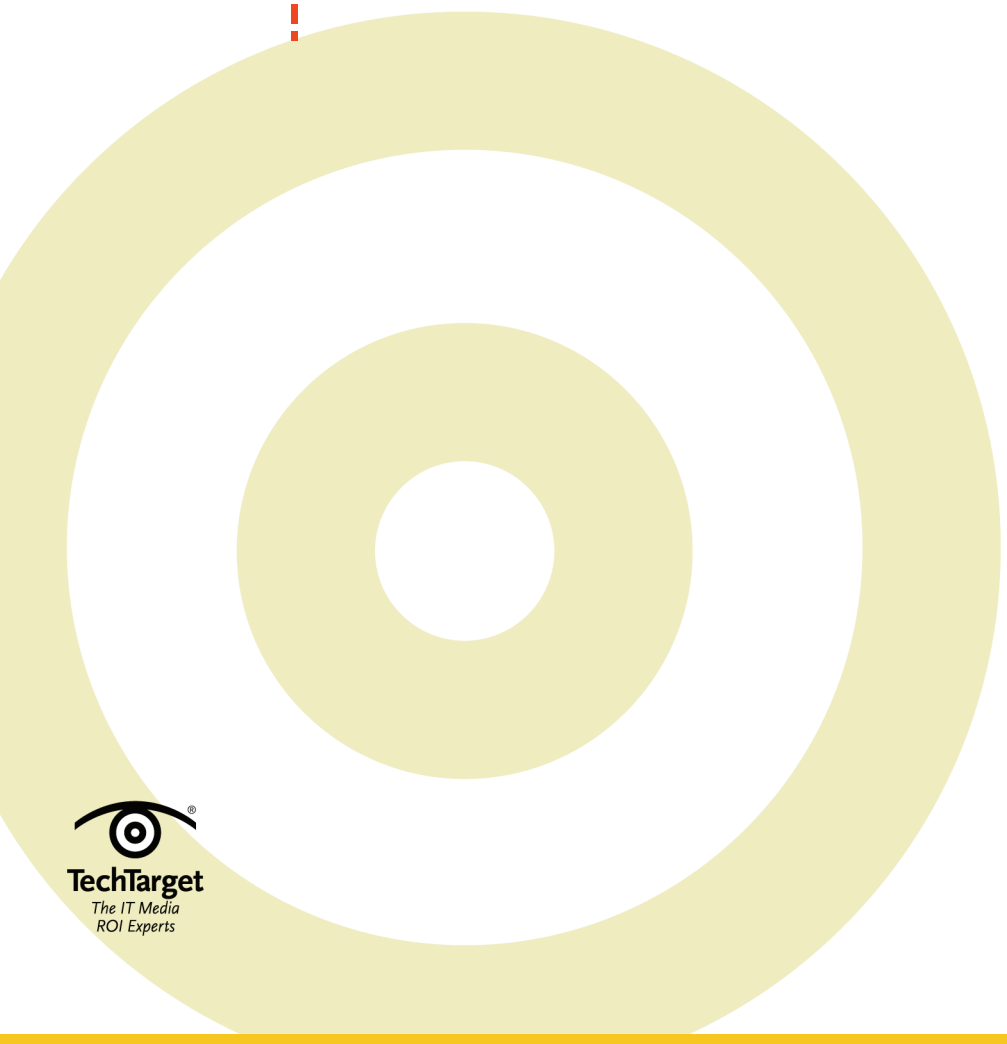
An *IT Briefing* produced by SearchDomino.com

IT Governance in an IBM Lotus Software Environment



TechTarget
The IT Media ROI Experts

Sponsored By: SHERPA SOFTWARE

IT Governance in an IBM Lotus Software Environment

This *IT Briefing* is based on a Sherpa Software/TechTarget Webcast, "IT Governance in an IBM Lotus Software Environment."

This TechTarget *IT Briefing* covers the following topics:

About Sherpa Software

Sherpa Software solutions provide extensive e-mail management, archiving, policy enforcement, and content filtering capabilities to companies addressing issues relating to storage management, content discovery, and compliance. For more information, visit www.sherpasoftware.com.

