



The Iam Lotus User Group

The eDiscovery Primer for Lotus Domino Admins

**Bill Malchisky Jr.
Effective Software Solutions, LLC**

© 2010 by the individual speaker



What We'll Cover ...

- **Introduction**
- **Laying the planning foundation**
- **Important Facets of Journaling and Compliance**
- **Options Impact Technical Planning**
- **Time-saving tips and techniques**
- **Advanced Compliance Measures**
- **Wrap-up**

Speaker Info – BillMal Your Lotus Pal

- **Working with Notes since 3.0c, in 1993**
- **Architect, admin, auditor, trainer, process engineer, team lead; “reformed” developer**
- **Co-authored two IBM Redbooks on Linux**
- **Multiple Lotus Certifications**
- **Frequent speaker: Lotusphere, THE VIEW events, and LUGs**
- **Significant regulatory compliance and Domino specialty project experience**

Disclaimer

- **All information in this session is provided as is. You are free to use it within your organization, and plan internally with no express written or other implied warranties. No one connected with this webinar is responsible for your environment. If there are any questions on the points presented herein, seek the advice of your corporate legal department. Use at your own risk and you accept all responsibility for doing so.**

Completing Your Evaluations ...

- **Please ensure that you fill-in your on-line session evaluation form**
- **Thank you in advance**

What We'll Cover ...

- Introduction
- **Laying the planning foundation**
- Important Facets of Journaling and Compliance
- Options Impact Technical Planning
- Time-saving tips and techniques
- Advanced Compliance Measures
- Wrap-up

Five Easy Steps to a Great Plan

1. What's our time horizon?

2. Meeting with company legal team to obtain compliance requirements

- ◆ Everyone's favorite meeting! :)

3. Determine your technical needs

- ◆ Journaling vs. archiving
 - ▶ Determine if/when to use journaling
 - ▶ Is it needed for disclosure motion response?
 - *A key defense strategy*

4. Identify project team members

5. Execution strategy

Ensure Your Team Comprehends The Timeline

- **Lawsuit imminent**
 - ◊ **Shorter timeline**
 - ▶ **Perhaps a multi-part implementation**
 - ▶ **Phase I – Complete enough to satisfy request**
 - ▶ **Phase II – Implement Best Practice solutions**
 - ◊ **Avoid purging any data for in-scope people**
- **Preventive maintenance mode**
 - ◊ **Longer timeline**
 - ◊ **Data purging within regulation confines outlined by your company legal team**

The Successful Team Lineup

- **Ensure you have responsible parties dedicated to your firm's success**
 - ♦ Key journal system implementation facet
- **Who's on the team?**
 - ♦ Compliance Officer
 - ♦ Security Officer
 - ♦ Domino Admin
 - ♦ Legal Team Representative
 - ♦ Backup Team Contact (if not Admin)
 - ♦ Network Admin
 - ♦ System Admin

Note: Company size dictates the team size

Technical Components Utilized

- **Backup**
- **Retention**
- **Restoration**
- **Data management process**
- **Testing each component at predefined intervals with a reasonable frequency is paramount to success**
- **Audit**
 - ◊ **Ensure all parts work consistently going forward**
- **Solution must cover all requirements**
 - ◊ **Multiple vendors and products possible**

Success Tip: Frequent Training is Key

- **Never inform your staff of the policy only once**
 - ◊ Update routinely
 - ◊ One errant task can cost millions
- **CIO/CTO's should embrace the K.I.S.S. method**
 - ◊ Steps to make sure compliance to the company records' retention policy is easy
 - ◊ Provides better end-user adherence over what robust and complex offerings yield
 - ◊ If it takes more than a few seconds to handle sensitive data, it will be managed improperly/inconsistently

Trust But Verify

- **Just because you have a drink or watch baseball with other team members...**
 - ◊ ...Does not mean they will support you when you need them
- **Corporate case-study: Legal response project**
 - ◊ Performed daily server backups
 - ◊ But no restores, till I arrived
 - ◊ Why?
 - ▶ “Our service level is to backup the servers”
 - ▶ “We have no service level for restores”
 - ◊ Result: 200k unmarked tapes arrived on-site
 - *How is that for a first day on a new project*

What We'll Cover ...

