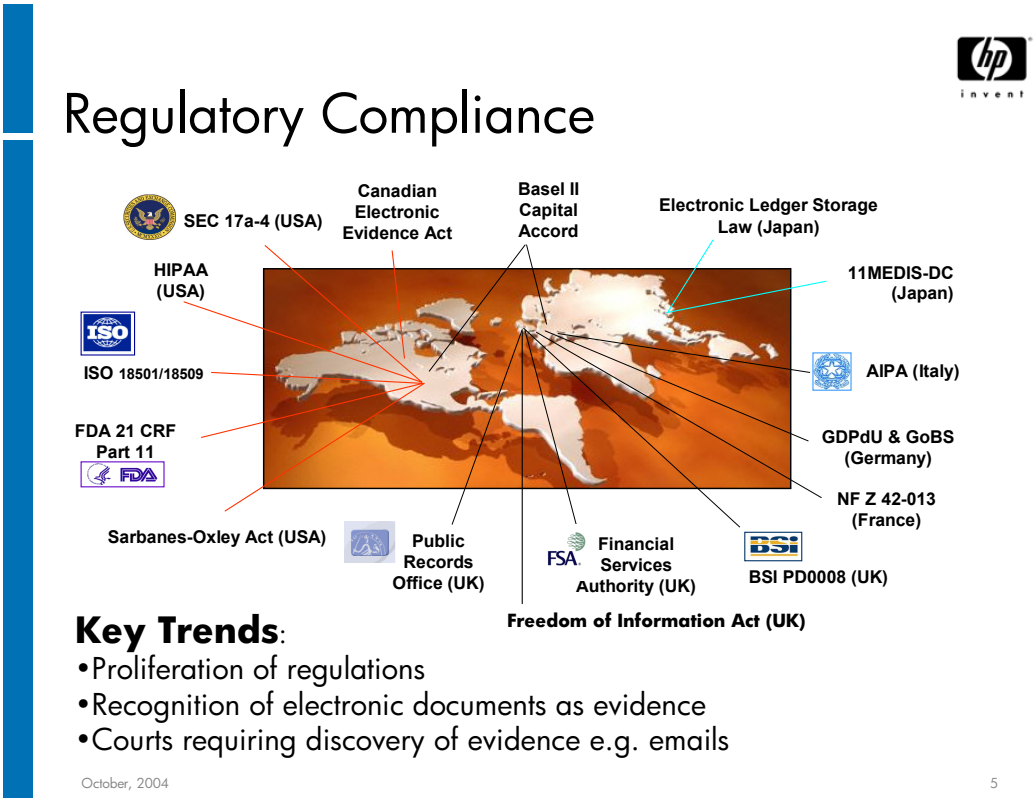
Using HP UDO and HP LTO WORM technologies as part of a regulatory compliance solution – white paper

Legal Notice

This document does not purport to provide legal advice. It is the reader's responsibility to decide whether or not the use of HP product will support a legally compliant data storage environment. For a variety of reasons, including the fact that different laws in different countries apply to different customers, HP cannot, and does not, represent that the use of HP product will result in a legally compliant data storage environment.

Figure 1.



Executive summary

- New legislation is re-defining the way to store and manage data. Information Lifecycle Management (ILM) is the new term used to describe the managing of data from its creation through deletion based on its business value.
- Depending on the legislation applicable to your company, generally speaking, legal compliance puts the onus on directors, board members, and company executive officers to ensure that organizations take all reasonable steps to protect electronic records, to ensure only authorized access, and to ensure that audit procedures are available for inspection by the relevant authorities. Individual technologies such as write once, read many (WORM) can be used to enhance protection and audit standards but are not in their selves legally compliant.
- To enable conformance with compliance regulations requiring non-alterable data formats, three technologies are emerging as ways of meeting these regulations: disk-based WORM, ultra dense optical (UDO) WORM, and WORM tape.
- Choose disk-based WORM technology when:
  - The compliance data capacity requirement is high (multi-terabytes to petabytes).
  - The data is required by several users (concurrent access to the data).
  - Fastest retrieval of records is required.
  - Long retention periods are required (and disk-based WORM supports automatic migration of data when old technology is decommissioned or fails).
  - Automatic deletion of records at the end of the retention period is required.

- Choose UDO WORM technology when:
  - The compliance data capacity requirement is medium (terabytes).
  - The data is required by several users (concurrent access to the data).
  - Relatively fast access to the compliance data is required, such that the data is online within seconds.
  - A long (up to 50-year) retention period is required.
  - Choose WORM tape technology when:
  - The compliance data capacity requirement is high (petabytes).
  - Slower access to data is acceptable (minutes to days if the tape is offsite).
  - Thirty years is an acceptable retention period.
  - You want to leverage existing investment in tape.
- HP leads the way in each of these ILM solutions, including the disk-based HP StorageWorks Reference Information Storage System (RISS) and a complete range of WORM-based UDO optical jukeboxes and LTO3 WORM tape-based libraries. RISS is a complete solution that can assist with meeting data retention and compliance requirements. Unlike most other disk-based WORM solutions, the RISS integrates all of the required hardware, software, and services that deliver cost-effective, long-term storage of reference information. You can read more about it at: http://h18006.www1.hp.com/products/storageworks/riss/index.html

- This paper focuses on the two most cost-effective media formats from HP: UDO optical and LTO3 WORM tape.

What is WORM?

WORM stands for write once, read many, and as this implies once data is written to a WORM device it cannot be changed, and hence becomes an audit trail. Magneto optical technology devices have been used since the early 1980s and were popular in situations such as:

- Nuclear industry—reactor activities logging
- Pharmaceutical industry—drug qualification records
- Brokers/dealers—financial transactions
- Legal—documentation
- Government—documentation

With the issues surrounding the Enron collapse where important data retention was key issue, together with the increasing use of email to facilitate contractual relationships, there has been a clamor for legislation to permanently protect data in a more rigorous manner. Probably the most famous legislation in this area is the Sarbanes-Oxley Act in the United States.

The Sarbanes-Oxley Act of 2002, which applies to all public companies of any size in the United States and any foreign companies that trade stock in U.S. markets, mandates data retention policies and criminalizes tampering with or destroying corporate financial records, even prior to a subpoena.

This kind of legislation is fuelling the demand for ILM capabilities in business. HP is a major player in information management solutions. WORM devices have an integral role to play in this arena. HP UDO WORM devices and the new HP LTO3 WORM tape devices are the most cost-effective WORM technologies that HP offers.

	UDO	LTO3 WORM tape
Capacity	30 GB	400 GB native
Write/read speed	Write 4 MB/sec Read 8 MB/sec	Write up to 80 MB/sec native Read up to 80 MB/sec native
Seek time or average access time to file	25 mS average seek time after media is loaded in drive	70 seconds access time after media is loaded in drive
Access to data	Normally always online/nearline Fast	Generally within a tape library or offsite Slower
Archive life	50* years	30* years
WORM media cost	$60 list	$190 list

* These figures are based on accelerated life tests. These figures do **not** imply continual usage for these periods but rather the archive periods where the media is stored in the correct environmental conditions. For more details on HP media and recommended usage consult http://h18006.www1.hp.com/storage/storagemedia.html.

For customers already using SuperDLT (SDLT) technology HP also offers WORM tape capabilities on its HP StorageWorks SDLT 600 tape drives. The brand name for SDLT 600 WORM technology is DLT*ice*. For more details, see Appendix D.

Technology attributes

Certain attributes of disk and tape lend themselves to being used in a particular environment.

Optical disk

- Random access
- Relatively small size of data transfers
- Medium capacity—medium $/GB
- Multiple requests simultaneously (concurrent access)
- Long product lifecycle (10–12 years, less frequent need to migrate to new media type)

Tape

- Sequential access
- High/very high capacity—low $/GB
- Large transfers (used in backup)
- Medium product lifecycle (5–8 years)
- Ferrous-based media—requires a more controlled storage environment

When used in a compliance environment, customers should ask themselves if the data to be archived will:

- Be in small continuous packets or large single volumes
- Require subsequent concurrent frequent access or serial infrequent access
- Require a storage/retrieval period that will require one or more migrations to new media

The following explains how these technologies can be utilized in the growing compliance-based environment.

Compliance best practices

- The need for compliance-focused content-storage systems is growing rapidly due to tremendous pressure on enterprises to establish data retention policies.
- Yankee Group (http://www.yankeegroup.com) estimates growth from $160 million in 2002 to $1.6 billion content storage market segment in 2006.
- The Enterprise Strategy Group (http://www.yankeegroup.com) estimates the worldwide capacity of compliant records will increase from 376 PB in 2003 to 1,644 PB in 2006, a compound annual growth rate (CAGR) of 64%.
- Sarbanes-Oxley Act of 2002 will put even greater pressure on all public corporations to improve governance and audit quality of financial transactions.
- The AMR Research Group (http://www.amrresearch.com) estimated that $1 billion would be spent in 2004 on compliance technology.

What is legal compliance?

Legal compliance can be defined as the requirement for individuals or corporate bodies to conform to all relevant legislation that pertains to their individual actions or those of the corporate body. This paper generally addresses regulations concerning electronic record keeping and electronic data processing.

For many years legislation did not keep pace with the advances in information technology. However, national governments began to recognize that even small companies used information technology as an integral part of running a business and many organizations kept large amounts of information electronically. Legislation began to be passed concerning data protection and the transfer of electronic information.

New legislation such as the Data Protection Act (UK 1975), the European Data Protection Directive (EU 1975), and amendments to the Securities Exchange Act of 1934 (Rule 17a-4, USA 2003) began to require organizations to look at their information technology systems so that they were compliant with the new legislation.

As a result of several corporate financial scandals in the United States, the Sarbanes-Oxley Act of 2002 was enacted, which imposed strict financial audit requirements on U.S. public and private corporations. It created the Public Company Oversight Board (PCOB) as a private sector non-profit making corporation to oversee auditing standards of companies. As much of corporate finance is managed electronically, this indirectly involves IT systems and data under strict audit standards.

In addition to company accounting standards, another major area of legislation applies to data stored electronically, which contains private information on individual persons. Much of the legislation concerns protection of that data and access to that data by the individual or other persons. Electronic transmission of such data is often subject to strict legislation. Guidelines are usually stated for the retention period for records and the process for data destruction.

Nearly all legislation carefully avoids references to specific technology and it is erroneous to state that a particular hardware or software product legally complies with specific legislation. Legal compliance, with only a few exceptions, really applies to the audit standards of the systems and processes used by an organization and this directly affects how electronic data processing and record keeping is applied to those processes.