About TechTarget *IT Briefings*

TechTarget *IT Briefings* provide the pertinent information that senior-level IT executives and managers need to make educated purchasing decisions. Originating from our industry-leading Vendor Connection and Expert Webcasts, TechTarget-produced *IT Briefings* turn Webcasts into easy-to-follow technical briefs, similar to white papers.

For inquiries and additional information, contact:
Dennis Shiao
Director of Product Management, Webcasts
dshiao@techtarget.com

IT Governance in an IBM Lotus Software Environment

When an organization has a strong IT governance focus, it can address any compliance issues that may arise. From a governance perspective, this document describes:

- Concepts and definitions for governance
- Elements of governance
- Distinguishing myth from reality
- Approaches that go beyond "just good enough"
- Control frameworks
- Information systems control frameworks for IBM Lotus software environments

Concepts and Definitions for Governance

At the highest level, "governance" is the setting of objectives, tone, policies, risk appetite, and accountabilities, as well as performance monitoring. Governance is a matter of who is allowed to make the decisions, who is enabled to make decisions, and who is accountable for those decisions once they are made.

Risk Management

What are the risks? Can the organization identify them? Can the organization assess these risks, and do they present a challenge in meeting that organization's objectives? How does an organization determine its response, strategies, and control activities to those risks?

Risk management includes identifying and assessing risks that might affect the ability to achieve objectives and determining risk response strategies and control activities. Many times, risks are difficult to quantify and identify, but they always exist.

Compliance

"Compliance" refers not only to laws and regulations (such as the Sarbanes-Oxley Act of 2002) but also to internal policies and procedures, as well as considering an organization's commitments to its stakeholders. Are the stakeholders other employees? Are they vendors? Are they suppliers? Are they Board members? When people think about compliance, they tend to think about Sarbanes-Oxley and may think compliance does not apply to their organization.

Elements of Governance

Compliance can have an impact on an organization at many different levels, which is why it is important to talk about governance and how the elements of governance can lead an organization to have the ability to comply. At the corporate level, governance focuses on ensuring that the policies, practices, and procedures of a corporation are legal and ethical and that they support stated business goals and objectives.

An organization should consider its business goals and objectives. What are the overall goals and objectives? Does the organization have policies, practices, and procedures? The organization should consider legal issues, ethical issues, and anything that will support that organization in achieving its goals and objectives. The idea of governance is to have a win-win situation for everyone.

IS/IT Governance

For most organizations, regarding information systems (IS) or information technology (IT) governance, consider these basic questions:

- Are information systems being acquired, deployed, and maintained in support of specific, measurable objectives?
- Are the systems being used for the purposes intended?
- Is there a disciplined approach to the management of information system assets, including personnel?

Personal Governance

Governance does not just apply to policies and procedures for equipment. It also applies to the human

nature and the human touch. How do we manage our personnel? How do we govern them? How do we enable them to do the jobs with which we charge them and hold them accountable for their decisions and actions?

With regard to personal governance, there are also some basic questions to consider:

- What are individual employees—including administrators, developers, or managers—doing to support business objectives?
- Are the employees behaving ethically?
- Are the employees putting the company at risk?

More specifically, are any employees sharing information with unauthorized instant-messaging systems or free Web-based e-mails? Are they sending information over which the organization has no control? What do the employees specifically do? They need to realize that they are an important key to governance.

Distinguishing Myth from Reality

An organization's long-standing policy is not always the policy that should be in place. For example, if a policy has been in place for 20 years, consider how technology has changed in the past 20 years. That policy may not work today and it may be a false assumption to work under a policy that is 20 years old.

Some organizations choose a policy because it works for another company, but just because it works for one company does not mean it will work for another. The two companies may have a different operating environment. They may have different systems. It is not a good approach to generalize from one company to another. Each organization must look at its own unique situation.

Some organizations make decisions based on information read in a technical bulletin or alert. It is important to consider where that information was read or who provided it. Was the information really in a technical bulletin? Was it in an alert? Was it published? Or was it false information provided by a vendor who is trying to drum up business? No one should depend on what other people have read or said.

Do not follow documentation without questioning its content. Software documentation can be inadequate or incomplete or it can fail to address what the user needs to know. Documentation cannot always be trusted.

Some organizations decide to turn off filters in an effort to prevent a server crash. However, problems can arise when filters are turned off.