- Introduction
- Laying the planning foundation
- **Important Facets of Journaling and Compliance**
- Options Impact Technical Planning
- Time-saving tips and techniques
- Advanced Compliance Measures
- Wrap-up

Compliance Can Force Data Management Policy

- **Compliance Drivers**
 - ♦ Corporate litigation
 - ♦ Intensified scrutiny of financials
 - ♦ Scandals
- **Courts refuse to accept non-compliance excuses**
 - ♦ “It will take us too long to complete”
 - ♦ “It will be too expensive to provide”
 - ♦ “We don't have all the required data”
- **Motivation is where you find it**
 - ♦ Failure to provide full information disclosure may introduce significant fines or imprisonment
 - ▶ **Local laws and infraction severity can vary**

Should Your Firm Be Concerned?

- **Investigations typically call upon these four verticals**
 - ♦ Financial
 - ♦ Legal
 - ♦ Accounting
 - ♦ Insurance
- **And the rest?**
 - ♦ Any firm's client can be investigated
 - ♦ Courts follow the trail during an investigation
 - ▶ **Non-regulated verticals can be in-scope if the case warrants such action**
 - *If your firm is unable or unwilling to respond, life can get interesting very quickly*

Steps to Protect Yourself

- **The best defense is a good offense**
 - ◊ Although I eschew clichés, it is fitting
- **Compliance: not just e-mail data management**
 - ◊ Text messages
 - ◊ Calendar events
 - ◊ Instant messaging data
 - ◊ Mobile equipment
- **Protection components**
 - ◊ Message journaling
 - ◊ Backups
 - ◊ Full and complete data management strategy

The Two Most Common Recent Regulations

- **HIPAA (Health Insurance Portability and Accountability Act)**
 - ♦ **Pub. L. 104-191 [HIPAA], enacted 1996**
 - ♦ **Title I: Health Care Access, Portability, and Renewability**
 - ♦ **Title II: Preventing Health Care Fraud and Abuse; Administration Simplification; Liability Reform**
 - ♦ **<http://www.hhs.gov/ocr/privacy>**

The Two Most Common Recent Regulations (cont.)

- **SOX (Sarbanes-Oxley)**
 - ◊ Pub. L. 107-204, 116 Stat. 745, enacted 2002
 - ◊ Enhances corporate financial responsibility
 - ◊ Federally mandated best practices
 - ▶ Disaster recovery
 - ▶ Data protection
 - ▶ Storage management pertaining specifically to sensitive data
 - ◊ <http://www.sec.gov/about/laws.shtml>

That's Not All...

- **Each industry presents its own set of unique regulations**
 - ◆ Financial firms need to track books and records
 - ▶ **Outside of SOX**
 - ◆ Food preparation firms require safe handling
 - ◆ Chemical firms introduce toxic waste management
 - ▶ **Environmental regulations**
 - ◆ Manufacturing firms machinery is in-scope
- **Each regulation must be audit-proof**
 - ◆ Born is the internal auditor
 - ◆ Works with the Legal department
- **Non-technical regulations can be technical**
 - ◆ Where is the data stored?