Who is responsible for legal compliance?

Depending on the legislation applicable to your company, generally speaking, in most cases the board of directors and executive officers are responsible in law for a company or an organization. In some cases of charities or non-profit making bodies, it is the trustees who are responsible. In the case of professional practices such as architects, accountants, lawyers, or similar organizations then, generally speaking, the partners have the responsibility. In large corporations responsibility may be devolved to individual group businesses operating under the control of a vice president or similarly ranked company officer. In multi-national organizations companies very often operate as wholly own subsidiaries, in which case there should be board-level appointees for the country involved.

It is good practice to appoint a compliance officer with a reporting line to the board or executive officer of the company who would be responsible for determining all relevant national and international legislation applicable to your company.

The role of WORM technology to as part of a compliance solution

Legislation does not specifically refer to a particular technology as being compliant but basically insists that WORM capabilities (in the device or the media) should not be capable of being turned off.

Depending on the legislation applicable to your company, generally speaking, the responsibility of legal compliance normally mandates that audit systems are in place to control the retention, transmission, processing, and destruction of electronic records and communications. WORM devices can be a key part of the audit process as they prevent accidental destruction or deliberate tampering with the electronic data contained on the media (tape, optical, or specialized disk-based storage systems). Email presents a big challenge as corporations who are involved in litigation are normally required to produce email evidence in case of any investigation by a regulatory body. As companies produce large volumes of email, it becomes a difficult task to search for individual messages and or attachments.

WORM tape and disk have the ability to store large volumes of such data and retrieve items in reasonable time. This would normally operate in conjunction with specialized email archive software. The WORM media enables an officer of the company to state that reasonable care is taken to preserve electronic records and should be part of a defined auditable process.

Procedures should be recorded in a written document, which should be available to investigating authorities at any time. Under some national legislation it might be necessary for the supplier of a particular technology (for example, WORM) to provide technical details on the technology.

Hardware is never submitted for compliance verification but should be detailed in all the audit documentation with technical specifications.

Specific national legislation

Sarbanes-Oxley Act—USA 2002

This much referred to act was introduced after several large corporate financial scandals and although has no references to electronic records, it does have far-reaching implications for corporate governance in the United States. The act requires organizations to comply with far more stringent accounting standards. Information technology can in fact be of great assistance in complying with the audit standards. Generally the act puts the onus on board members and corporate officers to be responsible for producing financial records if required for an investigation by relevant U.S. government bodies. Failure to comply with an investigation and to comply with certain standards of corporate governance carries very severe penalties.

The act requires all companies to comply with the financial accounting standards and disclosure rules for the financial year ending in April 2005. However, compliance with some requirements of the act

was required from 2002. Storing information on WORM media would become part of a company's solution and would demonstrate that company officers have taken due diligence with record keeping and could form a valuable component of an audit trail.

Securities Exchange Act—USA 1934 (amended)

The Securities Exchange Act applies to dealers or brokers in securities and other financial instruments. Rule 17a–4 applies specifically to records preserved by stock exchange members, dealers, and brokers. Records can be kept electronically or on microfilm (micro graphically) subject to the following:

- Preserve records exclusively in a non-rewritable, non-erasable format.
- Verify automatically the quality and accuracy of the storage media process.
- Serialize the original and, if applicable, duplicate units of storage media, and time-date for the required period of retention the information is placed on such media.
- Have the capacity to readily download indexes and records preserved on the electronic storage media to any medium acceptable under paragraph (f) as required by the commission or the self-regulatory organizations of which the member, broker, or dealer is a member.

If records are not preserved on optical disk WORM media or CD-ROM, then the dealer or broker must inform the designated examining body at least 90 days before employing the technology. The member, broker, or dealer must provide its own representation or one from the storage medium vendor or any third party with the appropriate expertise. WORM tape or WORM disk would be a suitable candidate for submission to the designated examining body.

European Data Protection Directive (European Union)

(Directive 95/46/EC)

This directive was established in October 1995 and has implications for individual national laws with the European Union. The directive applies in conjunction with individual European Union member state legislation, for example, Data Protection Act (UK).

U.S. Food and Drug Administration (FDA)

21 Code of Federal Regulation 11 (21 CFR 11) sets forth the criteria under which the agency considers electronic records and signatures. Computer systems (including hardware and software and attendant documentation) can be subject to FDA inspection at any time. The regulations mandate the accurate and ready retrieval of records throughout the retention period of the data.

Health Information Portability and Accountability Act 1996 (HIPAA)

This act was introduced as a result of congressional health reform. It enforces standards for health information stored electronically and the use of electronic signatures. Using the term "HIPAA compliant" is not allowed. The act sets standards for data privacy and security for organizations in the healthcare industry.

Freedom of Information Act 2002 (UK)

This legislation ensures access to personal information held on individuals by private or public organizations is available to the person whose information is being held. The act became law on January 1, 2005. There are no references to technology involved in data storage but organizations must be seen to be reasonable custodians of information.

A general checklist for the compliance officer (dependent on specific legislation applicable to your situation)

- Define a list of persons with responsibility for information systems within the organization and their access rights to the data both physically and electronically.
- Ensure that company officers are fully aware of their responsibilities under any of the relevant legislation.
- Ensure that all audit requirements for the relevant authorities are documented and that specific regulations are complied with.
- List details of all data storage devices together with technical specifications from manufacturers.
- Document processes for data backups and also the destruction of obsolete records.
- Ensure that all audit documentation is secured but available for inspection on demand.
- Consider implementing a quality management system to ISO 9000 standards.
- Ensure that good email archive systems are in place and documented.

Summary

The rising volume of legislation concerning corporate governance and reporting, including legislation pertaining to electronic information, means that organizations should consider designating a compliance officer who has responsibility for information security and the implantation of audit standards. The financial sector probably has the most stringent legislation and penalties for non-compliance. WORM technology is seen as a valuable component in enabling a company to develop IT systems and audit trails. Such IT systems and audit trails would be key components to indicate that company officers have taken all reasonable steps to maintain good standards in electronic data systems. Apart from one or two particular exceptions, no particular technology is defined as legally compliant. Legislation takes great care not to refer to specific products. However, legislation places great emphasis on the availability of information during the course of any official investigation, and poor practice and lost information would be seen as failure to maintain good standards and could result in severe penalties. The burden of increased vigilance is placed directly with organizations, and information technology can be seen as a valuable method of reducing the costs associated with legal compliance.

Hypothetical case studies

Following are two examples showing how compliant processes can be developed and deployed. Both examples contain references to HP products that can form part of the solution.

Case Study A: UK email implementation

Though the email retention requirements of a company will vary according to its own requirements (country, product, or service sold, statutory and legal retention periods, likelihood of legal action being taken, and so on), it can be useful to demonstrate how critical appropriate email retention can be through a theoretical example (used with the permission of Stephen Mason, author of "E-mail and the Internet at Work: A concise guide to the legal issues").

In the example company:

- The accounts department has put in place an online claims process for mileage and expenses. Employees download the claim form from the intranet, gain approvals for it by email, and submit it for processing as an email attachment.
- The accounts department frequently sends invoices by email, and subsequent queries and payment issues are resolved by email.

- The HR department requires that overtime forms are submitted by email, together with any supporting information.
- Documentary records relating to the concept, design, and testing of a new product are developed and managed primarily through email.

In this scenario, UK law could require you to retain all:

- Internal emails for mileage and expenses for six years.
- Invoices sent out of the company for a minimum of seven years.
- Overtime claims for three years.
- Documentation relating to current products for up to 10 years from the date of supply.
- Documentation relating to the product in development for a period exceeding 10 years to cover product liability.
- Documents relating to contracts entered into by exchange of emails for a minimum of six years and after the contract is terminated.

Retention policy decisions

After you have established what period of time different types of email documents need to be retained for in your organization, you must work out how to:

- Ensure that the retention occurs consistently.
- Retrieve documents in a cost- and time-effective manner when they are required.

In theory it is possible to ensure that every employee knows the retention period for each type of document and either files them manually or manually flags their content, so that an automated system can file them according to metadata. In practice it is usually more viable to basically keep everything, and put in place tools to extract data when it is required. Naturally this increases the requirement for digital storage media to hold this email repository within the organization. However, the costs of this do not tend to be an issue compared to the costs incurred in trying to extract legacy data from difficult to search backups, or the possible fines and legal costs associated with failing to comply with legislation appropriately.

In this example HP could offer three hardware solution components which, along with the defined process and a compliance officer, could enable the customer to create an IT solution to ensure adherence to the process and would constitute a good case for the company complying with the rule of law.

High-End Enterprise Solution: HP StorageWorks Reference Information Storage System (RISS)

Disk-based storage with indexing, HP StorageWorks Reference Information Storage System (RISS) can input data from a wide range of sources including Microsoft® Exchange. RISS offers fast retrieval through the powerful search tools and the indexing system. A comprehensive solution with an associated price point, this solution can scale to up to 67 TB of storage.

Mid-Range Solution: HP UDO Optical Libraries

When used with additional software such as KVS Enterprise Vault (email archiving), this solution can provide fast access to up to 7.1 TB of online data (using HP StorageWorks 7100ux UDO library). For example, the KVS archiving software uses the AltaVista search engine to allow fast indexing to the data required, which can search any text string within an email.

Entry-Level Solution: HP LTO3 WORM tape

You cannot keep all your digital data "online" indefinitely, so there will come a time when you must archive it to a non-tamperable nearline medium. HP LTO3 WORM technology is ideal for this and very cost effective (20 cents/GB). HP has a series of libraries that support LTO3 technology (see Appendix B), the largest being the HP StorageWorks ESL E-series library, which can store up to 521 TB. WORM tape capability can be used without any further software purchase, and archiving can become just an extension to your day-to-day backup regime. The issue with this solution is indexing. Although backup software will keep a catalog of the archived .pst files from an email archiving system and can retrieve a single email (if single mailbox backup options are used), the backup application has no text search capability. Therefore, customers would have to restore relevant archives (.psts) back into an Exchange recovery mailbox and then use the Microsoft Outlook search capabilities to find emails relevant to their needs.

For storing file types other than email .pst files, there are several companies that support indexable archiving to tape, which allows fast retrieval of archived information direct from tapes in libraries.