Any organization that works in a multinational environment needs to be aware of the laws of other countries, specifically in the area of privacy. What are the laws of those countries in terms of employee e-mail? In the United States, the presumption is that e-mail is owned by the company. In other countries, e-mail often belongs to the individual. How can an organization set its policies and governance procedures to respect the laws of other countries?

Some organizations use the excuse of making no changes simply because of habit. Times change, technology changes, and people change—and organizations need to adapt to those changes.

Also, just because someone (including auditors) makes a statement does not mean that statement is true or accurate. For example, discussion forums or IT auditors may claim that the Sarbanes-Oxley Act of 2002 requires something specific, but that is not true. Sarbanes-Oxley does not demand specific requirements. Section 404 states that organizations must have specific controls, but it does not say what those controls should be. Therefore, when an auditor or someone else claims that Sarbanes-Oxley requires something specific, remember that it requires organizations to *address* risks and controls.

When someone talks about Sarbanes-Oxley dictating policies and procedures, do not be afraid to push back. If an organization has controls in place that are thought out and documented, that organization has no need to worry.

CEOs often present a problem, because they do not follow their own company policies. Is this a myth or reality? Unfortunately, for many organizations this is a reality. CEOs say one thing and do another. They act as if the rules apply to everybody but them. That can cause organizations a lot of trouble.

HIPAA specifies health care rules in terms of what they do and do not allow people to say. For example, suppose someone states that a hospitalized

employee cannot notify clergy because of HIPAA. This is not true. It is important to be very clear in regulations and rules about what they do and do not specify, rather what people can and cannot do.

Should technology drive policy? Absolutely not. Policies should always be driven by business risk, business assessment, and risk assessment. Let the policy drive the technology—not the reverse—because the technology will not always fit the individual needs of a company.

Approaches That Go Beyond "Just Good Enough"

It is important for organizations to go beyond "just good enough" approaches, because what is "good enough" today may not be "good enough" tomorrow. This is a very important point: If organizations continue to do business based on hearsay, old practices, or undocumented practices, this can put individuals and the company at risk.

Furthermore, if the organization fails to perform due diligence into exactly what *is* required, it may be putting its employees and the company at risk. This can lead to a situation in which the organization does not have the best opportunity to succeed. The solution exists and if the organization performs due diligence, it will find that solution.

Learn from the Mistakes of Others

It is important to learn from other people's mistakes. Do the research, talk to people, and find out what has and has not worked for them. For example, in the case of a Domino environment that has experienced failure, ask why that failure happened. One of the best examples of learning from others is Paul Mooney's and Bill Buchan's "Worst Practices" sessions at Lotusphere—these sessions are about real mistakes that people have made.

Do Not Run a Business in Silos

It is very important that an organization does not run its business in silos. Taking a silo-based approach to governance and compliance can lead, for example, to dealing with HIPAA one week and Sarbanes-Oxley the next. In other words, this approach is a constant knee-jerk reaction. Organizations cannot approach governance in a silo-based manner.

The best study on this topic is Redmonk's document, "Compliance Oriented Architecture," which describes a more holistic approach. When an organization puts a strong IT governance architecture in place, new rules or laws are not an issue because the organization can respond effectively and efficiently. An organization should have an architecture in place that safely addresses issues and risks, and then move on.

Do Not Hesitate to Invest in Resources to Reduce Risk or Protect Assets

If the organization needs to spend resources to reduce risk or protect its assets, it should not be afraid to do so. Do not be "penny-wise and pound-foolish." If an organization believes it cannot afford to spend money on a firewall or archiving, it should consider the money required to address a future lawsuit or other issue. Will that organization spend more in the future than on making an investment today? What is the return on the investment?

The Need for Strong IT Governance

It is very important to realize that information technology—particularly Lotus technology—is so embedded in the operations of the enterprise that strong IT governance is needed to support corporate governance objectives and compliance requirements. For example, some people believe that e-mail is not an essential system. But what will happen if e-mail goes down? E-mail and instant messaging are mission critical systems. People tend not to think about these systems until they are not available. If an organization has strong governance procedures in place, its risk of these systems going down is reduced.

But the question is, how can this be accomplished? What can an organization do to have strong governance for its Lotus environment or IBM software environment?

Control Frameworks

The topic of control frameworks is very detailed. This document provides an overview of control frameworks, as well as links for more information.