Your Federal Requirements: Know Them

- **Data Storage Duration**
 - ◊ SOX: 5 year minimum for all accounting and audit records
 - ◊ HIPAA: 6 year minimum for all health records
- **Change Management: a critical success factor**
 - ◊ Ensure your firm handles change volatility
 - ◊ Inter-team communication is critical to success
 - ◊ Communicate with Legal Team liaison quarterly
 - ▶ **Exchange/receive any IT-appropriate updates**
 - *Act upon all plan modifications*
 - *Implement before the need becomes a crisis*
 - ◊ This simple procedure can reduce dramatically the risk of impromptu 80+ hour implementations

Corporate Safety Net: Journaling Messages

- **Archiving does not equate to journaling**
- **So, what is journaling?**
 - ♦ Captures e-mail transmissions
 - ♦ Storage via a digital safe
 - ♦ Located apart from in-scope end-users' mail files
 - ♦ Unavailable to the end-user
 - ♦ Scales for individuals, group, server, or entire company
 - ♦ Unless informed, users never know of existence
- **Multiple location preferences**
 - ♦ Domino server
 - ♦ Remote storage area, such as an appliance

I Thought That Was Archiving?

- **Actually, archiving takes messages out the primary database and places them into a separate data store**
- **Generally on a slower filesystem**
 - ◆ Keeps down costs
- **Archive file is accessible by the end-users**
- **Allows for deletion**
- **Cost-cutting play**
 - ◆ Most recently used messages in the primary mail file
 - ◆ Least recently used mail in the archive
 - ◆ Generally increases server-side performance

Data Mining Tools Provide Little Compliance Risk Reduction

- **They utilize a mail file for their target DB**
- **Search mail after-the-fact**
- **Provide powerful data extraction capability**
- **End-user can edit or purge messages before the manual capture/search agent executes**
 - ♦ **Makes it compliance adverse**
- **Best served for managing an archive, rather than a compliance-oriented task**
- **Know your tools**
 - ♦ **Mail archiving and related tools: Controlling end-user mail files**
 - ♦ **Journaling tools: Recording and reporting messaging transactions**

The Many Forms of Routed Mail

- **Routed mail sources**
 - ◆ Lotus Notes clients
 - ◆ Lotus iNotes
 - ◆ Lotus Domino application agents
 - ◆ External or internal SMTP servers
 - ◆ Mobile mail conduits
- **Real-time management programs couple tightly with proper journaling tools**
 - ◆ Ensure all message types flowing into, out-of, or within a Domino server are captured
 - ◆ Immediately the digital vault stores messages

Capture and Extraction: Journaling's Two Sides

- **Capturing made better through Lotus**
 - ◊ Domino offers a decent native journaling tool
 - ▶ **Included with the core server product**
 - ◊ Provides a real-time management program
 - ◊ Automatic naming rollover
 - ◊ Pre-defined naming convention
 - ▶ **Allows for better storage management**
 - ▶ **Can off-load older journals to new storage area**
 - ◊ But, the extraction tool is slightly less robust
- **Extraction search tools**
 - ◊ Look at journal(s), returning matching messages
 - ◊ Select appropriate message(s) from return set
 - ◊ Package results into court acceptable format

How eDiscovery Tools Operate May Not Be Obvious Initially

Know your tool requirements before implementation

- ◆ Some utilize Domino journaling task
 - ▶ Avoids re-creating a journaling capability
 - ▶ Offset with a more elegant search tool
- ◆ Others prefer to replace the Domino capability
 - ▶ More common with appliance setups

Real-Time Message Management Benefits

- **Stop content delivery capability**
- **Keep a message internal**
 - ◊ If subject or body contains a word or phrase of interest
- **Message body filtering**
 - ◊ Pattern matching included
 - ◊ Regardless of the message's source, if it hits a Domino box, the real-time engine captures and measures the message against your pre-defined criteria or filters
 - ◊ Failures are handled by the respective filter's action

What We'll Cover ...