Case Study B: U.S. corparate company with UK subsidiary (see Figure 2)

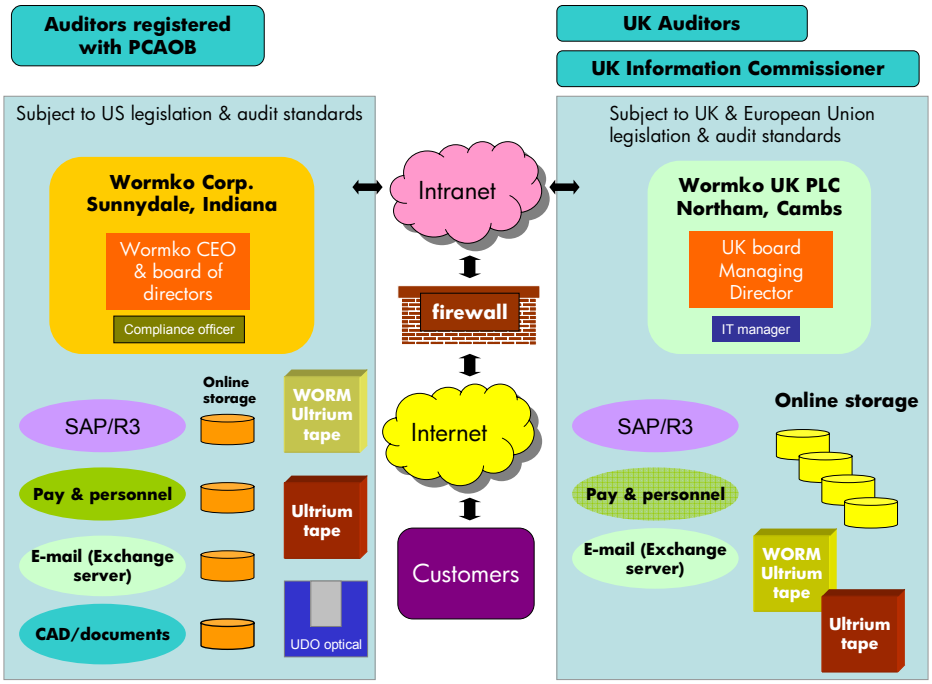
The Wormko Corporation has headquarters in Sunnydale, Indiana, USA and a subsidiary in Northam, Cambridgeshire, United Kingdom. Wormko is registered in Delaware and Wormko UK operates as a wholly owned subsidiary of the Wormko Corporation.

Wormko has an annual turnover of $1.5 billion and manufactures industrial heat exchangers in its plant in Sunnydale, USA. The UK company is registered as a limited company with companies housed in the United Kingdom. It performs light assembly work and manages all sales within Europe and the Middle East. Wormko's products are sold into both manufacturing and military environments. The U.S. navy is a large account in the United States.

Wormko operates IT systems in both the United States and the United Kingdom and has a company intranet with a firewall to the public Internet. Information flow to customers such as email and electronic data interchange uses the public Internet connections. Both hardware and software firewalls are in use with anti-virus software used to scan all incoming mail. Systems are all password protected.

Wormko has appointed a compliance officer in the United States who reports to a board member. The board and executive officers have responsibility for all legal compliance issues. The UK subsidiary has a managing director who is responsible for company actions in the United Kingdom.

Figure 2.



The compliance officer has implemented an audit procedure for all electronic data retention and transactions within the company. The UK IT manager is tasked with ensuring that all UK systems meet the necessary UK and EU audit standards. The UK Public Limited Company has also registered under the UK Data Protection Act, as it holds personal data on employees within the pay and personnel system. There is a set procedure for access by individuals to their own information.

The U.S. company IT audit procedures concern the complete lifecycle of data from creation to destruction. There are separate policies for email, commercial sales data, and technical information. The documentation of the audit procedures is available to the company auditors who must by U.S. law be registered with the PCOB.

Email archives are managed by an additional commercial email archive package and these are retained on optical disk and magnetic tape. The email archive package provides complete indexing and search facilities. Offsite copies of emails are maintained. As the UK operation is smaller, the email server is backed up to WORM-capable tape on a regular basis. Retrieving archived emails is more difficult but the volumes are low. The UK email systems will be migrating to an archive solution identical to the system in the United States in the near future.

Technical information and drawings concerned with U.S. navy projects are retained on WORM UDO optical media using a single drive disk library, and compliance to the U.S. Department of Defense Directive 5015.2 is ensured.

Commercial systems (sales order processing, stock control, and ledgers) using the SAP software are based on an Oracle®10g database and regular backups are made to standard LTO Ultrium tape media. All database transaction logs are kept in duplicate online but are also copied to LTO Ultrium media.

HP OpenView Storage Data Protector is used as the media management system and has the ability to interface directly with the SAP/R3 backup tools.

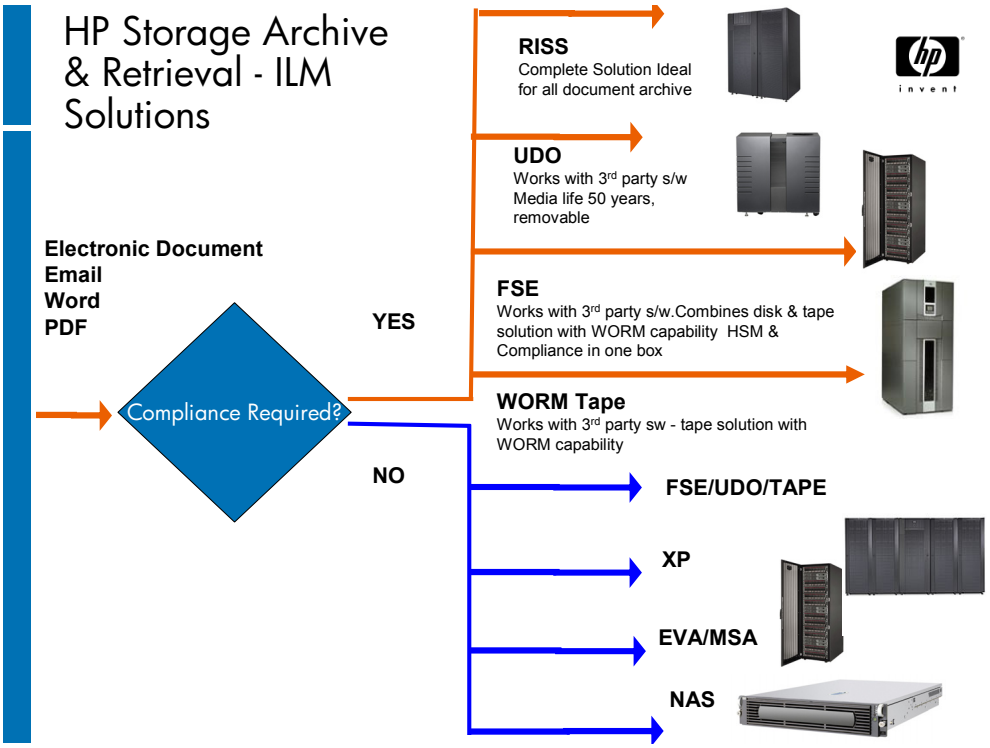
Tape and optical media are stored offsite in a secure facility. All tape movements offsite are documented and a copy of the media register is kept offsite.

Wormko is registered as an ISO 9000 company in both the United States and the United Kingdom, and IT procedures and audit standards are maintained to ISO 17799 standard.

The board member responsible for information technology, the compliance officer, and the UK IT manager hold quarterly meetings to review procedures. These meetings are officially recorded and minutes taken. Wormko is subjected to regular ISO 9000 audits in both locations.

This example shows how processes and technology can be used to meet the regulatory compliance standards and directives in a diverse IT environment divided between two countries. The directors, board members, and company officers, having ensured that the correct systems and processes are in place for this company, would be seen to have taken all reasonable steps to comply with all relevant legislation.

Figure 3.



RISS = Reference Information Storage System

FSE = File System Extender

UDO = Ultra density optical

WORM = write once, read many

XP = The HP very high-end enterprise disk array

EVA = The HP Enterprise/Mid-range disk array

MSA = The HP entry-level disk array

NAS = Network attached storage

HP offers a wide range of data storage solutions on disk, optical, and tape that can assist the customer in designing a compliant solution. Some products such as HP RISS are a complete solution, others rely on other HP software for which use licenses can be purchased (such as HP OpenView Storage Data Protector or HP StorageWorks File System Extender [FSE]), and some rely on third-party software (such as KVS, XenData, or K-PAR archiving software).

Figure 4.