Why should an organization have a control framework? Organizations need to build a control framework for strong IT governance to support clear business objectives. If a business objective is not being met or identified, a control framework is not necessary. Decisions

need to be reflect business objectives and the framework selected needs to address that, as well.

Strategic IT objectives should align with defined business goals and objectives. To achieve a specific goal, a specific IT objective needs to happen. For example, suppose the goal is to communicate effectively with an organization's customers. The IT objectives are:

- The Lotus Notes e-mail system must be up and running 99.9% of the time.
- The organization must have clustering in place.
- Disaster recovery must be in place.

Objectives from the IT level must also meet the business objectives.

Implementation of a control framework does not happen overnight; it is a very lengthy process. An organization can start small. It should not expect to have everything in place right away. This process requires assessment, development, deployment, training, and education.

IBM and Lotus Software professionals who understand control frameworks at a high level will make themselves more valuable members of the IT governance team. An organization has the option of hiring outside administrators or developers but they do not bring business value to the team.

Control Frameworks that Support Compliance and Governance

Two well-defined frameworks are available that support compliance and governance:

- COBIT (Control Objectives for Information and Related Technologies)
- ITIL (the Information Technology Infrastructure Library), which is intended for a support function of service desk calls and an up-time type of environment

Understanding COBIT

This document focuses at a high level on COBIT, because this is a very detailed topic. COBIT has been developed as a generally applicable and accepted standard for good IT security and control practices. Financial auditors talk about GAAP (Generally Accepted Accounting Principles) and GAAS (Generally Accepted Auditing Standards). If an organization is in the financial world and has GAAP and GAAS, that organization is in good shape. Auditors will comment that everything is fine. This is equivalent to the IT governance world. If an organization has COBIT in place, IT auditors will perceive that organization as having strong governance in place, because COBIT is the de facto international standard for information technology controls.

COBIT provides a reference framework for:

- Management
- Users
- IS audit, control, and security practitioners

It is a well-defined written framework and helps employees perform their jobs. COBIT contains high-level and detailed control objectives. It walks an organization through control objectives about documenting a system and applications.

As an example, how many people can say they have an updated position description for their job? COBIT puts procedures in place to make sure that each job description is current and that employee's responsibilities are reflected.

Information Systems Control Frameworks for IBM Lotus Software Environments

How can the topic of information systems control frameworks be considered for an IBM Lotus Software environment? IBM Lotus Software performs many tasks in many places. This software includes IBM Lotus Notes, IBM Lotus Domino, IBM Lotus Sametime, and IBM Lotus Quickr. Consider how all of this software is set up and how people are using it, because these tools all have unique but common governance requirements.

In an IBM Lotus Software environment, control frameworks should include:

- Acceptable use policies
- E-mail retention policies
- Instant message retention policies
- Record retention policies
- User creation policies

- User termination policies
- Naming conventions and standards
- Group creation, naming, and management
- Server security policies
- Server configuration documentation
- Segregation of duties (administrator versus developer)
- Application development environment
- Application development standards
- Approval authorities

For example, suppose an organization assumes that Lotus Sametime is being used in an acceptable way. But if a problem is reported and it seems as if Sametime is being misused, that organization might be tempted to shut down Sametime. This is probably not an appropriate response. A better idea is to monitor Sametime to find out how it is being used.

Organizations have retention policies. Do they have to require retained e-mail? Do they have to require retaining instant message transcripts? The answer to these questions will depend on the organization's environment and on how the organization is using the tools. How long that organization should retain these messages is driven by those requirements.

What is record? How long should the organization keep it? Consider user creation policies. What is the organization's procedure for training a user? What is its procedure for terminating a user? Is this documented? Who initiates it: Human Resources? IT? The key is having all this information documented.

It is frustrating to work with an organization that has no naming conventions or standards. This will cause problems down the road.

It is important to consider that the employees who understand an organization's server configuration should document that information in case of an emergency. The documentation should explain the rationale and the decision making behind each setting.

Administrators should not be doing development work and vice versa. In a large environment, that may be easier to accomplish. When a company employs hundreds of thousands of people, it is easy to separate duties. But smaller organizations may have only one or two people to perform the same duties that many employees perform at a large corporation. How is it possible to document the organization's procedures in a way that separates these duties, minimizes the risk, but also recognizes that these duties sometimes overlap?