- Introduction
- Laying the planning foundation
- Important Facets of Journaling and Compliance
- **Options Impact Technical Planning**
- Time-saving tips and techniques
- Advanced Compliance Measures
- Wrap-up

Critical Success Factor: Obtaining Basic Requirements

- **You really do need a plan**
 - ◊ Too many teams implement the “Just do it” project execution methodology and hope for the best
 - ▶ “We need to get this done,” is quite common
 - ◊ Planless = recipe for cost overruns
 - ▶ Worst-case is a pending disaster
- **Mandatory input: Legal**
 - ◊ But as new details emerge, decisions can change
 - ▶ Document all decisions agreed upon
 - ▶ Version your notes after each change
 - ▶ Ensures you are protected and covered
 - *Internally and in a court proceeding*

Poor Planning Has a Price

- **Project deliverables are as good as the time you commit upfront for thorough planning**
- **If you lack a good eDiscovery process model, expect to burn cash quickly**
 - ♦ Observed many firms spend tens to hundreds of thousands of dollars—per request—for disclosure motion responses
 - ♦ Ad-hoc execution drives up costs, wastes employee time, and introduces team frustration
- **It can be operational: roll-out a good model**
 - ♦ Drops associated costs markedly
 - ♦ Avoids any legal business liability for failing to comply
 - ▶ **Untimely response can incur significant costs**

Considering Multiple Journals?

- **When to use multiple journals**
 - ♦ More complex legal requirements
 - ♦ Involved in multiple court-ordered disclosure responses or investigations
 - ♦ When responses have unique timelines or person(s) to monitor, apart from the primary journal (which is generally company-wide)
- **Ensure your search and capture tools allows for multiple journals**
 - ♦ Simplifies overall process

Multiple Journals: Usage Scenario

- **Usual path**
 - ◊ Search the primary journal database for a 30-day window for user11
 - ▶ **User might not have been in-scope originally**
 - ▶ **Can increase response time for larger firms**
- **Improved path**
 - ◊ Add a new journal specifically for user11
 - ◊ Populate said journal during the capture window
 - ◊ Provide resulting file to legal
 - ▶ **Quickly and easily satisfies their requirement**
 - ◊ Saves you time and impresses the attorneys for quick turn-around

Planning Ahead Yields Cost Saves

If there is even a small chance of performing specialty captures or sub-set groupings

- ♦ You will want to plan for that now
- ♦ Always ensure that whatever your selected tool provides, it can still scale to meet future needs

The Three Journaling Model Types

- **Appliance**
 - ◊ Stand-alone network add-on, stores messages in a digital safe
- **Domino**
 - ◊ Tools and capabilities included with your license
- **Third-party on-server journaling models**

Appliance Journaling Insight

- **The stand-alone unit**
 - ◊ Insert into your network
 - ◊ Designed for larger enterprises or verticals that incur significant paper needs
 - ◊ Does not alter your Domino configuration per se
- **Each Domino box needs a hook**
 - ◊ Causes mail.box to route a message copy to the digital safe
 - ◊ May need Corporate approval for this configuration enhancement
 - ▶ **Company policy may prevent altering the default installation of any server-product**

Appliance Journaling: Design Consideration

- **Understand that this architecture will significantly increase traffic**
 - ◊ The appliance takes a copy of each message and routes it to the appliance
 - ◊ If you have 100+ Domino servers, on a saturated LAN...
 - ▶ **Imagine the calls you will receive**
- **Failing to account for this side-effect can bring your network to its knees in heavy messaging environments**

The Lotus Approach — Domino Journaling

- **Lotus provides a native journaling feature**
 - ◊ **Easy to setup**
 - ▶ **Just edit the respective server(s') Configuration Settings document's Journaling tab's fields**
- **Two installation styles**
 - ◊ **Mail-in DB mail destination option**
 - ▶ **Sends a message copy to the target server**
 - ▶ **Becomes a simplified appliance**
 - ◊ **Local journal**
 - ▶ **Zero increased traffic**
 - ▶ **Routes message to a local journal on the same server**