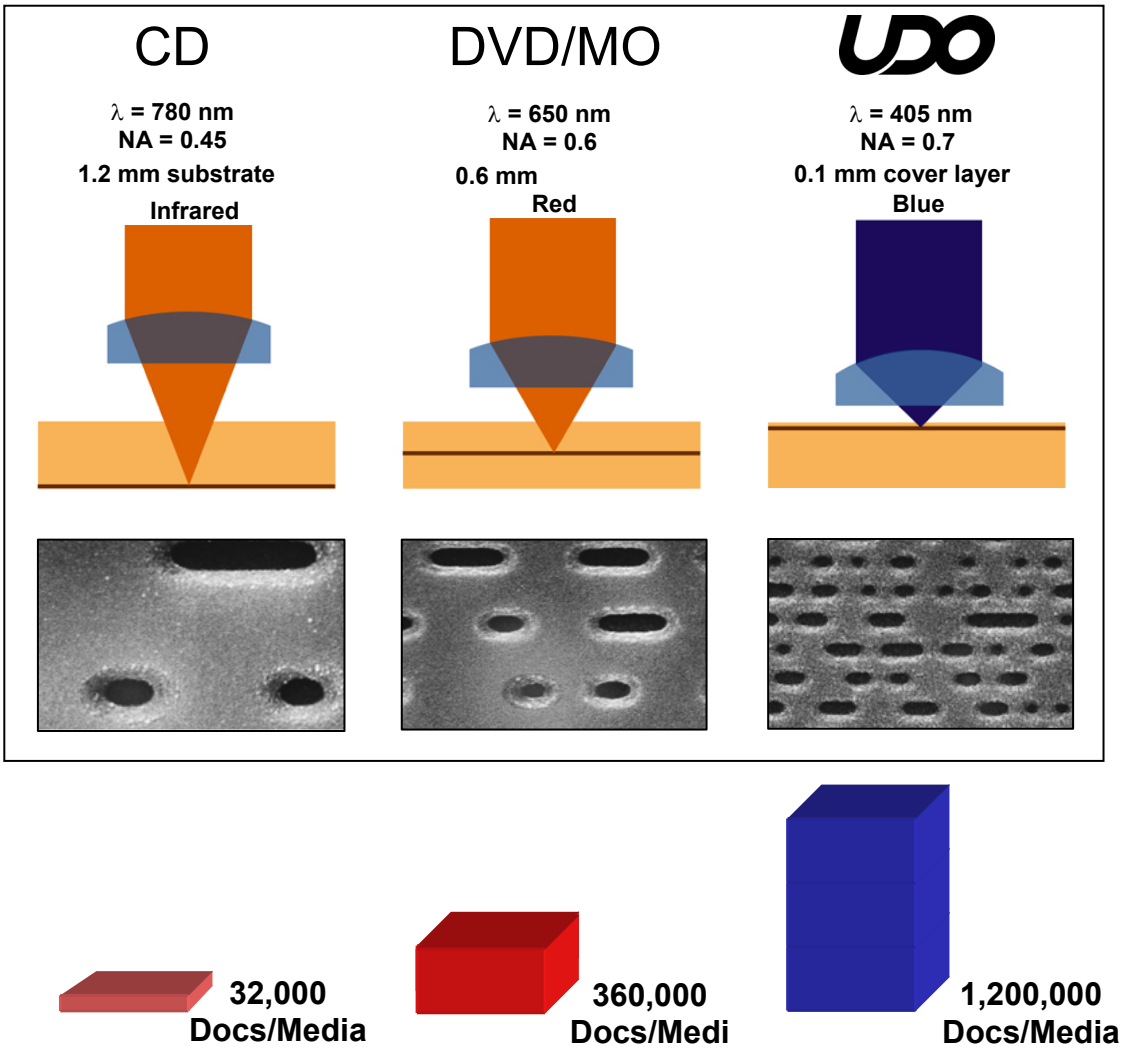


Figure 4 shows the major developments in optical technology. Unlike CD or DVD, UDO technology uses blue lasers with a smaller wavelength (λ) together with a numerical aperture (NA) of 0.7. The NA of a laser is a measure of its ability to gather light and resolve fine specimen detail at a fixed object distance—similar to the "f" numbers used in photography. The smallest optical dot that can be achieved is proportional to λ/NA.

The net result is that UDO technology can offer an approximate 2.6 times increase in densities over DVD/MO technologies.

The recording process uses phase change technology, and is a totally non-magnetic process based on a specially designed recording layer that can exist in both amorphous and crystalline states. The layer is transformed between these two states by the heat from the precision laser.

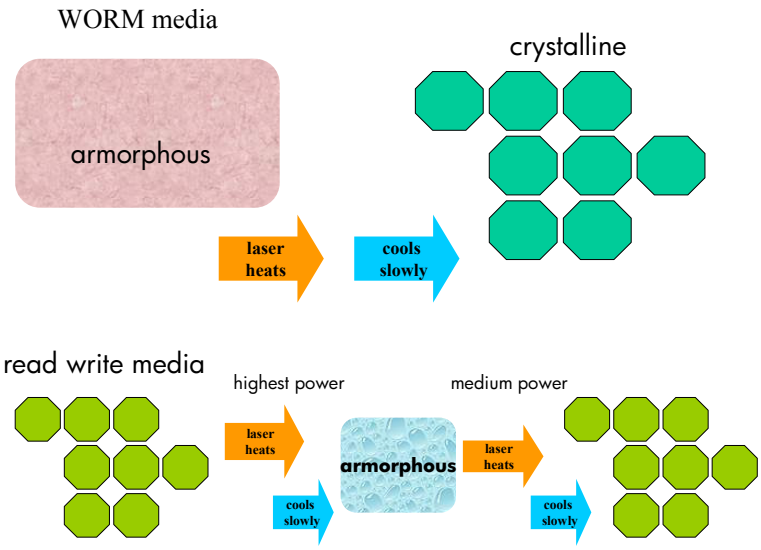
For write once media, the transition is from amorphous to crystalline and is irreversible.

For write/read media, the transition is from crystalline to amorphous.

The drive is multi-functional in UDO as it takes WORM and write/read media. The laser is not multi-functional although it does have different power settings. The reason why WORM media cannot be changed back into an amorphous media is both chemical and thermodynamic. The WORM formulation becomes crystalline as it cools slowly. If it is heated again, it is not possible to change it back to amorphous material as it would require much quicker cooling than is possible within the UDO disk layer.

The write/read media works the other way and is changed from crystalline to the amorphous state on the application of heat (different temperature). However, when re-heated with a lower power and allowed to cool, this material is made so that it crystallizes. Read is done at the lower temperature again.

Figure 5.



HP re-writable UDO media

HP write once UDO media

Features and benefits of UDO technology

Feature	Benefit
ISO and ECMA certified	Investment protection, multi-vendor support, mainstream device
UDO's patented Phase Change recording process permanently alters the molecular structure of true write once media, ensuring data integrity at the most fundamental level.	UDO provides absolute data authenticity to assist the customer in designing a regulatory-compliant solution or for any application where archived information must remain 100% unchanged.
Ratified by Cohasset Associates as having the necessary capabilities to assist the customer in designing a regulatory-compliant solution.	SEC legislation is the most well-defined data protection compliance methodology. Customers can buy with confidence that HP UDO WORM is a robust component to help meet compliance requirements.
15 GB per side, 30 GB total. Available in write/read media (10,000 re-writes) and WORM media. Around $60 list	Allows jukeboxes to utilize optical for both write/read and compliance (WORM) applications. Low cost of ownership
Robust media cartridge 750,000 mean swaps between failure (MSBF) (15 GB per side, 30 GB total)	High data integrity and reliability through well-protected media
25 mS average access time	Fast access to data
Random access	Supports concurrent access from multiple requestors
Long archive life (up to 50 years)	Preservation of data and secure record keeping
Long product life (10–12 years)	Less need to frequently migrate the data
Wide range of mainstream ISV support	Customer has wide choice of solutions

Typical usage model for HP UDO WORM

Following are some real-world examples of using optical WORM technology:

Major European airline in Germany

This European airline is regulated by law to preserve flight coupons on a non-alterable media for up to 10 years. Over 40 million coupons a year are gradually digitized and archived. Over 100,000 requests monthly are made to access old flight coupon information. Optical WORM media is ideally suited to repeat fast access (concurrency) and has a high media life.

Major European bank in London

Banks are generally required to preserve stock transactions for several years, and these stock transactions are interrogated fairly regularly by multiple people (up to 2,500 per month). Hence, the system must offer concurrent access, so UDO optical was chosen.

Austrian insurance company

The records and policies of an insurance company are its lifeblood. Litigation and audit trail requirements are also a requirement. So for purely pragmatic reasons this insurance company chose UDO optical because of the 100% absolute true write once capability of UDO WORM. Being an insurance company they did not want to take any risks!

Major European aircraft manufacturer/civil engineering company

Aircraft and civil engineering constructions can have life expectancies of 30–50 years, and during this time the design information must be readily available for inspection and review (especially in the case of accidents) and be the original data. UDO with its fast access time and low requirement to urgently change media type as new technology becomes available is ideal for these types of long-term projects.

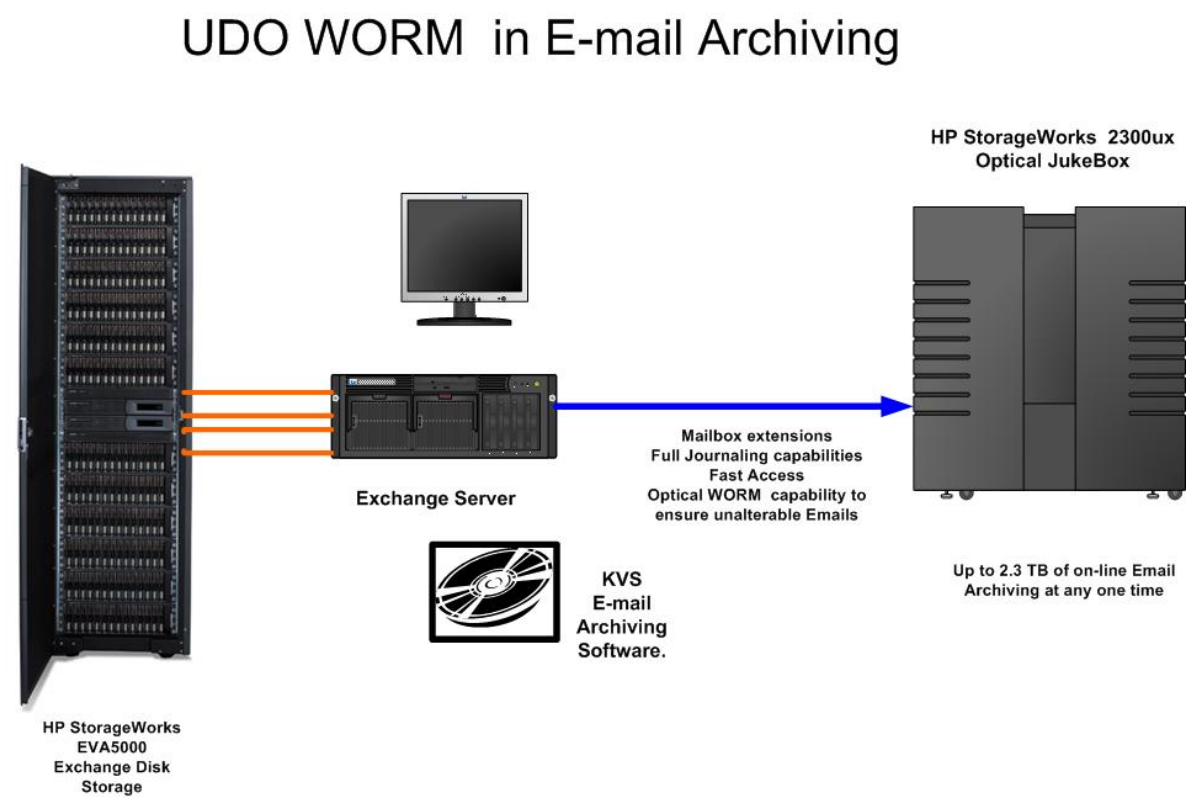
U.S. aerospace company

This major U.S. aerospace company is responsible for launching and supporting global positioning systems (GPS) for the U.S. air force. The operational nature of this telemetry data from the orbiting satellites meant it had to be highly secure. Optical was chosen as the media of choice to store the online data for the following reasons:

- Economical
- Quick access time
- Small volume incremental data
- Long, secure archive life
- WORM media

A practical hardware scenario

Figure 6.