What is the application development environment like? Does the organization have a development environment? Does it have a test environment? Or are employees developing, testing, and deploying on production servers? This is a very high-risk approach. Can the organization afford the software needed? Can the organization afford the hardware? Does the organization have the staff to support it?

The same issue is true for application development standards. Does the organization have standards that it follows for deploying Domino applications? If the organization does not have standards, then it is reinventing the wheel. How can an organization put standards in place, for example, for using code libraries or script libraries? Having standards for naming a field fosters communication, as well. Developers can talk with developers through code and documentation. Otherwise, a developer could inherit an application and be frustrated because there is no evidence for why the code was written in a certain way.

Who are the approval authorities; in other words, who is responsible for approving applications? Who can approve external Sametime users, and so on? The list is long and that is why this is not an overnight process.

The Importance of Managing the IBM Lotus Software Environment

This is a key issue: If the organization does not manage its IBM Lotus Software environment, that organization will never have full control over the environment. It is necessary to take control. That does not mean dictating everything that will happen. Instead, it is important to talk to decision makers and have effective communications about managing the environment. But remember, people do not think of Lotus Software as being critical until it is not available. When problems arise, it is difficult to manage the situation—administrators and developers will work 10 times harder. On the other hand, if an organization has controls and procedures in place, the job of an administrator or developer is 10 times easier.

How can an organization understand its IBM Lotus Software environment? The answer is to use control self-assessments.

Control Self-Assessments

Using control self-assessment means meeting with an internal team, an external team, or maybe a combination of the two teams to look at what the organization has, the IBM Lotus Software that has been deployed, and how it is documented and managed. The goal is to uncover problems before the auditors or management has the opportunity to find those problems. Taking this action demonstrates proactive management of the organization's system. This may be difficult because of everyone's daily workload. It is necessary to approach management and get a commitment from them.

The goal is to create the control environment before the organization's management or auditors dictate the environment.

For More Information

To learn more, visit the following recommended reference sites:

- The IT Governance Institute, which publishes COBIT: http://www.itgi.org/
- The Information Systems Audit and Control Association (ISACA): http://www.isaca.org/
- Andre Guirard's "Best Practice Makes Perfect" blog describes best practice for application development: http://www-10.lotus.com/ldd/bpmpblog.nsf
- The Business Controls Caddy: http://www.controlscaddy.com/

Another recommendation is to consider becoming a certified auditor or a certified security professional from ISACA. This provides additional credentials and knowledge to help employees do their jobs better.

Summary

IT governance not only creates accountability and establishes decision-making processes, it also helps an organization manage its environment in an easier way. Do not be afraid of the term "governance to compliance," because it can help rather than hinder. Published and peer-reviewed control frameworks will make the task easier. COBIT is published and available. ITIL is published and available. These are both very good tools. Control self-assessments help identify risks earlier and mitigate them faster. The value of a control self-assessment is enormous. Using this approach puts a company miles ahead of many other organizations. Organizations should not be afraid of IT governance. It will help employees perform better and it will make their lives easier. Given limited resources and a tight economy, employees should make themselves as valuable as possible to their employers.

Let Sherpa Software Be Your Guide

Key to successfully executing internal controls and governance is the management of the electronic information stored within your systems. However, implementing policies and actions that support IT initiatives while satisfying compliance requirements can prove to be a challenging, uphill climb for any IT manager. Why go at it alone? Sherpa Software solutions offer control frameworks that allow you to archive information, enforce management policies, enforce legal holds, and control user activities to satisfy the requirements you are addressing today and put the proper frameworks into preparing your information for future initiatives.

Sherpa Software products manage information within Lotus Notes e-mail, instant message (IM) logs, and files stored on users' hard drives or Domino servers.

Enterprise Wide Policy Enforcement

It is essential that companies know more about the information stored within their systems than ever before. In order to comply with internal and external requirements, companies need to have a clear understanding of the breadth and the depth of their information stores and establish archiving/retention/preservation policies. Equally important are taking measures to delete e-mails, attachments, and files that are not relevant or not necessary. Purging excess information can limit your organization's risk and reduce the time and effort involved in searching information for a future e-discovery inquiry.