Design Considerations for Domino Journaling

- **Normal Domino backups will include the journal**
- **Special care may be required**
 - ◊ Mail-in database or multiple journal databases
 - ◊ Consider this option carefully
- **The strength of your extraction tool determines how effective retrieving messages becomes**
 - ◊ Enabling roll-over for your journals does not equate a multiple journal setup
 - ▶ **Different than having two files capturing mail from different sources**
 - ▶ **If you have multiple journals, you should be able to search them**

Third-Party On-Server Journaling Perspective

- **Two usage styles:**
 - ◊ **Domino's journaling service**
 - ▶ **Provide a better front-end**
 - ▶ **Enhances filtering and retrieval**
 - ◊ **Their own journaling task and database structure**
 - ▶ **Tool installs easily without disturbing your existing Domino infrastructure**
 - ▶ **Better tools allow you to simply append their task name to the ServerTasks= line**
 - *Turn off the native Domino task*
 - *Configure your settings and filters*

Third-Party: Design Considerations

- **Several independent on-server journaling models utilize real-time management techniques**
- **Provides increased filtering by inspecting the message before the mail.box receives the message**
- **Additional design considerations are vendor specific**

A Good Retrieval Tool Makes a Good Journal

- **Third-party tools shine here**
 - ◊ Ability to acquire data, regardless of search criteria is a critical success factor
 - ◊ Draft a few of the more complex searches you might need and see if your tool holds-up
 - ▶ **A good test in evaluating products**
- **Searching across multiple databases is key**
 - ◊ Effective tools search across all your journals
 - ◊ Allow specific people to monitor subsets of files
- **The best tools allow for complex extractions**
 - ◊ Ensures you meet tough legal requirements or requests

What We'll Cover ...

- Introduction
- Laying the planning foundation
- Important Facets of Journaling and Compliance
- Options Impact Technical Planning
- Time-saving tips and techniques
- Advanced Compliance Measures
- Wrap-up

Journaling Worst Practices

- **Utilizing a message journal repository to perform:**
 - ◊ Message recalls
 - ◊ End-user message restores
 - ◊ DB recovery operations
- **Using the admin ID for journal access**
 - ◊ Always set up a separate mail journal user
 - ◊ Best Practice – Maximizes security
 - ▶ Create and register a special user ID for the Mail Journaling database
 - ▶ Assign multiple passwords
 - ▶ Distribute passwords so that no one person knows them all
 - ▶ Ensures the consent of multiple parties is required to view the contents of the database

One Practice to Consider Avoiding

- **Avoid alerting all end-users to its existence**
 - ◊ Only a select few should know of its existence
 - ▶ **Legal**
 - ▶ **IT Department and Corporate Management**
 - ◊ Otherwise the calls for restores come quickly
 - ◊ Alerting end-users of its existence is situational and falls into company culture in many cases
- **Business justification example:**
 - ◊ Person suspected of nefarious activities
 - ▶ **Best to not alert the subject**
 - ▶ **You can accurately prove/disprove without bias/malice for the concerned activities**

Domino Journaling ID Access Safeguards

- **Domino journaling preserves the user ID in the ACL with any journal file rollovers**
- **But, if you remove the Mail Journaling database, during the next restart:**
 - ◊ **Domino creates a new journal DB**
 - ◊ **Then inherits the ACL from journal.ntf file**
- **Want to avoid being potentially locked-out?**
 - ◊ **Always place the special user ID utilized for encryption in square brackets within the ACL**
 - ◊ **Domino automatically adds this ID value in each successive journal DB created**

Journaling and DAOS Burn Protection

- **During backups, always ensure you capture:**
 - ◊ The attachment repository
 - ◊ Archived journal(s)
- **Covers you for restore and retrieval operations**
 - ▶ **Otherwise you will learn — the hard way — a new definition of pain**

Capture “All Data”: What Does It Really Mean?