ISV solution vendors

ISV	Expected support date (as of 12/01/04)	Mixed drive support	Fibre Channel support
ADIC	October 2004	Not in first release	TBD
Comsquared	June 2004	No	No
EiStream	June 2004	Yes	No
FileNet	March 2005	Evaluating	No
IXOS/OpenText	December 2004	Not in first release	Yes
KOM	June 2004	Yes	Yes
K-PAR	October 2004	Yes	No
KVS	Support by Qstar		
Legato (AX)	June 2004	Yes	No
Legato (EX)	Support by Legato AX	Yes	No
Legato (DX/DXUL)	June 2004	Yes	Yes
Optika	June 2005 (Stellent Acquisition)	TBD	No
Pegasus	June 2004	Yes	Yes
PoINT	June 2004	Yes	Yes
Qstar	June 2004	Yes	Yes
Seven Ten	June 2004	Yes	Yes
Tivoli	In progress	TBD	TBD
Unisys	Launch + 180 days	TBD	No
US Design	In progress	TBD	No
VERITAS	Support by Pegasus		

Introducing HP LTO WORM technology

Linear Tape Open (LTO) technology is rapidly becoming the de-facto standard in the enterprise tape market. Designed and developed by HP, Certance, and IBM, it offers customers choice, uncompromising reliability, and performance.

The latest feature addition to the LTO standards is WORM media support from LTO3 onwards.

The HP StorageWorks Ultrium 960 tape drive WORM capability is fully certified by the LTO technology provider companies as meeting all the requirements of LTO tape standard AU-WORM1.31.

A recent survey on http://www.searchstorage.com indicated that:

- 25% of respondents were already using WORM tape because they needed it as a component in their compliant IT solution.
- 52% thought WORM tape was overkill for their particular operations.
- 22% were actively looking into using WORM tape.

Features and benefits of HP LTO3 WORM technology

Feature	Benefit
LTO tape standard ref AU-WORM1.31	Investment protection, multi-vendor support, mainstream tape device
Ratified by Cohasset Associates[3] as having the necessary capabilities to assist the customer in designing a regulatory-compliant solution.	SEC legislation is the most well-defined data protection compliance methodology. Customers can buy with confidence that HP LTO WORM is a robust component of a solution to meet compliance requirements.
High capacity (up to 800 GB per tape)	Low cost per GB of storage
Three levels of protection i) Media Cartridge Memory[1] defines media as WORM. ii) Media servo code[2] is uniquely encoded and different from the standard "write many" media. iii) Drive can automatically detect any attempts at tampering with data and report it back to the application by way of HP TapeAlert messages.	High-integrity solution Absolute guarantee against tampering Fail-safe
High performance (up to 160 MB/sec) given a suitably fast data source	Reduced backup compliance windows—more productive "uptime"
Two-tone cartridges (see Figure 9)	Easily recognized in and out of libraries as being WORM type media
Wide range of mainstream ISV support	Customers have wide choice of solutions, and can even use their existing backup software
New bar code layout—WORM media will end in "LT." Multi-write media barcode will end in L3.	Easy recognition of WORM media by doing inventories of media within the library

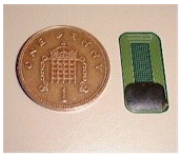
[1] All LTO media has embedded in it a 4-K flash memory (called cartridge memory). This memory is used to hold unique media ID and has a directory to allow fast access to files on the media, media performance information, and now a WORM media flag. When the media is loaded into the drive, the drive reads the cartridge memory to determine its type, condition, and so forth.

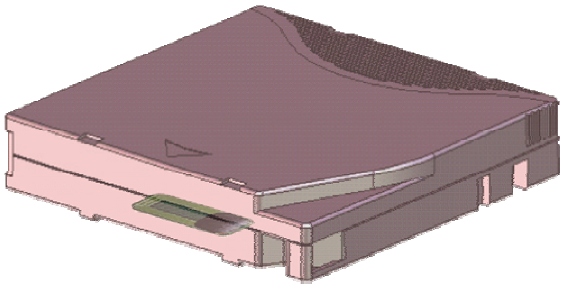
[2] LTO media contains embedded servo tracks along the full length of the tape. WORM media is manufactured with a completely separate servo writer and in the servo data is an area called the "manufacturers word." This "manufacturers word" is distinctly different between normal write/read media and WORM media. Hence, WORM tape is considered immutable because it is impossible for anyone to change the encoded data within the servo code on a piece of media all the way down tape.

[3]Both HP LTO3 and SDLT 600 DLT*ice* WORM implementations have been assessed for compliance with SEC 17a–4(f) by an independent body (Cohassets Associates Inc.) and have been found to "provide the features and functionality that either directly meet the relevant requirements of SEC17-a-4(f) or allows them to be met."

Figure 7.

Cartridge Memory (LTO-CM)





- 4KByte data, similar to technology used in Smart cards.
- Readable from ~15mm from front of cartridge using Radio Frequency
- Primarily used to improve speed and reliability of drive
- Stores media usage & ID information
- Spare space can be used by backup application

Within the 4 Kb of the cartridge memory is a *format type* field. For LTO3 WORM media, this field is set to 2-0-0-4, the "2" bit signifies this is WORM type media and the "4" bit signifies it is an LTO3 format media. (For LTO4 the field will be set to 2-0-0-8.) Therefore, using the cartridge memory format field, the tape drive can instantly recognize the media type installed in the drive and the format of that media.

Figure 8.

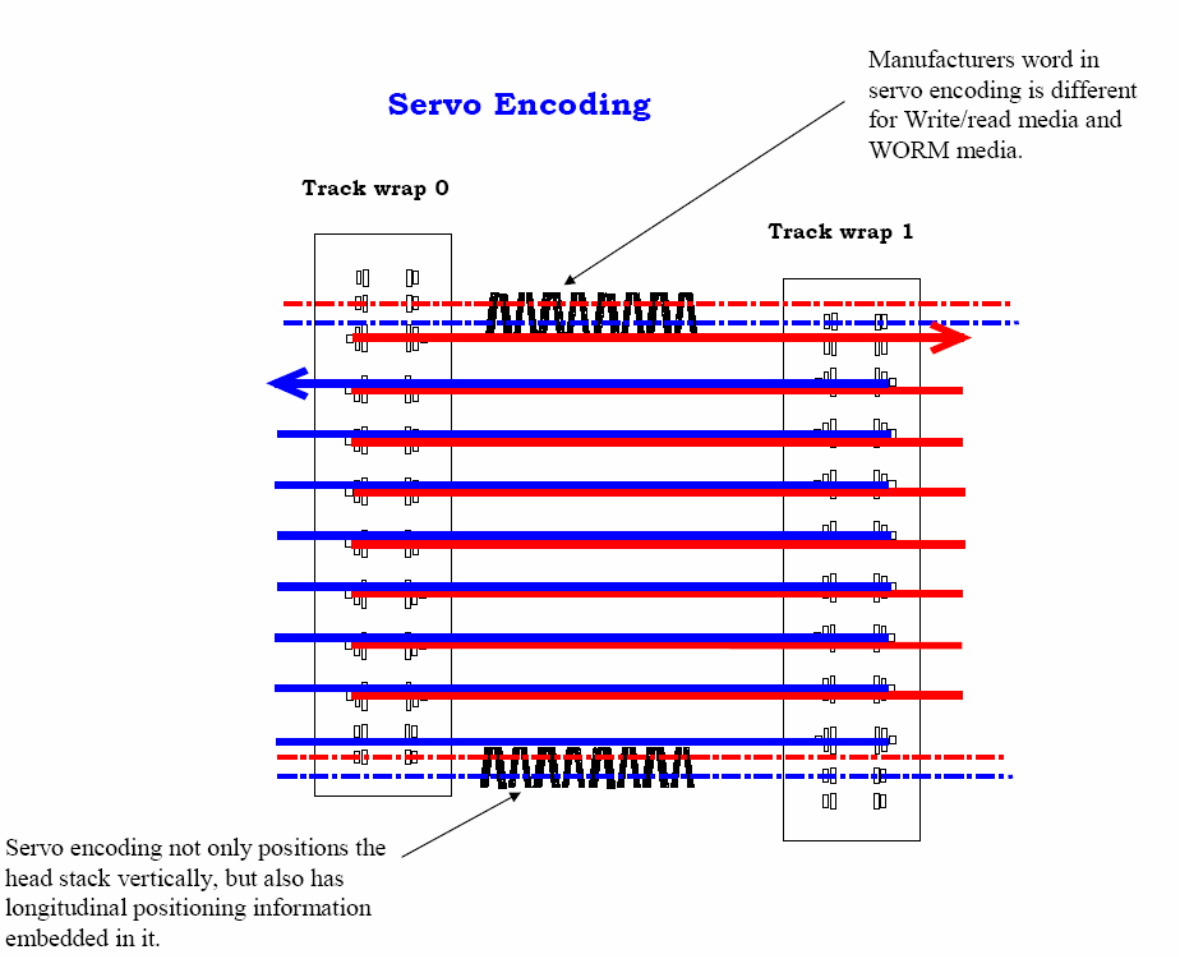


Figure 8 shows the layout of the write/read data heads and the servo heads on LTO.

LTO has dual redundant servo heads. The servo encoding information is shown in black as a series of peaks. By reading the "gap" across peaks, the vertical position of the head stack can be changed on different passes of the tape, therefore data is written forwards and backwards across the tape, then the head is stepped up or down and the process repeated until the tape is full. The data contained in the embedded servo also changes down the length of the tape to give a longitudinal position. It is the manufacturer's word within the longitudinal embedded data that is different between WORM media and multiple write/read media. The drive detects that the servo code is that belonging to a WORM piece of media and so overwrite is prevented.

As the servo format is written only at the time the media is manufactured, it is impossible for anyone to change the servo tracks for the complete length of tape, hence the true WORM capability of HP StorageWorks Ultrium 960 media.

Figure 9.

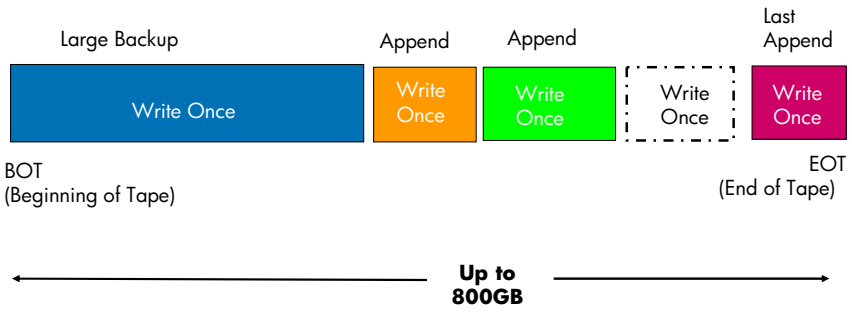
Write/read media and WORM media for HP StorageWorks Ultrium 960 (LTO3)

HP LTO3 WORM media is easily recognized because of its two-tone yellow/grey livery.

