Design Planning for the Records Center of the Future

Presented at ARMA International
Long Beach California
October 2004

By Hugh Smith
Firelock Fireproof Modular Vaults

Presentation available in Adobe .pdf format at www.firelock.com

Design Planning for the Records Center of the Future

INTRODUCTION

This presentation will describe records center design criteria capable of supporting your organization into the next generation of records management. It is intended to take a serious look at the functional performance that will be expected from records management as their control expands across the spectrum of all information assets. Our goal is to help you develop a comprehensive understanding of efficiency of design, incorporating adequate protection and appropriate security into the design plan as well as planning for growth and changing technology.

The Records Center of the Future must satisfy the information asset management needs of any organization. The participant should leave with a basic understanding of the following concepts:

How the records center will meet the challenges of protecting vital information assets in current and future formats?

1) What are the issues for achieving information longevity while protecting the records from identified threats?

2) What Standards are relevant to your design planning?

How the records manager will deliver a level of performance that relieves the organization of liability due to negligent records storage and protection?

1) Prudent Man issues or just keeping pace with the peer industry?

2) What are the regulatory pressures that impact on your design?

How the records manager provides immediate accessibility to records at appropriate levels of the organization without loss of control or security.

> **The proper management of records requires a collaborative effort between the records management. IT, legal, and audit functions to serve the overall needs of the organization. Security procedures must be consistent with a defined risk tolerance program to ensure a cost beneficial solution for executive management and the shareholders.**

NFPA 232 “The Standard for the Protection of Records” defines the role of the records manager as the “Responsible Party” in records center and vault design and specifically states that you are responsible to manage the fire protection design aspects of the records center. From selecting the fire protection engineer to guiding the architectural requirements, the Records Manager needs to be prepared to control the design process of the records center of the future. The records manager

must be aware of the standards, trends and emerging technologies that impact the protection of the information assets of the organization. This session will help you fill in the blanks of your future planning criteria to not only store information assets but protect them in a manner consistent with the controlling legislation.

Challenges for the Records Center of the Future

Paper is easy! We understand paper documents! But they only represent one third of the information assets in a records management program.

How does one make permanent a technology that was by its design temporary? Digital Preservation is an oxymoron to the very engineers who develop hardware and media for the Digital World of Information Management. Yet 90% or more of an organization's records begin their life as digital records and less than 30% migrate to the stable media of paper. The majority of vital and mission critical records remain in digital format and present an entire array of problems for the Records Manager and Information Technology Manager. These problems range from exponential growth to the virtual elimination of the enforceable retention period, due to a lack of established controls being exercised on the digital format records. Another concern is the permeable layer that fails to prevent records from flowing away from control. This same permeable layer that grants instantaneous access to the user is often under attack by viruses that threaten the integrity of the original master digital format records.

Organizational Management can also pose a threat to the records management program. Executive management addresses records protection in times of risk or regulatory enforcement, but can lose their will during periods of profit downturn or during mergers and acquisitions. Long-term preservation of information stored on electronic media is extremely costly; it requires a set of defined procedures for conversion and migration. Management has also turned out to be a threat to records during periods of wrong-doing and criminal activity. How does one protect records from the enemy from within?

Management can also pose a threat to a records management program by adopting new technology without regard to the ongoing preservation of records left orphaned by new information technology that runs faster but lacks compatibility. Technological obsolescence is the prime threat to legacy data.

To insure the long-term survival of digital format information the following procedures need to be implemented:

- The environmental storage conditions for the media must be designed by those familiar with the fragile nature of media, and include an appropriate conversion and migration strategy which addresses the records classifications and the associated retention periods.

• The records center must satisfy a wide array of needs to deliver protection of the information assets, including the system hardware, software and operating systems. The difficulties arise from the need to protect all the information assets for the duration of the retention schedule.

• Computer systems utilized for managing the information assets included in the records management system should be protected as part of the archival collection along with operating manuals and spare parts in the event of equipment failure.

To be effective in protecting media in a records center environment, the records center must be able to offer services similar to those being provided by an outsourced service provider.

• High-end data storage vendors are already offering these services providing media storage, offering e-vaulting, and recently some of these companies have added creation to tape capabilities.

• Imaging companies are expanding into offering media storage for the same data banks they created by mass imaging projects.

Autonomy is critical to protecting the media from a variety of threats. The records center must also have the ability to remain current to meet the various roles that it will provide over time to an organization. To function as the operational storage center, the recovery site and near line or online data bank, much thought must go into the long-term capabilities of this records center of the future. The records center must not be viewed as a cost center, but as an ongoing benefit to the well-being and profitability of the organization. The marriage of information protection and accessibility, resulting in superior business continuity, will define the success of this new records center.

What should we expect to see in the records center of the future?

E-vaulting will emerge as a reasonable solution within the records center as pricing for hardware comes down.

- The ability to provide a high integrity back-up will be as much a driver as the ability to recover information assets.

Mirror sites can be located in the records center along with the call center function to insure fail-safe capability.

- Terrorism and the dramatic fines and criminal penalties for loss of information assets have triggered a new wave of data center and information management enhancements.
- Creating vaults for the data production capability is popular in Europe and South America, and the trend is spreading to the United States.

Data mining is now a common function for many organizations and as such, creates a value added to an organization with strong records management capabilities.

Conversely, competitive intelligence and espionage promote storage of information assets off-line to all but those entitled to manipulate or access the data.

