



NEWS RELEASE

FOR IMMEDIATE RELEASE

CONTACT AGENCY:
Judy Smith
JPR Communications
818-884-8282
judys@jprcom.com

CONTACT DIGITILITI:
Ken Peters
Executive Vice President
651-925-3200
kpeters@digitiliti.com

Tech Alert: Eight Tips on an Information Management Strategy for Regulatory Compliance

ST. PAUL, Minn., November 4, 2010 – The increasing emphasis on corporate and financial accountability at the federal and state levels should motivate all companies to evaluate their ability to protect and manage potentially sensitive information, say experts at [Digitiliti, Inc.](#) (OTC: DIGI), a pioneer and technology leader in the Information Management business.

Here are eight tips for developing an information management strategy to meet regulatory compliance.

1. Know what compliance laws/regulations apply to your company. Legal departments, chief financial officers and/or chief information officers should know what compliance laws and regulations apply. These may include Sarbanes-Oxley (SOX), Gramm-Leach Bliley Act (GLBA), Health Information Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standards (PCI), Federal Rules of Civil Procedure (FRCP), Federal Information Security Management Act (FISMA), the Patriot Act, and/or regulations from agencies such as the SEC, NASD and NYSE.

2. Know what data has to be protected. Each regulation identifies what type of data has to be protected. In some cases only data identified as sensitive or private is affected, so not every department or PC may require the same degree of data control and security.

3. Conduct a full Risk Assessment. This can be done internally, or through an outside security consultant, to identify vulnerabilities that will impact the organization's ability to meet requirements for information management and compliance. In conjunction with the Risk Assessment, you need to conduct an enterprise-wide Data Assessment to identify and locate where sensitive data resides, how much is there and what the data is. You cannot secure your data until you know where it is.

4. Identify the Data Flow. Once you have identified where the data is, you need to document the data flow. In all work environments, there is an "official flow" and an "unofficial flow." How people go about getting their jobs done doesn't necessarily conform to who is on the organizational charts, or what is written in company policies. Data flow factors include who creates the data and has access to it; when the data is created, stored, accessed, and disposed of; where the data resides, both at rest and where it goes when in motion; how business processes and workflows use the data; and why the data was needed, is currently needed, or will be needed in the future.

5. Design, budget, schedule, and implement the network security architecture.

The network security plan will be based on the risk and data assessment, data flow, and any applicable policies, both internally defined company policies and externally defined regulatory policies. Basic ideas are available from sources such as the U.S. Department of Commerce's [National Institute of Standards and Technology \(NIST\)](#) as well as the individual regulatory acts. Forklift upgrades will likely require the approval of senior management and possibly affected department heads, and the timeline for implementation may need to be adjusted accordingly.

6. Use tools for discovery/search/archive/hold/alert/audit. A good information management system is needed to meet requirements for discovery retention, search/e-discovery, and disposal of sensitive information. It should include tools that proactively identify documents containing sensitive information anywhere on the network, including the desktops, and "hold" capabilities to prevent disposal schedules from removing

critical information if litigation is pending. It should also provide automatic alerts when data is somewhere it's not supposed to be, and can run data audits and detailed reports on the data status if required by law and for the auditors.

7. Use tools for backup/disaster recovery. A Rock-solid information management system does not eliminate the need for backup and recovery. The archiving capabilities in the information management system will show a history of the files, where they existed, when they existed and who created/changed them. Backup systems do not do this but they are necessary to enable the recovery of lost, corrupted, or damaged files and can provide bare metal restores of desktops, servers and data bases. You really should have both a backup/disaster recovery and information management system.

8. Document/Monitor/Test/Train. Create and update the Security Policy Document for the compliance regulations. Auditors first look to see if you have a security policy document covering the compliance rules. They are looking to see if you are following what you have written down. Say what you do in the document and then do what you say. First time the auditor finds a process not in the policy document, you are in for a long audit. You will always have to monitor and test your secure network. Networks, and the people connected in the network, are dynamic and are always creating change. Not to mention the bad guys outside your network. Invest in some good vulnerability tools and consider contracting out for a security service to do an external and internal security audit at least twice a year. Finally, train the people who handle the sensitive data on the security policies. This is another area an auditor will look at-do the people handling the data know what the rules are!

Digitiliti's [DigiLIBE™](#) is a simple-to-use system designed to protect the confidentiality, integrity, availability of data from its point of origin to final disposition. All user data is captured at the point of origin and becomes a unique DigiLIBE Information Object. The Information Object contains a uniform set of metadata and preserves the integrity of the data-essential elements for compliance and timely business decisions. The Information Object is indexed, cataloged, encrypted and stored in a Virtual Corporate Library further

protecting the confidentiality, integrity, availability of corporate data. DigiLIBE also provides essential data and information management capabilities such as eDiscovery, email and auto-desktop archiving, global deduplication, content indexing, retention management, local storage, compression, encryption and long-term archiving. DigiLIBE has three simple components – Workstation Clients, Information Director, and the cloud based Archive Information Store, DigiLIBE reduces the number of disparate IT products needed, and the complexity and costs involved with managing your information growth.

A flash presentation is available at:

<http://www.digitiliti.com/index.php/solutions/digilibe.html>.

About Digitiliti Inc:

Digitiliti develops and provides advanced Information Management solutions that address the cost, complexity, and compliance problems associated with controlling and utilizing unstructured data. Digitiliti provides enterprise-class products and services that are easy to use, cost effective and always deliver the right information, to the right people, at the right time helping them make informed business decisions. Digitiliti services include DigiBAK™, a complete offsite data protection/backup solution, and DigiLIBE, a single integrated information management solution that allows customers to extract and use the valuable business knowledge hidden in their unstructured content. Digitiliti markets and sells solutions solely through its worldwide network of channel partners. For more information please visit

<http://www.digitiliti.com>.

###