The use of appends on WORM tape

Tape is a sequential access device, not a random access device-like disk. It is common practice for many varied backups to take place to the same physical piece of tape media. Each additional transfer to tape is known as appending. The same principle applies to WORM tape media.

Figure 10.



In Figure 10 the WORM media is written to several times. Each transfer to tape can be written only once, but the full capacity of the tape (up to 800 GB at 2:1 compressible data for HP StorageWorks Ultrium 960) can still be used.

Typical usage models for HP LTO3 WORM media

There are numerous ways that HP LTO3 WORM tape technology can be utilized as a component in the compliance environment that the customer designs. Following are some examples.

Major British telecommunications company

The consumer interests for telecommunications in the UK are protected by a government body called Ofcom, the UK regulator for the telecommunications industry. Ofcom requires UK telecommunications companies to keep unalterable billing records for up to seven years for inspection in case of litigation. As you can imagine the volume of data being generated for billing is huge, and what is the most cost-effective way of storing large volumes of data—tape!

Therefore, WORM tape was chosen for its cost-effective GB/$ and its suitability for being tamper proof after the data is written.

Medical imaging records—major UK pharmaceuticals company

Drug research and development legislation in the UK requires medical records and medical images to be kept for many years. Large mass scanning devices used in medical research create large volumes of data that is first held on fast disk but then after awhile is migrated to tape. To meet the required drug development legislation, the data and patient records when held electronically must be tamper proof and so this major pharmaceutical manufacturer is developing a scanning capture and migration process that will include WORM tape.

United Kingdom armed forces—geographic data storage facility

In this example, the requirement was for a low-cost, high-density, and high-volume (132 TB) digital storage system. It had to store all objects securely, ensuring confidentiality, integrity, availability, and accountability at all times. The solution involved XenData archiving software and meets the compliance requirements of the most stringent regulations.

Document management systems—Germany and United Kingdom

There are several examples where WORM tape has been used in local authority document workflow systems and Web-based document location services. The WORM tape cartridges provide an audit trail allowing retrieval of all old file versions and deleted files. In the Web-based document retrieval applications, the additional benefits of documents being stored on WORM tape provide customers the proof they need as to the legal admissibility of image data.

Instant archiving using HP OpenView Storage Data Protector

Many of the existing HP OpenView Storage Data Protector software customers use HP LTO3 WORM tape drives as instant archiving using the media copy functionality within the software. This allows objects from multiple existing backup tapes in a library to be selected and compiled onto a single WORM tape within the library, preserving the data forever.

Major Britsih television company

A major British television company is evaluating the use of HP LTO3 WORM media for storing very high volumes (up to 12 PB over several years) of "rich media" content. "Rich media" content is the terminology used to describe digitized broadcast content, television programs, and so on. High storage capacity, long storage life, a long roadmap into the future, the high write/read performance, and low cost/TB are key factors in favor of using WORM tape in this scenario.

Figure 11.

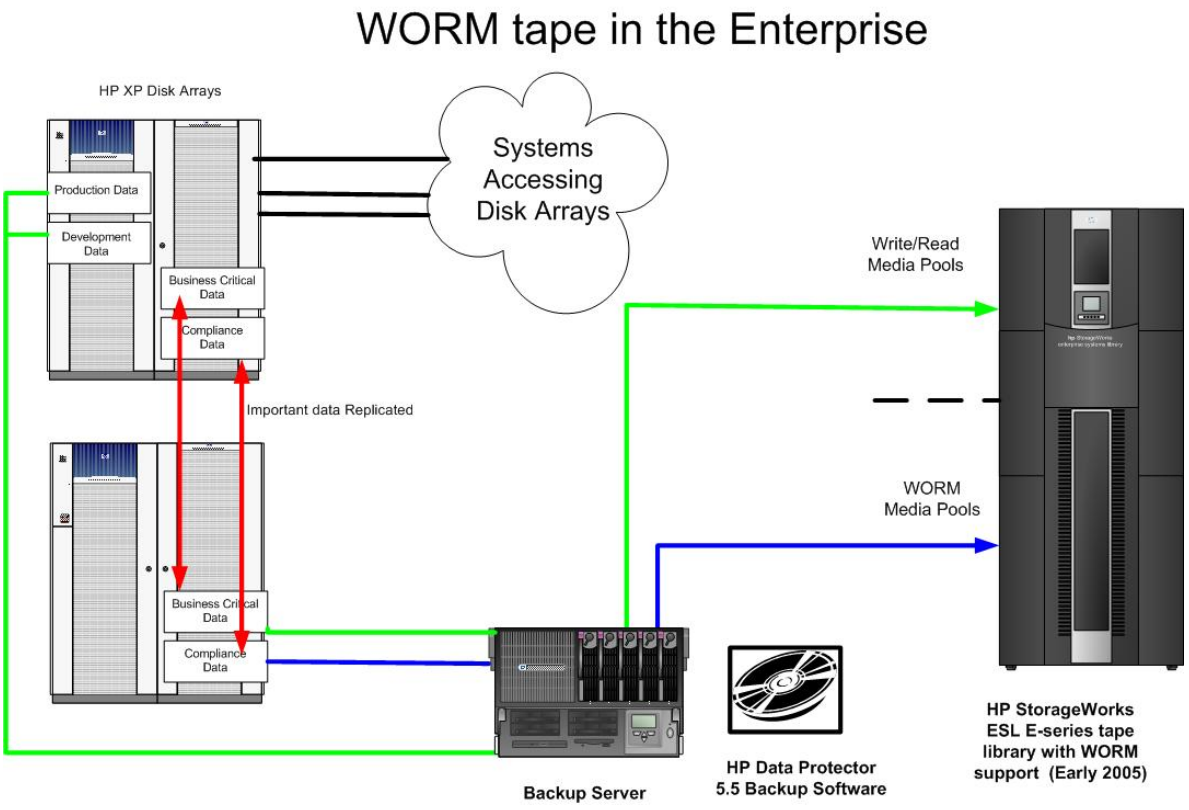


Figure 11 shows how HP LTO3 WORM technology can be easily integrated into an enterprise backup environment. In most enterprise environments, critical data is generally replicated, and this can be seen in Figure 11 where business-critical and compliance data are replicated to a secondary disk array. In turn, this secondary disk array can be presented to a dedicated backup server, and using a suitable ISV backup package such as HP OpenView Storage Data Protector 5.5, the data can either be backed up to standard write/read media in the case of the dynamic business-critical data or alternatively backed up to a WORM media pool in the case of compliance data/archive data. HP LTO3 WORM media is easily identified because of its unique barcode numbering, and Storage Data Protector will allow a media pool called WORM media to be created where only WORM media will be deployed. As can be seen, this is a relatively straightforward process to implement after the compliance data has been identified.

ISV solution vendors

What is meant by "WORM" support? With HP StorageWorks Ultrium 960 and the LTO standard WORM support becomes mainstream on tape. The other LTO manufacturers—Certance and IBM—support exactly the same functionality for WORM tape as does HP.

From an ISV perspective the initial support for WORM tape will be simply a matter of the software detecting and reporting that the media is write protected when an overwrite of existing data is attempted. Only Yosemite TapeWare currently recognizes the media as being specifically WORM media; the other ISV vendors will follow suit in their next scheduled product releases.

The following vendors currently support HP LTO3 WORM technology. For updates to this list, visit http://www.hp.com/go/connect.

ISV	Product	Support from
Hewlett-Packard[1]	HP OpenView Storage Data Protector for: Microsoft Windows®, HP-UX, Tru64 UNIX®, Netware, Solaris, Linux 64bit	V5.1
	File System Extender (FSE)	TBA
Yosemite Technologies[2]	TapeWare for Windows, NetWare, Linux	7.0 with SP7a
VERITAS	Netbackup for: Windows, HP-UX, Tru64 UNIX, AIX, Solaris, Linux, SGI Irix	V5.1 + MP1
Legato	Networker for: Windows, HP-UX, Linux, AIX, Solaris	7.2SU1
Computer Associates	Brightstor Enterprise Backup	V11.1 for Windows
FileTek	StorHouse	TBA
Grau	Infinstor archive filer	July 05
EverStor	HiARC	TBA
KoMnetworks	KomWorx	Q105
Pegasus	InveSTore for Windows	Jan 05
QStar	QStar HSM	Q105
XenData	Archive Series Software	Q105
EMC/Legato	DXUL	TBA
EMC/Legato	DiskExtender 2000	TBA
Tivoli Storage Manager	TSM	Q205

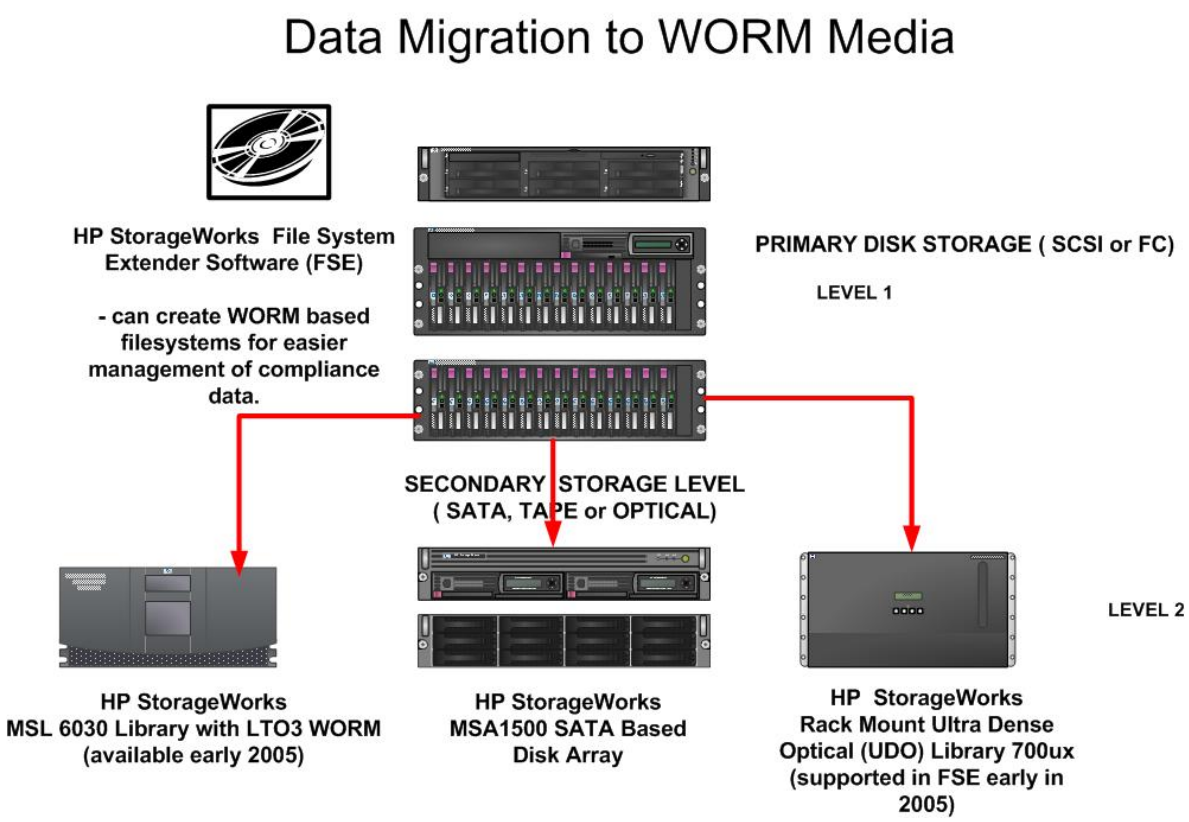
[1] A downloadable single server version of this software ships with the HP StorageWorks Ultrium 960.