Estimates are that up to 50% of critical business data does not exist inside the organizational data center. Yet this same data forms the basis for the information on which today's business leaders make strategic decisions.[1]

Initiating the Design
Planning for the Records Center of the Future

RM and IT must collaborate with Facilities to develop solutions to protect the survival of the organization in this new world of information management.

Therefore the records center of the future design must accommodate the various types of media, as well as the access needs of the users.

Integrating immediate access for users while insuring long term protection of the record content is a challenge that must be addressed in the early stages of the design. Failure to address both needs will be catastrophic at some point in the life cycle of the records.

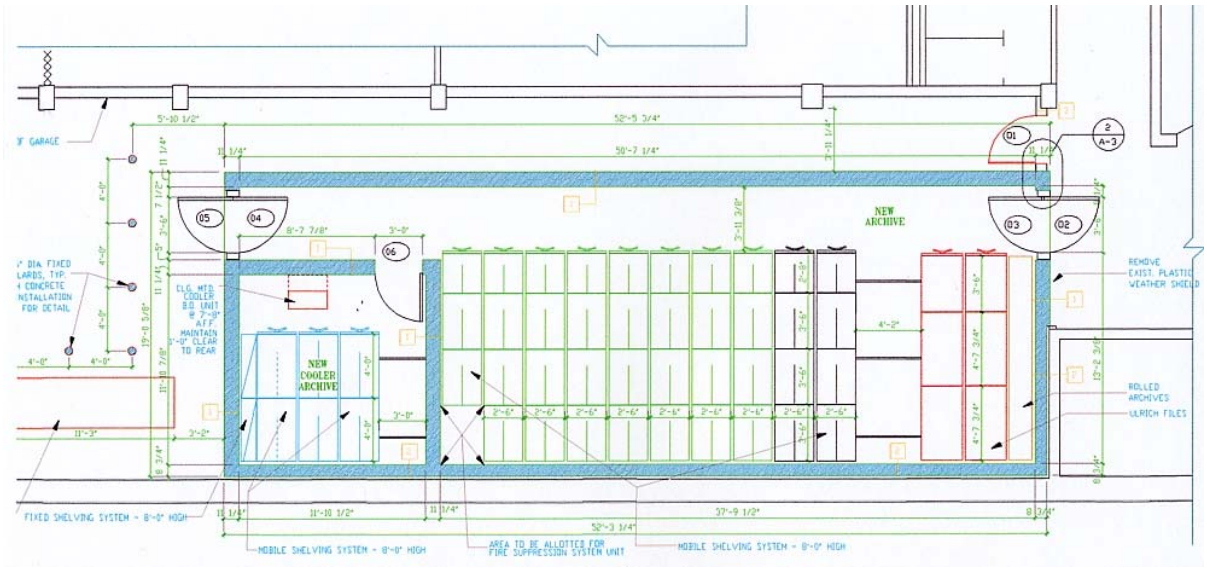
Recent efforts outlined in Standards such as NFPA 232 and NFPA 75 have attempted to reduce the risk to certain classifications of records by addressing design specification requirements for the: 1) records center building, 2)

[1] The Disconnected Data Dilemma, Craig McClellan, StorageTek, May 2, 2000

compartment size, 3) vault type and size, 4) environmental conditions, and 5) requirements for a Disaster Recovery Plan.
The computer equipment, which houses the massive volume of on-line and near-line mission critical information assets and records, can be considered vital to an organization. However, by design, a vital records repository should not be co-mingled within the active information management system. Records in computer media format are viewed as “vital records” in the new NFPA 232 Standard.

Both the Records Management and the IT communities are tasked with the protection of the records produced in the data center. Increasingly, the records center is becoming the fail-safe location for the protection of information assets. The records center provides the basic elements of any disaster prevention program: 1) distance from the data center, 2) proper management of the records, 3) physical security and access control, and of course 4) redundant master copies to the working set or on-line records. Recent legislation has made the CEO, the CFO and the Auditors responsible for ensuring the long-term protection of all the elements of the information management lifecycle. Managing the lifecycle of records, while familiar to records managers, is now becoming a concern to IT management, as well, as they seek to respond to new legal requirements for data protection.

Further proof of the co-mingling of functions is that the growing E-Vaulting community is now addressing tape storage and the offsite tape storage community is exploring the addition of technology for adding capabilities for E-Vaulting. In the end, it is still records protection, only at the earliest stage of records production prior to the classification of the records. How the records evolve in classification and value will still depend on legal requirements or circumstances that affect the record at various stages in its lifecycle. e.g., litigation, new legal requirements or value to the end user.



ENVIRONMENTAL STANDARDS:

Digital Format Records are generated and managed electronically, in a form that makes them more fragile than paper, and it is critical that we concern ourselves with preserving the accessibility of the information because of the unstable life of the media. The records manager cannot be concerned only with the loss of records due to catastrophic causes, but must also address issues such as environmental decay.

While protecting media from catastrophic loss by storing within a vault must be considered within the records center, the loss due to a catastrophic event is not as great a risk as loss due to the effects of poor environmental control. For this reason we place special emphasis on environmental control in this presentation.

Environmental Standards, such as ANSI IT9.11 for IMAGING MATERIALS - PROCESSED SAFETY PHOTOGRAPHIC FILM – STORAGE, ANSI/NAPM IT9.21 the standard test method to establish the life expectancy of compact discs (CD-ROM) and ANSI/NAPM IT9.23, the standard providing appropriate recommendations for the storage of magnetic tape must be used to establish the requirements for storage of film and electronic media.