- **If you think you want to journal every document that passes through your mail.box, guess again**
 - ◊ **Monitoring messages can fill up a journal fast**
 - ▶ **Forces frequent roll-overs**
 - ▶ **Increases backup costs, needlessly**
 - ▶ **Increases search response times**
- **Journal filters are very important**
 - ◊ **ISpy messages normally are captured**
 - ▶ **Create exception rule for the “Ispy” sender**
 - ◊ **Create an exception to avoid capturing DFRs**
 - ▶ **The original message is in the DB**
 - ▶ **If the user re-sends it, you will capture that message too**

Domino and Third-party Journaling Solutions

- **When utilizing a secondary tool for journaling**
 - ◊ **Disable the Domino journaling service**
 - ▶ **But a few vendors may specifically use the service, so double check**
 - ◊ **Competing journaling services**
 - ▶ **Can cause daily-run issues**
 - ▶ **Worst-case providing an incomplete data set provided to a court**
- **When using an appliance solution ...**
 - ◊ **Team discussions typically breach digital safe backup within the appliance**
 - ▶ **Can we run a backup? If so, how?**
 - ◊ **Ensure the vendor approach meshes well with your risk assessment and company culture**

Specific Information Regarding Backup Procedures and Issue Avoidance

- **Review backup reports on a pre-determined but regular and consistent frequency to ensure confidence**
 - ◊ Sometimes backup teams know of missed backups but do not disclose unless asked
 - ▶ **It is imperative that all journaled data outside of an appliance is backed-up reliably**
- **Know your message retention requirements**
 - ◊ Mail file and backups may be different
 - ◊ Key for planning and physical storage needs
 - ◊ Disaster recovery plans must be included

Some Clients Think They Are Fine, Until...

- **Real-world example**

- ◊ Assisted a firm that implemented a backup tape recycle at 60 days, violating SOX
 - ▶ They began storing these tapes for five years
- ◊ Discussions around where to store “all these tapes for an additional 58 months — each”
 - ▶ Capacity increased from hundreds of tapes to recycle to thousands
- ◊ Quickly exceeded their off-site storage capacity
- ◊ New budget considerations introduced
 - ▶ Tape increases
 - ▶ New SANs to handle on-site restoration needs

Capacity Planning, By the Numbers

- **Looking at the previous example...**
 - ◊ **Such a change will impact internal operations**
 - ▶ **Present state**
 - *25 tapes per night to handle a backup*
 - Presuming full backups nightly
 - *Multiply by 60 days = 1,500 tapes*
 - ▶ **Future state**
 - *Minimal growth and five years of storage*
 - *Tape inventory = 45,650 tapes*
 - Recall that within a five-year window you will have at least one leap year
 - *Some industries require seven years*
 - Equates to 63,900 tapes

What About Restoration Factor?

- **Ensure that you are able to properly pull data from any stored backup tapes at any time**
- **Pull random tapes from all archived backups**
 - ♦ **Ensure your system can read the tapes and properly restore files**
 - ♦ **Although tedious, it is absolutely critical to ensure compliance**
 - ♦ **Record any tapes that fail**
 - ▶ **Inform Legal**
 - ▶ **Ascertain your solution/work-around for those data set(s)**
 - ▶ **Plan to prevent the dilemma going forward**
 - ♦ **Failure to succeed here can be very expensive**

Final Tips

- **Reduce backup requirements and thresholds**
 - ◊ Utilize Domino 8.5.x with ODS51
 - ▶ Design compression
 - ▶ Document compression
 - ▶ LZ1 attachment compression
 - ◊ All combined can save tens of GBs per server
- **Bit of redundancy here, but...**
 - ◊ Be certain to include your disaster recovery (DR) site into your journaling and compliance requirements
 - ▶ Ensure business continuity during a disaster

A Positive Side-Effect from Compliance

- An effective setup can be utilized to remove doubt or misplace ill will against a colleague
- Real-world example
 - ◆ Client asked that I research mail activities for a suspected security breach
 - ◆ For the areas of my concern, the Domino environment allowed for unequivocal suspicion removal
 - ▶ Person did nothing wrong, but falsely accused

That level of proof is very powerful and ensures that persons of interest avoid any lingering cloud of suspicion that can damage team morale long term

What We'll Cover ...