[2] A CD single server version of this software ships with the HP StorageWorks Ultrium 960.

Using WORM UDO versus using WORM tape

WORM UDO	WORM tape
Medium capacity (TB)	High-capacity compliance requirements (PB)
Very long-term archive requirements (> 30 years)	Long archive life (30 years) if stored in correct environmental conditions
Minimal data conversion over time. A UDO format will typically be around for 10 years or more.	Over time a data re-format may be necessary. Most LTO tape formats are current for around 6–8 years.
Fast access—almost online, concurrent access to many users	Slower access from within tape library/offsite. Generally only single user access at any one time.
Multiple single file transfers	High-volume single instance capture—Siezmic/Satellite data or High-volume data migration to "safe" media Both these play to HP WORM tape transfer rate (80 MB/sec native versus 4 MB/sec with UDO) Time to migrate 1 TB of records to HP LTO3 WORM tape is 3.5 hrs or less.
Mid stage in an Hierarchical Storage Management (HSM) solution	Last stage in an HSM solution
Generally needs a specific investment and tailored ISV package $$	Low investment costs—uses existing tape library infrastructure and software $
Cost GB = 50 cents	Cost GB = 47 cents (or less if data is compressible)

Figure 12.



Ideally what customers require is the ability to migrate fixed content data to the storage medium that best suits the particular data's characteristics.

- Low-cost disk for very frequently accessed data
- WORM optical disk for regular access data and added true write once capability
- WORM tape for large volume fixed content data storage with reasonable access rates, 1–2 minutes

HP StorageWorks File System Extender (FSE) software allows data to be migrated to a secondary storage layer that can be disk, optical, or tape, and allows precise control of the factors governing that migration. From the very outset, FSE has the ability to make even file system storage on primary disk (level 1) WORM capable.

Summary and conclusions

Regulatory compliance legislation is set to increase, so IT managers can no longer ignore the need to take action.

Management has several different laws pertaining to data retention, corporate governance, and audits to follow. It is up to IT managers, with the assistance of management, to decide what policies to set on what data types in order for the appropriate technologies to be deployed.

The vast majority of customers have many storage options available to them that can assist in designing IT systems that meet compliance regulations. Most customers want a cost-effective way of conforming to the regulations.

HP UDO and HP WORM tape offer cost-effective components together with appropriate processes to best meet the demands of regulatory compliance. Disk-based solutions, although a valid component in a compliant solution, are a much more expensive option.

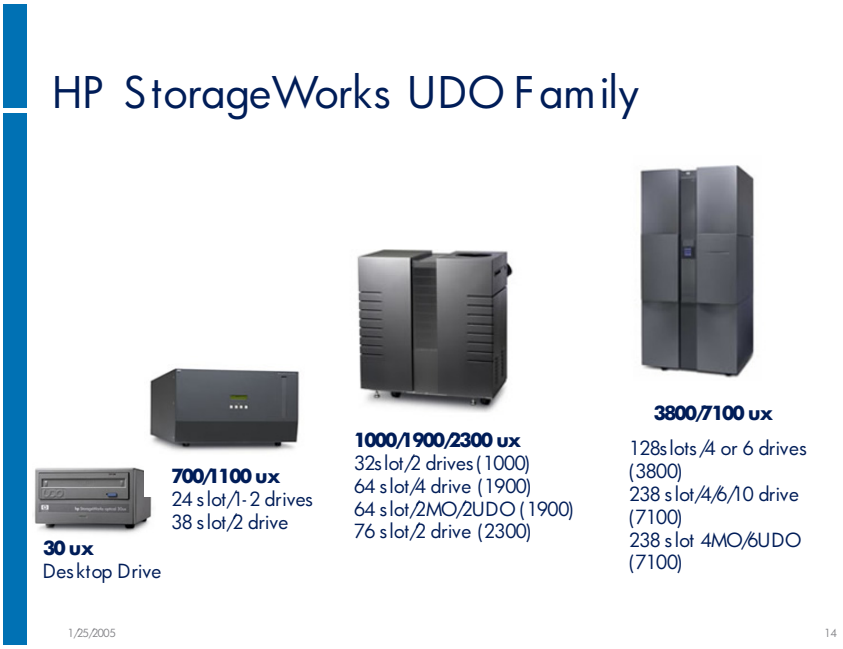
- Choose disk-based WORM technology when:
  - The compliance data capacity requirement is high (multi-terabytes to petabytes).
  - The data is required by several users (concurrent access to the data).
  - Fastest retrieval of records is required.
  - Long retention periods are required (and disk-based WORM supports automatic migration of data when old technology is decommissioned or fails).
  - Automatic deletion of records at the end of the retention period is required.
- Choose UDO WORM technology when:
  - The compliance data capacity requirement is medium (terabytes).
  - The data is required by several users (concurrent access to the data).
  - Relatively fast access to the compliance data is required, such that the data is online within seconds.
  - A long (up to 50-year) retention period is required, with minimal re-formatting over the life of the data.
- Choose WORM tape technology when:
  - The compliance data or archive data capacity requirement is high (petabytes).
  - Slower access to data is acceptable (minutes to days if the tape is offsite).
  - Thirty years is an acceptable retention period.
  - You want to leverage existing investment in tape.

HP leads the way both in ILM solutions, including a complete range of WORM-based UDO optical jukeboxes and LTO3 WORM tape-based libraries (see Appendixes A and B).

Appendix A: HP UDO roadmap and product line-up

Figure 13.

Figure 14.



Appendix B: LTO roadmap

All generations of HP LTO from Generation 3 onwards will support WORM tape.

Figure 15.

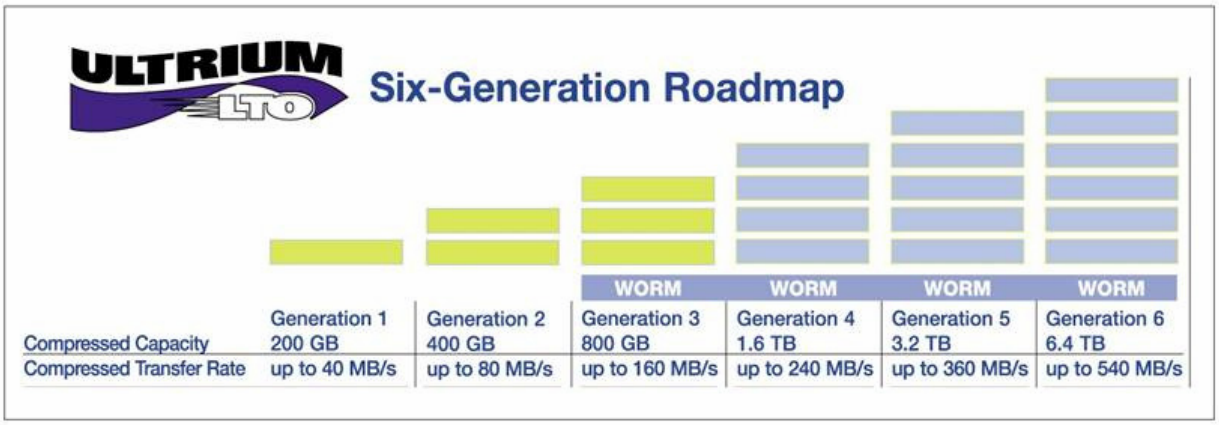
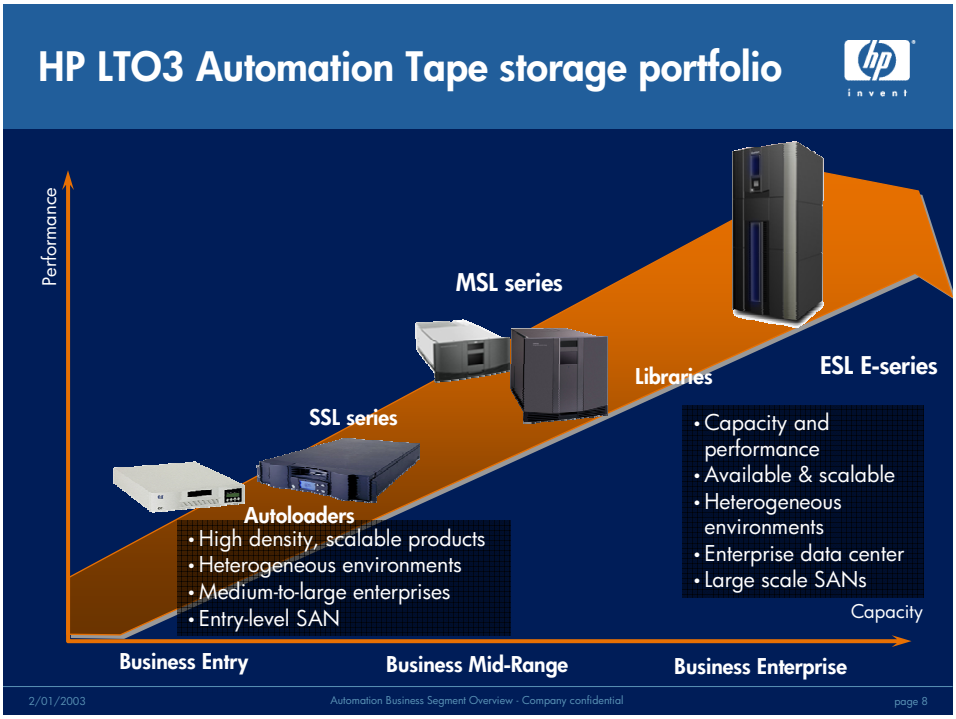


Figure 16.