Care must be taken to concern ourselves with the operational use area (data center or server room) of the media, because cycling media in and out of a master storage or archival environment to serve as back-up requires that we consider the temperature of the computer room or use environment. Here the computer equipment dictates the proper temperature and humidity requirements for effective operation of the computer equipment and tape drives. To avoid cycling the temperature through the 5º F. cycle level, the storage environment for back-up media should be the same as the computer room or use environment. This is typically 65º- 68º F. in standard design applications. Therefore, to extend the life of the media, the designer should plan the vault environment to maintain a constant state of 30% relative humidity. By reducing the humidity and eliminating cycling temperatures, the life of the media is extended and the stability of the media is improved by avoiding the stresses which are known to shorten the life of the stored master media units.

Furthermore, the minimization of dust in the environment through the use of special filtering devices such as HEPA filters increases the life span of the media. It is recommended that dust and vapor resistant light fixtures be utilized within the media vault chambers.

Magnetic shielding should be considered within the archival or media vault. Storage areas should be analyzed for the presence of magnetic fields as continued exposure to fields of 10 milligauss can alter the information contained on magnetically recorded media.

Additionally, off-gassing from laser printers can negatively impact media and care should be exercised to avoid storing media adjacent to the processing equipment.

Since damage to media begins at 120ºF., it is also critical to control the rotation methodology of media from storage to the use environment and back again. Refrigerated vehicles should be outfitted with air conditioning equipment which continue to operate even when the delivery vehicle is parked to ensure damage does not occur during transit. Special transit containers are required to protect the media from impact shocks, magnetic fields and other risks encountered in the delivery path and from outside elements.

Even in a paper storage environment it is important to consider environmental controls, as it is recommended that air be completely circulated at least three times each hour to avoid mold and mildew developing on the paper records.

PLANNING FOR THE VAULT CHAMBER

In the outline to follow, the various factors the records manager must consider in the design planning for the Records Center of the Future will be detailed. One key issue is protecting the documents you consider most vital. But in the role you play as Gate-keeper you are tasked with protecting documents that are not always in paper format. In the past, an insulated file cabinet could protect paper documents and provide the fireproof label you required. As you moved into computer media, you advanced to Data Safes with Class 125 Fire Protection Labels.

This same issue confronts you with protecting your media now that it is part of your role in protecting all the information assets regardless of the format the records are stored in. Now you are looking for fireproof labels and data safe chambers to protect potential huge amounts of information assets.

Just as environmental control took a jump up in specific control, you must now address different fire protection ratings and enhanced needs for security in your new center. The only way to effectively protect the organization's information assets is to perform a step-by-step planning program to answer your design questions as they relate to your organization. It is our intent to provide this criteria in the following pages.

RECORDS CENTER DESIGN PLANNING CRITERIA:

The records center of the future will satisfy these needs to be a viable repository for the active, long term and vital records of the organization…

Information protection must be designed to protect assets in a solid cascade from digital birth to online storage to tape Storage……. the integrity must be absolute.

- Technical solution is prime with repeatable proof
- Back up program with restorable capability
- The production platform must be integrated with the storage platform
- Information must be continually available for delivery

Integrity requires a continual “Gatekeeper” function

- Proof that information is complete
- Proof that information is un-tampered
- Proof that the complete set is available
- Proof that is understandable to a jury of society's lowest common denominator
- Proof that will satisfy a critical auditor

Security of information assets

- Cannot be destroyed accidentally
- Cannot be stolen
  - -Is impervious to environmental decay
  - -Is able to migrate -software and hardware
  - -Is protected from criminal activity
  - -Is protected from catastrophic destruction

Efficiency of storage

- The user must be able to find desired records
  - absolute integrity in the tracking software
  - reduced search costs
- Store at efficient cost level
  -reduce retention periods to control cost
- Minimize threat of expired records being discovered after scheduled destruction date

RECORDS CENTER DESIGN PLANNING CRITERIA:

The records center should deliver a substantially lower cost of ownership of the records while providing the dedicated user instant access within a secure environment.

- Cost of ownership must detail in case study analysis
  -actual costs incurred by destruction
  -savings achieved by avoiding major losses

- "Average box sits on shelf for 16 years." (PRISM)
  -this is a defect that records management must seek to eliminate
  -cost savings from improved life-cycle management will fund modernization of information management

Enhanced security of the electronic documents provides an incentive for lowered dependency on paper documents

The records center's mission in protecting records:

- Eliminate the loss of income that results from prematurely destructed records. (e.g. Accounts payable)
- Support the errors and omissions policy
- Provide documentation necessary to protect against claims of gross negligence or fraud
- Avoid loss of reputation -- loss of stock value
- Provide documents necessary to avoid legal liability –
  - criminal punishment for the ceo & cfo
  - civil penalties that punish the organization

THREAT RISK ASSESSMENT

What are the threats that the records center must be able to withstand? New threats evolve and persistent threats plague the records center of the future.