- Introduction
- Laying the planning foundation
- Important Facets of Journaling and Compliance
- Options Impact Technical Planning
- Time-saving tips and techniques
- **Advanced Compliance Measures**
- Wrap-up

Safeguarding Domino from Internal Threats

The Need:

- ♦ Some firms have the desire to safe guard their DBs and respective documents
- ♦ Domino is great with security, but document-level change history may not provide enough information for your needs
- ♦ Sensitive databases may have increased projection requirements
 - ▶ Internal auditors may mandate field-level data and author change history
- ♦ Government agencies, top-secret projects; internal traders, merger & acquisition teams (behind the wall)

The Fix: Developers to the Rescue

- **Fortunately, Domino offers an excellent API**
 - ◆ Lotus provides the capability to take security to the next level, without impeding application workflow usage
 - ◆ Good solutions couple cohesively with the Domino security model
 - ◆ Flexibility in what and how much protection you need
- **Ensure the development team is on-board with your requirements**
 - ◆ They can enhance any application's audit features
 - ◆ If Management's needs exceed the resource availability or capability of internal talent, seek third-party/ISV solutions

Nod to the Coders...

- **Reduce, Reuse, Recycle...**

- ◊ **Once you determine your increased audit requirements:**

- ▶ **Make the team aware of the new development enhancements**
- ▶ **Put code modules in a script library**
- ▶ **Usage decreases development timelines**
- ▶ **Admins should test special attention apps**
 - *Refuse to deploy if app fails to meet basic requirements*
 - *You need to know what's on your network*
 - *Important to determine that the special app you manage satisfies Legal/Audit*

Areas of Concern: More Than Many Realize

- **Domino Directory**
 - ♦ Who keeps creating rep/save conflict docs?
 - ♦ Determining the right level of control
- **Notes.ini**
 - ♦ Tracking edits, date-time stamps
- **Mission critical/high-visibility applications**
 - ♦ Finding corporate data being printed against policy
 - ♦ More advanced agent log statistics
 - ♦ Longer ACL change list requirements
- **Intrusion detection**
 - ♦ Internal accessing attempts to off-limits areas
- **User activity beyond Notes user activity**

Logging the Concerns

- **Once you decide to take the advanced steps to protect your environment...**
 - ◆ Need to locate warning signs easily
 - ◆ It is hardly adequate just to capture data, you have to use it
 - ▶ **Recall the unmarked backup tapes example presenter earlier...**
- **Powerful capture system lets you find what you need**
 - ◆ Capture data in areas of concern
 - ◆ Statistics can provide data mining capabilities
 - ▶ **Eye-opening situations are generally revealed with a deeper cut of one's environment**
 - ▶ **The answers are usually there, but unseen**

What We'll Cover ...

- **Introduction**
- **Laying the planning foundation**
- **Important Facets of Journaling and Compliance**
- **Options Impact Technical Planning**
- **Time-saving tips and techniques**
- **Advanced Compliance Measures**
- **Wrap-up**

Resources

- www.ibm.com/developerworks/rational/library/sep05/cancilla-bennet
 - ◊ IT Responses to Sarbanes-Oxley
- http://searchdomino.techtarget.com/generic/0,295582,sid4_gci1321695,00.html
 - ◊ IT Governance in an IBM Lotus Software Environment
- http://searchdomino.techtarget.com/news/article/0,289142,sid4_gci1222736,00.html
 - ◊ IM, Blogs Next Target for Litigation

Contact Info



How to contact me:

Bill Malchisky Jr.

Bill@BillMal.com

Blog: www.BillMal.com

Follow me on Twitter: [BillMalchisky](#)

AIM, Skype, Y!: [FairTaxBill](#)