Sherpa Software's solutions allow you to define broad or granular policies that can manage the entire life cycle of information by dictating what information

needs to be retained, what should be deleted, where information will be preserved, how long it will be maintained, and so on. Policies can be enforced by multiple criteria including name, keyword, date, and size with actions such as archive, delete, copy, and report. When executed properly, these policies can address current internal governance and external compliance requirements while proactively preparing your information for future regulatory requirements and discovery inquests.

Information Archiving

A critical aspect of policy enforcement is the preservation of corporate knowledge, which is usually accomplished through an archiving strategy. Archiving enables organizations to move or copy business records from live information stores into a centralized location for safekeeping. Increased storage limitations, government regulations, and potential legal implications have made archiving not only a good business practice but a necessary one.

Whether the information you want to archive is in the Domino Journal, in Lotus Notes mail files, on user hard drives, or within IM logs, Sherpa's archiving solutions can successfully use customizable criteria to nominate documents for the archive. Once secured, messages and attachments can be single-instanced to reduce storage, data can be encrypted for increased security, and retention policies can be enforced to purge archived records upon their expiration.

Real-Time Archiving/ Management

In addition to managing the information that exists within data stores, it is important that controls be in place to capture inbound/outbound messages before they are routed and to block potentially hazardous communications from entering or exiting your organization. By auditing a message as it enters your environment, managers can assess and remove potential liabilities, thereby reducing your risk exposure.

Sherpa Software offers real-time auditing and capture capabilities that allow you to have fine-tuned control over all sent and received messages in the mail environment. Messages are captured before they are routed, allowing you to collect, quarantine, archive, or disclaim messages in response to risk management and compliance rules. With real-time controls in place, companies can reduce their legal exposure and comply with increasingly stringent industry regulations, government legislation, and internal compliance polices.

Legal Hold and User Controls

Since e-mail is owned by the company, it is critical that e-mail users protect corporate knowledge and conduct business in the best interests of the company. One employee's discretion can have a disastrous affect on the company's well-being and future. With the amount of critical information passing through the corporate e-mail system, companies must take measures to protect themselves from potential risks.

Sherpa Software solutions allow you to protect intellectual assets by enforcing controls over what employees can send, edit, or delete. Through activity and creation restrictions, corporate officers can use specific criteria such as keywords, recipients, size, and subject line to prevent an employee from deleting or editing documents in their e-mail files. The same criteria can also be applied to stop employees from saving or sending inappropriate content. Domains to which an employee can send information can also be limited.

Taking proactive steps to monitor and manage information is vital. However, litigation can be hard to avoid. If an outside legal request is received or anticipated, information must be preserved and suspended from further management actions. Sherpa Software products can lock information in place and create a hold for later review. Through Sherpa's location and legal hold abilities, companies can save precious time and resources by not requiring manual searches of disparate information throughout the environment.

Reduce Risks and Address Compliance Requirements with Sherpa Software

For over 10 years, Sherpa Software has been providing award-winning software specifically designed to address e-mail management, archiving, e-discovery and compliance requirements for Lotus Notes and Microsoft Exchange environments. Sherpa's products are reasonably priced for organizations of all sizes and are designed to streamline administrative processes while taking advantage of internal systems and architectures.

You wouldn't tackle Mount Everest without the help of a Sherpa, so why tackle IT governance and compliance without Sherpa Software? Our products for Lotus Notes include Compliance Attender, Mail Attender, File Attender, and Discovery Attender. For detailed product descriptions, free white papers, and evaluation versions, visit www.sherpasoftware.com or call 1-800-255-5155 to speak with a Sherpa Software sales representative.

About TechTarget

We deliver the information IT pros need to be successful.

TechTarget publishes targeted media that address your need for information and resources. Our network of technology-specific Web sites gives enterprise IT professionals access to experts and peers, original content, and links to relevant information from across the Internet. Our events give you access to vendor-neutral, expert commentary and advice on the issues and challenges you face daily. Our magazines give you in-depth analysis and guidance on the critical IT decisions you face. Practical technical advice and expert insights are distributed via specialized e-Newsletters, video TechTalks, podcasts, blogs, and wikis. Our Webcasts allow IT pros to ask questions of technical experts.

What makes TechTarget unique?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events, the expert interaction of Webcasts, the laser-targeting of e-Newsletters, and the richness and depth of our print media to create compelling and actionable information for enterprise IT professionals.

Sherpa_11_2008_0005