Identified threats: (in-house)

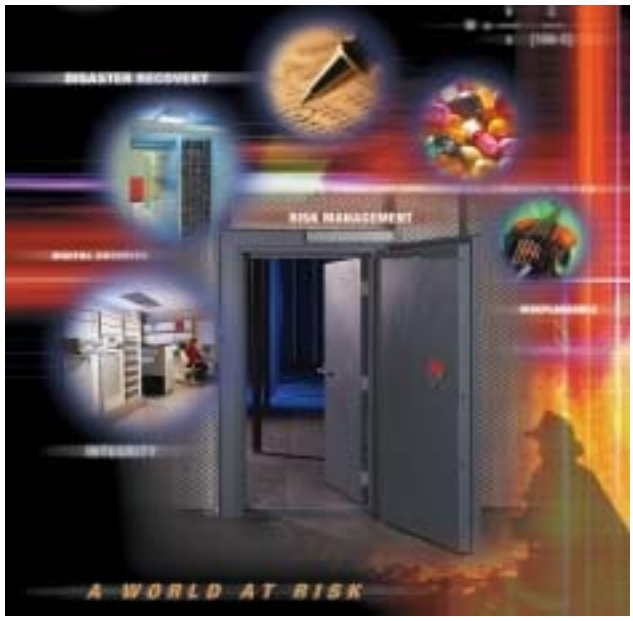
- Deliberate destruction to hide evidence of wrongdoing
  - To hide evidence of product liability
  - To hide criminal activity
  - To prevent loss of equity in stock value by concealing information that would affect stock value

Identified threats: (external agents)

- Accidental loss is no longer prime
  - Arson is the leading cause of fire
  - Repositories are desirable targets for terrorists
  - Espionage and sabotage
  - Domestic radical groups

Identified threats: (adverse interests)

- Imperfect technology
- Fragile media
  - Manufacturers continually choose volume and density over stability as the prime attributes of their product
- Trade associations fight to weaken standards
  - -Avoiding cost increases at the expense of safety
- Non-interested IT management
  - Production driven, not performance driven
  - Hardware centric, not information centric
  - Failure to take the long view on records
- Records managers have been too concerned with storage and not user's access to information assets
  - Myopic view of business continuity
- Poor image from the user group
  - Impediment to user's access to records
  - Storing documents no one really needs
- Hardware and software obsolescence to promote sales
  - No support for existing technology
  - Owner must continually migrate data
- Security emphasis must be on the active records
  - One set of active records is always at risk
    - ~ Exposed to sabotage



"The usual answer has been to archive boxes full of papers off-site. But the horror of September 11 - with its "rain" of documents over lower Manhattan - made it clear that archives are not the critical issue. Your most vital paper-based records are probably the ones in active use today, from contracts to regulatory filings, claims files to purchase orders, technical drawings to financial reports."

AN OVERVIEW OF INCORPORATING SECURITY INTO THE DESIGN PLAN

The records center design should facilitate the information assets being protected to the retention schedule

- All types of mission critical information assets should be protected along with the software configuration and the hardware necessary to achieve the full term of the retention schedule.
- The retention policy should be reviewed to minimize the terms of all document types so that documents are not kept beyond the required life-cycle
- The records model should enforce the number of duplicate records in the system so that bonafide destruction at end of the life-cycle can be achieved.
    - A horrific volume of records exist in one format or another after a certificate of destruction has been provided to records management
- The records center should promote organization of the information assets as well as the ability to achieve the longevity required of all the records media.
- No records can exist outside the control and security of this facility so that a scheduled destruction can target all versions of a document
- Information assets should be available across the client-base in a searchable and structured on-demand format for instantaneous use by approved clients.
- The organization shall be designed so that each migration of data requires a review of the records
    - Out of date records are purged
    - A determination as to whether the media format can survive the evolution to the next technology or hardware evolution

MANAGEMENT IS LOOKING FOR DIRECTION ON THE FUNCTIONAL PERFORMANCE REQUIREMENTS OF THE INFORMATION MANAGEMENT PROGRAM. HUGE AMOUNTS OF MONEY ARE BEING SPENT TO ASSURE COMPLIANCE. THE RECORDS CENTER OF THE FUTURE HAS A DYNAMIC ROLE TO PLAY IN DELIVERING THIS FUNCTIONAL PERFORMANCE WHILE PROVIDING THE ORGANIZATION THE SECURITY THAT CURRENT LEGISLATION MANDATES.

FUTURE INFORMATION REPOSITORY TRENDS

Functional performance requirements:
Protection must begin with the genesis or creation of the information asset.

- Methodology must incorporate electronic records from the production platform,
  - Imaging paper documents into a monolithic entity, archiving email, instant messaging and soon voice records.
- The genesis or master records must be free from threats, while the operational records must be available to the dedicated user instantly.

Distribution of information assets
New fiber and web communications make transfer of information from records production platforms and data centers to storage centers and mirror sites almost instantaneous.

Drastic reduction in hardware costs and networks of high-speed communication wiring coupled with the density of information storage facilitate these new designs.

Records identified as permanent or vital can be output to microfilm for vaulting or offline storage.

Imaging of incoming documents that are also identified as being vital allow long term storage while placing the information into the data base for instantaneous access across the proprietary network.

Managing growth

As the digital archive grows the records manager must be able to address issues of:

- Accidentally deleting files
- Corrupted files due to missing metadata
- Losses due to viruses or sabotage
- Loss of control for new record types

These technology failures can lead to criminal penalties for executives charged with negligent or willful spoiliation and an expectation of extremely large fines by regulators.

In addition, there is a loss of image and integrity in the marketplace when CEO's and CFO's are charged with criminal charges that leads to loss of stock value and investor confidence.

In light of the downside, the investment in an effective records management program is then very beneficial to the organization.