WORM tape is being integrated into all of the HP automated tape libraries during early 2005.

Appendix C: Regulatory compliance references

Industry segment, regulator, and type of record	Typical retention period
Securities broker/dealers: new account records	Life of account plus six years
Pharmaceutical: FDA Good Laboratory Practices; records related to a new drug applications (NDAs)	Date of submission plus five years
Life insurance: policy information	Life of policy plus 6–10 years
Financial services: mortgage loan files	Life of loan plus 6–10 years
Healthcare: medical records	Life of patient plus "n" years
Government records	Many have a longer life (20–50 years, including permanent*)
Copyright records (all organizations)	Life of copyright = 95 years or as business needs dictate
Employee records (all organizations)	Termination plus 6–10 years
Employee medical records (all organizations)	Termination plus 30 years
General contract records (all organizations)	Life of contract plus 6–10 years
Utility (non-nuclear); FERC; plant records	Plant retirement plus 10 years

* Records transferred to the National Archives and Records Administration (NARA)

Following are examples of industries with a high risk for litigation.

Securities	Construction materials
Insurance	Food manufacturers
Healthcare providers	Automobiles, parts and tires
Consumer product manufacturers (toys, household appliances, and so on)	Pharmaceutical and device manufacturers

Following are examples of industries with a high risk for regulatory investigation (parentheses indicate the applicable regulatory agency).

Securities firms (SEC)	Insurance (state insurance commissioners)
Food manufacturers (FDA)	Pharmaceutical and device manufacturers (FDA)
Healthcare services (HIPAA)	Utilities—non-nuclear and nuclear (FERC and AEC)

Appendix D: DLT*ice*, WORM technology on HP StorageWorks SDLT 600 tape drives

SuperDLT (SDLT) tape technology also has WORM capability but it is implemented in a slightly different way compared to that of LTO technology. It is available on HP StorageWorks SDLT 600 tape drives with SDLT 600 media, and the brand name for the technology is DLT*ice*.

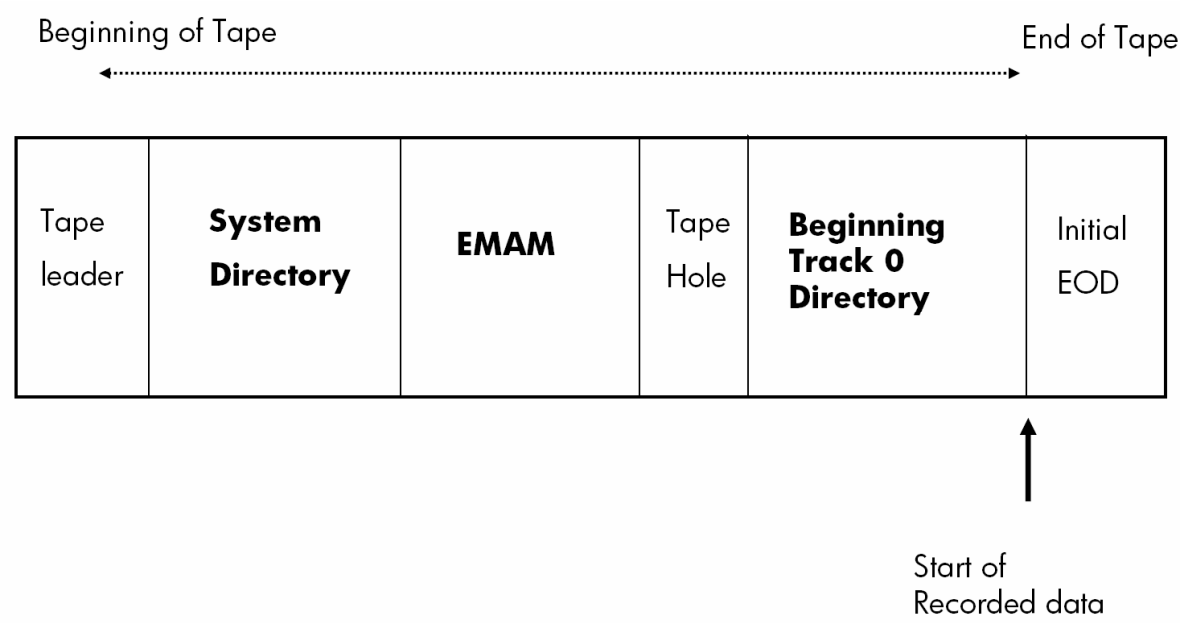
Feature	**SDLT 600 WORM tape (DLT*ice*)**
Capacity	300 GB native
Write/read speed	Write up to 36 MB/sec native Read up to 36 MB/sec native
Seek time or average access time to file	79 seconds average access time after media is loaded in drive
Special features	A special program DLTSage available only from Quantum is required to convert write/read media to WORM media. ISV backup software will also gradually support the ability to initialize WORM media for SDLT 600 during 2005.
Media life	30 years
Media cost (uses standard SDLTII media)	$169 list

DLT*ice* technology does not use specific WORM media but allows standard write/read media to be converted to WORM media by use of a specialist program (DLTSage) or by a utility program within the backup software that writes "WORM keys" to three protected areas physically on the media. Only when all three "keys" on the media are read by the tape drive and agree is the media deemed as valid (unaltered).

Media must be unformatted, formatted with no data on it, or formatted with one filemark and EOD to be eligible for conversion to WORM media. The SDLT 600 drive must have version 30 or later to support DLT*ice* functionality.

It is recommended that SDLT 600 media is bulk erased before WORM initialization to ensure that it can be converted.

Figure 17.



The bold areas in Figure 17 show where the WORM keys are written. The enhanced media auxiliary memory (EMAM) location on the physical tape media is also used to store other relevant media information. These areas can be written to and read from using the SCSI commands write media auxiliary memory and read media auxiliary memory.

Because the WORM-initialized media physically looks the same as write/read media, special yellow labels are supplied with the SDLT 600 media and should be applied to the media after it is converted to DLT*ice* media to clearly identify the media as WORM media.

The usage methodology is the same as LTO3 WORM media, in that after the WORM media has been initialized/converted, the media will only allow appends of data and not overwrites of data.

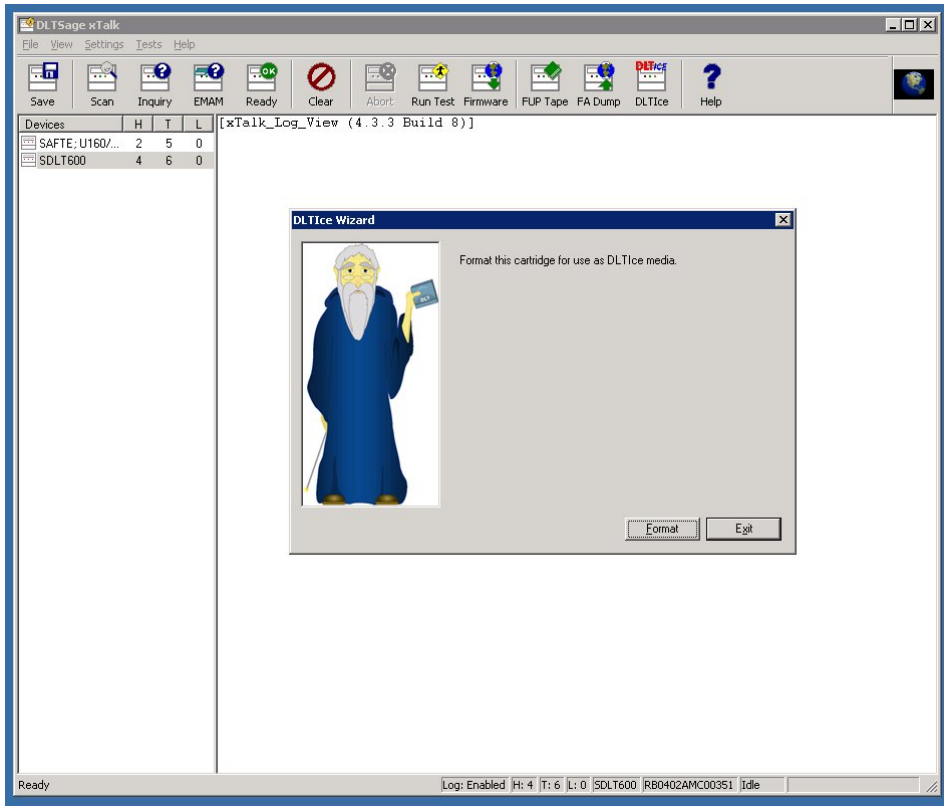
WORM media can be converted back to write/read media by bulk erasure of the media, which eradicates all data on tape (including the WORM keys). DLT*ice* is expected to be supported in the following ISV software:

- VERTIAS Netbackup
- CA BrightStore Enterprise Backup
- CA ARCServe Linux/Netware and Windows
- Legato NetWorker
- Yosemite TapeWare
- IBM Tivoli
- Commvault Galaxy
- Arkeia Enterprise Backup

VERITAS Netbackup 5.1 + Maintenance Pack 1 currently supports the ability to perform WORM cartridge initialization with HP StorageWorks SDLT 600.

Figure 18 shows the DLTSage Utility. Load the media, click the DLT*ice* logo on the toolbar, and the media is formatted as WORM media.

Figure 18.



For more information

http://www.hp.com/go/tape

http://www.hp.com/go/udo

http://www.hp.com/go/ILM

http://www.plasmon.com

http://www.xendata.com

http://www.k-par.com

European Union

http://europa.eu.int

United Kingdom

Information Commissioner

www.informationcommissioner.gov.uk

Data Protection Act (UK)

www.hmso.gov.uk/acts/acts1998/19980029.htm

Financial Service Authority

www.fsa.gov.uk

Stephen Mason, "E-mail and the internet at work: a concise guide to the legal issues" (Pario Communications Limited, 4th ed, 2004) ISBN: 0 9543245 3 6.

United States of America

Food and Drug Administration

www.fda.gov

Securities Exchange Commission

www.sec.gov

Public Company Oversight Board

www.pcaobus.org

U.S. Department of Health and Human Services

www.hhs.gov/ocr/hipaa

U.S. Department of Defense—Washington Headquarters Services

Directives and Records Division

www.dtic.mil/whs/directives

5983-0581EN, 01/2005

invent