records management is with the Regulatory Profile. Get the profile right and the enterprise can better protect itself from information risk and liability.

#### *IT Functional Specifications Definition*

The regulatory requirements are combined with your business requirements to create a complete information management requirements definition. These requirements are then translated into the IT functional specifications needed to address the needs defined in the requirements.

Regulatory management of electronic records is new to many enterprises. The first inclination is to apply the retention schedules of the paper records to the electronic records. That is only a partial solution. It is a solution that can be both costly and full of risk. Regulators and litigators have quickly learned that electronic records have very different forensic qualities from physical records and must be managed differently. CII addresses those differences. Retention alone is no longer enough. Electronics records must be managed to a different standard. CII implementations meet that standard.

Regulations are often vague and imprecise. The result is difficulty in determining the IT functionality needed to properly manage and protect the information. This is further complicated by the fact that many regulations focus on the same data. The IT functional specification process deals with the vagaries created by the regulations and translates them into a set of network, hardware, information security and software specifications that when implemented will meet the requirements of all the regulations. These specifications form the criteria for the design of the Compliance Integrated Infrastructure. These same specifications are used in the evaluation and implementation of the specific network, hardware and software elements.

#### *Solution Design*

The Design of the Compliance Integrated Infrastructure combines many elements. The elements specifically address the requirements for information management that includes:

- Accessibility
- Change management
- Confidentiality
- Continuity
- Economy
- Integrity
- Retrieval
- Scalability
- Security

## PROTECTING ENTERPRISE VALUE

### #2. Compliance Integrated Infrastructure

The design integrates policy, procedure, and proof with network, hardware and software products created to facilitate managing large stores of information to today's information management standards.

A key principle in the development of the CII is to leverage existing technology investment. While changes may need to be made, the best design will minimize the cost and disruption by using as much of the existing infrastructure as possible. Whenever the technologies that are already installed at the enterprise meet the requirements of the IT functionality they will be an element of the final design.

When complete, the design will identify the network, hardware and software elements of the infrastructure. The criteria for each element will be based on the requirements in the IT functional specification.

#### *Solution Deployment*

Once the design is finalized, deployment follows. Network, hardware and software components are evaluated against the functional specifications to ensure that the design meets the requirements. As a part of the deployment, detailed project plans are developed to ensure that continuous operation is minimally disrupted. Once approved, ACS works with enterprise personnel to complete the implementation. As a final deployment step of each phase of the deployment, the installed elements are tested for compliance with the IT functional specifications.

#### *Enablement*

More than most systems, CII is closely linked to enterprise policies and procedures. In order for the solution to properly serve the enterprise people must not only understand the workings of the systems but must also clearly understand the policies, procedures, practices and proofs that govern their use.

ACS works with its enterprise clients to ensure that users are fully trained in the systems and that IT fully understands the legal and regulatory framework that surround the CII.

#### *Optimization*

Optimization is an ongoing effort to fine tune the CII for best performance and economy. The regulated records management environment is dynamic. New regulations, new products, new geographic markets, new software, new hardware and new network components all converge in the CII. The result is the constant need to refine and adapt the system to meet changing compliance requirements. Formal processes for the compliance review of any change to the environment are an integral part of the solution. Regular periodic reviews that examine the system, its performance and its ability to address regulatory demands are also a part of the optimization process.

The intent of the CII is to provide the fundamental infrastructure that will support the security of information of an enterprise related to compliance, confidentiality, litigation and the protection of enterprise information assets. Properly designed and implemented, the CII makes compliance manageable.

## PROTECTING ENTERPRISE VALUE

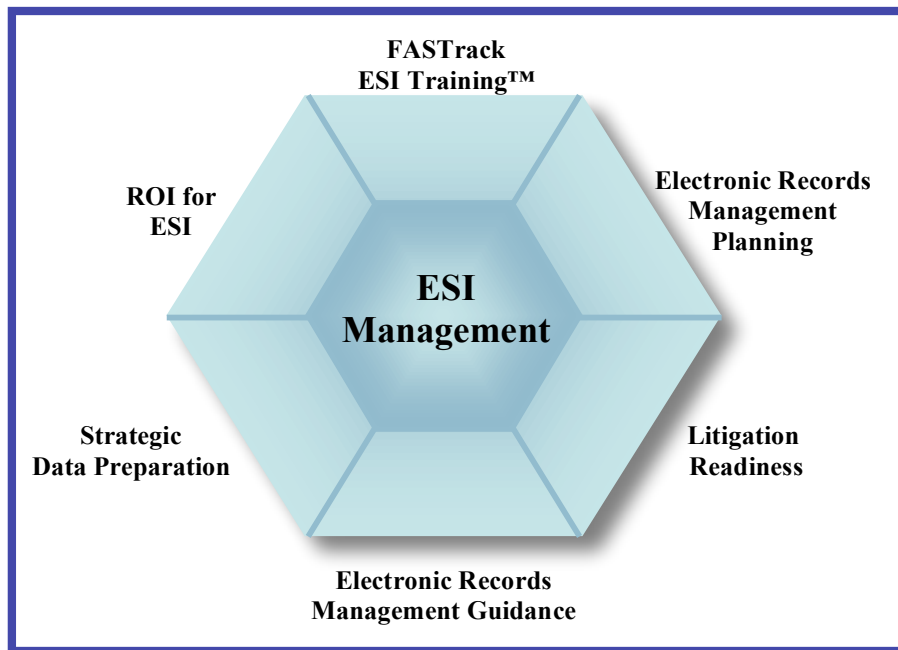
### #2. Compliance Integrated Infrastructure

#### About FMDC

Founded in 1987, FMDC has focused on the issues relating to the processing and management of information in regulated environments. Since its inception, FMDC has been at the nexus of regulation, industry and information technology. With projects in over twenty countries, FMDC professionals have gained first hand knowledge of the nuances of the different regulatory jurisdictions and how they impact the use of technology. In early 2002, FMDC turned its attention to the issues relating to the handling of e-mail, instant messaging and other records in the context of regulatory requirements and litigation.

The advent of laws and rules such as SEC Rule 17a-4, the Sarbanes Oxley Act, State and Federal privacy legislation, industry standards such as PCIDSS and most recently, court rules or guidelines such as FRCP, CCJ-ED, local federal district rules and the Sedona Conference has changed the standards by which companies must manage their information. FMDC professionals work to guide companies through the morass of regulations to find cost effective solutions for the management of ESI. Our services include:

- FASTrack ESI Training™
- Electronic Records Management Guidance and Policy Development
- Strategic Data Preparation
- Litigation Readiness
- ROI for ESI
- Electronic Records Management Planning



If you are concerned about ensuring that your ESI management meets your business, litigation and regulatory obligations or if you must find ways to reduce the associated costs contact FMDC.

#### Western US Region

Joseph Santoro, VP  
Newport Beach, CA  
949 231-9602

[joseph.santoro@fmdc.com](mailto:joseph.santoro@fmdc.com)

#### CEO

Thomas Bookwalter  
Santa Fe, NM  
908 812-5000

[thomas.bookwalter@fmdc.com](mailto:thomas.bookwalter@fmdc.com)

#### Eastern US Region

Michael Shope, VP  
Middletown, NJ  
732 687-2680

[michael.shope@fmdc.com](mailto:michael.shope@fmdc.com)