DEVELOPING YOUR UNIQUE DESIGN PLAN FOR YOUR RECORDS CENTER

Develop Your Specific Prototype

- Visit other records centers and develop a plan
- Visit Data Centers and Mirror Sites and develop a plan
- Solicit design planning from internal departments
- Develop support for the prototype while in schematic stage
- Look for criticism not support in the early stages to validate the design
    - Get advice from other records managers
    - Get advice from vendors
- Finalize a rough draft before searching for a site or a facility
- Assemble the relevant Standards (NFPA 232, ISO 154891)
- Determine early on whether center will be a business continuity site
- Build into the model future growth on the site or within the facility design

Selecting the Design Elements of Records Center Components

- Type of Facility
    - Freestanding or combined
    - Proprietary or multi-use
    - Owned or leased
- General Records Storage Areas – Active Records
- Secure Data Platform
    - RAID, SAN, NAS Environments
    - E-Vaulting
- Man-traps and access control components
- Microfilm Storage and access area
- Vault Area for Vital Records
- Vault Area for Data Storage
- Staff Office Areas
- Conference Rooms
    - Audit Areas (SAS 70)
- User Viewing Area
- Staging areas for documents and media
    -Staging areas for both receipt and departure
- Mezzanine or Picker type shelving design
- Visitor and Vendor control areas
- Hierarchical zone control from building exterior to most secure zones
    - Controlled access at all times
- Docks and Receiving Bays for records transit.
- Control areas for destruction
- Lounge and rest room areas
- Janitorial and Cleaning supply areas
- Accession areas for bulk transfers
- Disaster Recovery War Room

Mechanical Rooms

- Telephone Equipment Rooms

- Pump room for sprinkler system
- Mechanical and Equipment Rooms
    - -HVAC room
    - - Batteries and generator equipment
    - -Transformers
- Equipment and Spare Parts Storage
- Back up Generators

Selecting the Site

- Desired Proximity to Users
- Proximity to fire station and police station
- Requirements for Turnaround time on records
- Evaluate the site
    - - Flood Plain, risks in adjacent occupancies
    - - Water run off
    - - Wild fires
    - - Risk of hazardous adjacent tenants
- Traffic Analysis
- Potential for building set backs, security fencing, traffic control
- Risks of hazardous materials
- Neighborhood crime
- Employee safety
- Environmental study should be done on site (Phase III)
    - - Underground tanks, groundwater contamination

Selecting the Building

- Structural soundness of building and roof
- Ceiling heights
    - -Determine shelving heights and floor loads
- Floor load capacity
    - - Based on height of shelving and media being protected
- Quality of floor surface
    - - Laser-flat for shelving height above 20’
- Loading and delivery docks and bays
- Existing back up generator
    - - Can a generator be added in the future
- Security of building design
    - - Minimum of windows and doors
- Compartmentation of building
    - - Improved fire protection
    - - Facilitates Security Zones and access control
- Electrical service to building
- Water supply for sprinkler system and fire fighting
- Proximity to airport
- Traffic concerns in a disaster
    - - Is pathway from records center to user group viable in the event of a natural disaster
    - - Proximity to recovery facilities or airport
    - - Flooding, seismic area, wild fires, poor roads

Age of the facility
- Appraisal of existing wiring
- Contamination from mold, asbestos and environmental hazards

• Quality of electrical service
• Structural analysis
• Roofing material – Age and quality
- Flat roof concerns

• Sprinkler system
- Age and certification
- Fuel load design
-Compatibility with intended use

• Building Code effective at time of construction
• Fire Rating for the structure.
- Is the building four hour rated

• What is the structural design load of the building
- Will the building survive a shelving collapse

• In a seismic activity zone, is the building design adequate
• In a hurricane prone area, what is the height above sea level
- Is the building accessible in times of a storm

• In snow load area, what is the capacity of the roof.
- Is a snow loading area possible

Develop the Security System Plan

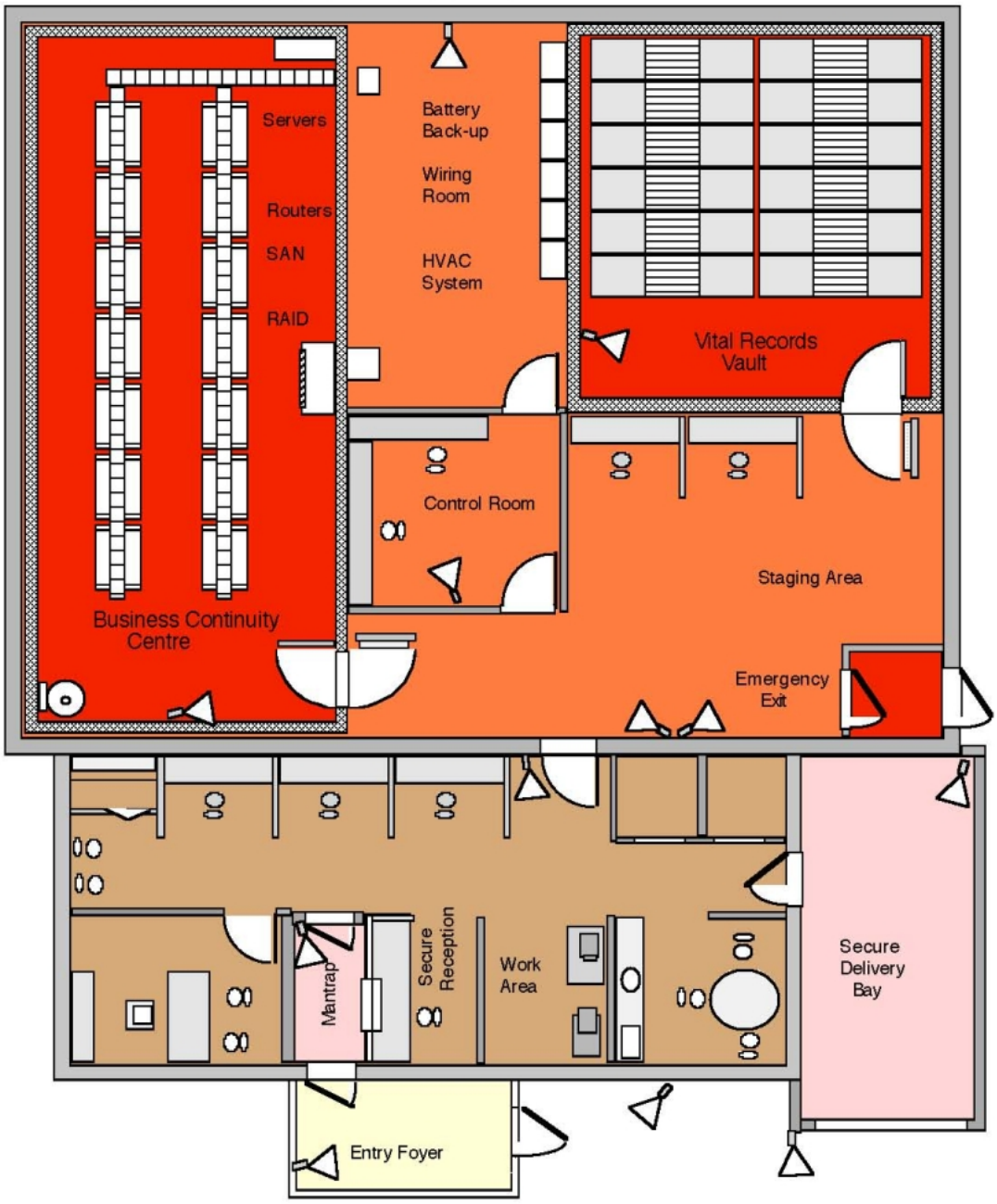
• Perimeter Security
- Smoking areas outside the building are a security risk
- True security starts at the property line
- Vendors must be escorted onto property

• Access control for the secure zone
- How many levels of security are appropriate
- Card and pin pad for dual control
- Time zoned with anti-passback
- Synchronized with the surveillance system
- Synchronized with the alarm system
- System must prevent tail-gaiting

• Surveillance Systems
- Monitored or unmonitored
- Digital cameras allow remote monitoring (web monitors)
- Hidden Cameras with motion sensors

• Central Station reporting
• Environmental alarms
• Water sprinkler alarms
• Fire Alarm detection
- Traditional or VESDA Type
- What temperature will water release
- Infrared detectors for components of combustion for data environments

Records Center of the Future



Fire Suppression and Alarm Systems

- The records center will employ a water sprinkler system for the box storage areas (Misting Systems may also be employed)
  - Choices will include large drop heads or in-rack systems among others
  - The Responsible Party chooses the fire protection engineer and the appropriate choices will be described by the engineer
- The media vault chamber and data chambers will typically employ gas suppression systems. Not all gases are equal
  - NOVEC 1230, FM 200, FE-13, FE-227, etc may be used
  - Hypoxic environments and Inergen are also possible but carry

certain life safety risks due to lowered oxygen content and volume of gas that must be forced into the environment
- Life safety must be considered for vault staff – Toxicity levels
- Residue on media and acid levels on the media are a concern
- Not all gas systems are equal in performance

• Water and gas systems and the alarm panels require maintenance and inspections and this must be rigidly monitored

Physical Facility Security Design

Can you control access to the areas adjacent to the building
What are the wall construction and roof construction
Is visibility on sides of the facility designed to prevent intrusions
Avoid concrete bollards that become propellants in an explosion
Unmarked building and delivery vehicles for proprietary facilities
Vans should be able to unload in enclosed bays
Loading doors and docks should not face traffic side of building
150' – 200' setbacks from roadways to building
Access road for fire trucks on all sides of building

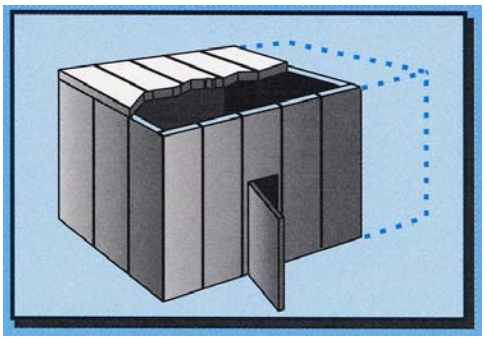
Access and Traffic Control

Access control systems and the facility design should be used to progressively handle traffic within the Centre. Some evaluation such as a Threat Risk Assessment should guide the determination of the security methods employed. The Zones may follow this pattern:

• Site Control
• Public Zone
• Reception Zone
• Operations Zone
• Security Zone
• High Security zone
    -Records Storage Areas
    -Electronic Records Storage Platform
• Mechanical Systems (Pump Rooms, Back-up generators, Alarm Panels)

Phased Growth for Physical Facility

Lack of expansion space often degrades existing security
Prepared phased growth drawings at project inception
New requirements for office space in the records center
    Provide additional parking area space
    Provide additional support areas (Lounge, rest rooms, etc.)
    Avoid loss of integrity in secure zones



Life Safety Issues

- Access Control to the site itself
  - No unsupervised visitors
  - Prevent unauthorized vehicles from proximity to the building
- Exterior Lighting should promote safety and discourage crime
- Ease of access for fire fighting equipment
  - Location of hydrants
- Fire Exits are not impeded by interior storage volumes
- Air quality within the records center
- No chemical storage on site (cleaning chemicals, paints, fuel)
- Fire Wall separation between areas and rated fire doors
- Smoke evacuation equipment in use
- Skylights and emergency lighting
- Cross ties and bracing to avoid shelving collapse
- Elimination of hazardous building materials from project

Heating, Cooling and Dehumidification, Electrical Systems

- The addition of media storage mandates special control
- Heroic environmental systems are required
  - Special dehumidification is required
  - Back-up generators may be required
  - Special switch gear to avoid power loss (UPS)
- Redundant systems may be called for
- Emergency power grid must be designated in advance
  - Not everything needs to be backed up
- What type of fuel system is required for the generator
  -Where will the tanks for fuel be located to avoid risk
- Tank size should be determined by worst-case outage model
  - Hurricane or Seismic area may create long-term outages
  - Special protection for transformers
- Surge suppression in place for system
  - Energy spikes and lighting strikes

Protecting the Vital Records

Protecting the vital records of an organization are mandated across the international spectrum. Again and again, countries and standards bodies have addressed the issue of protecting those records vital to the business continuity of an organization, government agency or corporation.

The requirements to protect vital documents in all media formats are described in consistent terms in the following Standards:

- International Standards Organization - ISO 15489.1 Records Management
- Australian Standard AS 15489 equivalent to ISO Standard
- British Standard - BS 5454:2000 Recommendations for the Storage and Exhibition of Archival Documents
- Historical Manuscripts Commission: HMC Standard for Records Repositories
- Canadian FC 311 (M), Standard for Records Storage
- National Fire Protection Association NFPA 232 - Standard for the Protection of Records – 2000

In each of these documents they describe a responsibility to protect the vital records, regardless of the format that they are archived in: paper, parchment, film, microfilm, magnetic media or digital or electronic formats.

What is unique in our current situation is that the mandates to protect records are now backed up by civil and criminal penalties for both the individual and the organization. The management team for the records must protect the records from destruction, unlawful distribution or willful spoiliation. The management is now driven by legislation such as:

- Sarbanes Oxley
- Graham Leach Bliley
- SEC Rule 17 (a)
- HIPAA
- The Personal Information Protection and Electronic Documents Act

The combined effect of these and upcoming legislation are forcing management to be more aware of the methodology for protecting vital records in their various formats. The risk of inaction combined with the risk of incarceration are all the incentive that the management and board room require to direct action in improving the protection of mission critical records.

Changes in the way information assets are created and stored in the organization have forced us to move the methods for protecting the assets closer and closer to the creation of the information assets. The trend is being established to protect the Main Frame Computer System that produces the records or the Servers, Storage Area Networks and the Redundant Arrays of Inexpensive Tape Drives that store the information in a business continuity center. The lower cost of equipment along with the reduced size required for mirror sites has made the vaulting of data rooms a viable approach to information integrity and business continuity planning.

This trend has been enhanced by the development of vault chambers that can deliver a Class 125 vault environment that protects both the computer media as well as the tape drives, servers, routers and peripheral equipment.

Vault Design Categories

Vault Design – Paper Documents – Class 350 Fire Vault

Design the vault to NFPA 232 Vault Requirement

Vault Design – Media Vault Chamber – Class 125 Media Rating

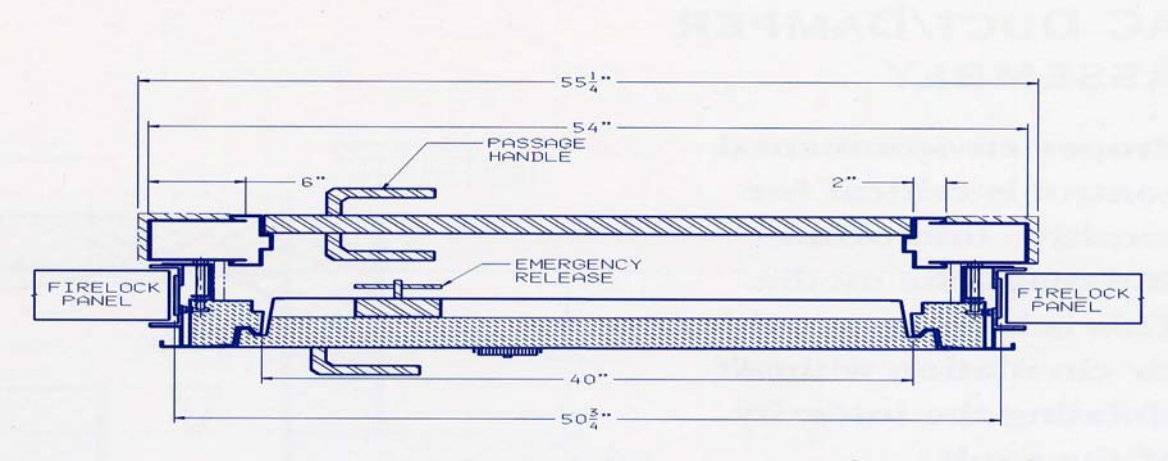
Design the vault to comply with NFPA 232, NFPA 75
Design to comply with UL 72 Test Standards for Media Protection

Vault Design - The Data Center Platform – Class 150 Media Rating

Design the Data Room to comply with NFPA 75 for the computer hardware and equipment (Servers, Hard Drives, Routers, SAN, etc.)
Design to comply with UL 72 Test Standards for Media Protection

Vault Design Elements – Vault Doors, Man-trap, Fire Dampers

- The vault door shall provide protection from intrusion
  - Dual control locks should be part of the security design
  - The door should include relocking devices to protect from attacks
- The vault door rating shall be consistent with the Vault Rating
  - The vault door for a media vault shall deliver a Class 125 Rating
  - The vault door for paper document storage shall deliver a Class 350 Rating
- No single vault door will provide Class 125 Two Hour or greater protection for computer media – a double door assembly is required

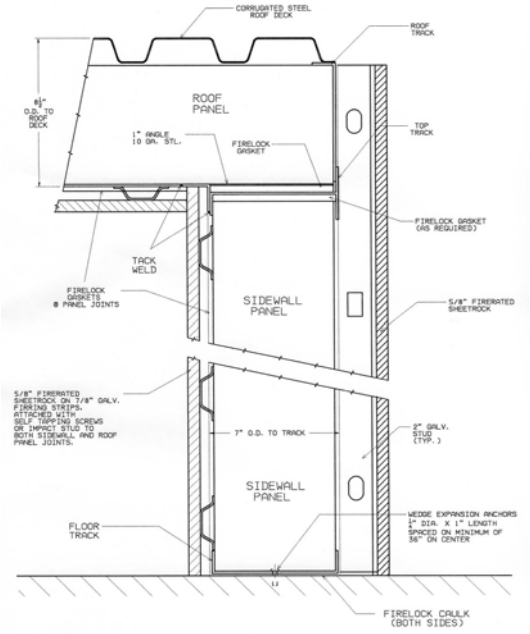


- The inner door should provide:
  - Card Access to track vault traffic
  - Vapor barrier protection for smoke and steam
  - Tightness for design concentration on the fire suppression gas
- The Door Assembly should allow emergency egress in an auto-close event or a power loss closing
- The door assembly should lock out undesirables during an auto-close
- The doors and chamber should combine to prevent steam, smoke or toxic gases from entering the vault chamber during a catastrophic event.
- The door assembly should have auto-closers which are triggered by smoke detection, heat detection, detection of flammable gases, an alert from the alarm system or interior fire suppression panel or power loss

- Mock drills with the fire department shall educate the fire fighters as to the proper procedures for fighting fires in the records center in and near the vault area
- A man-trap foyer shall be part of the media vault design plan.
  - Allows for additional tiers of security near the vault
    ~ High Security Control zone (access control)
  - Facilitates the environmental stability of the vault
  - Provides a secure staging area for ingress and egress of assets
  - Provides an additional fire wall barrier around the vault entry
  - Prevents clutter in the vault and improves efficiency
  - Provides risk reduction for the media in transit
  - Minimizes accidental discharge of suppression system
- The interior lighting for the vault shall include emergency lighting for egress from the vault in the event of a power failure or fire event
- A phone should be located on the interior of the vault
- Klaxons and strobe lights should alert personnel in the vault of an alarm
- Environmental control must be accomplished with fire rated dampers or through the use of a split system environmental package
  - Motorized louver dampers must also be utilized to seal of HVAC System from the vault chamber to prevent smoke from entering the vault and to provide containment for the fire suppression gas

Vault Design Elements – Wall and Ceiling Construction

- Vault Design must consider the threat risk assessment of the geographic area in which the vault is located
  - Is the vault in a seismic area
  - Is the area prone to hurricane or tornado events
  - Is the vault designed to be above the flood plain
- Structural integrity of the vault from collapse from above
  - Structural load for vault ceiling (300 lbs/sq.ft. load)
  - Is the strength of the vault calculated after exposure to fire
- Vault walls and ceiling shall be structural in a fire
  - No walls of the building shall serve as a wall of the vault
  - Fire resistant walls are not equivalent to a vault wall
- Walls shall be able to resist fire hose spray and sprinkler discharge without damage to the vault interior contents



- Wall penetrations for conduit and sprinkler piping shall not void the Class Rating for the wall and ceiling
  - Special Cable Trays are required

- Structural steel assemblies from the building structure shall not penetrate the vault interior chamber
- Walls of vault shall serve as a vapor barrier against moisture, steam, smoke and gases which may endanger the vault contents

Vault Storage - Care and Handling Issues

- Media should be stored in a slotted media cabinet for long-term storage
  - Cartridges to stand on end for tape tension
  - Tension system on slots to avoid cartridges falling from units
- Rolling carts should be used to avoid dropped cartridges
- Enclosed cabinets for protection from sprinklers discharge and fire hose • Enclosed cabinets for protection from dust particles
- Enclosed cabinets for protection from UV light
- Transfer Cases to be designed to avoid shocks to media in transit
  - Media should be secure in case with padded slots or spaces
    - ~ Cases should be equipped to avoid tampering
    - ~ Cases should be equipped to avoid unauthorized access
    - ~ Magnetic shielding on case interior – metal case
- Vault Floor to be anti-static finish or painted seal-coat finish
- Microfilm should be tested for vinegar syndrome before storing in vault chamber with other media
- Media should be stored in sealed containers (cartridges or cans)

Storage methodology

- Media should handled by staff knowledgeable about the fragile nature of the media
- Staging areas are necessary for bar coding media prior to slotting in storage containers inside of vault
  - Staging areas should be secure and access controlled
  - Media should move into staging area immediately upon delivery to records center
- Sufficient work space should be available to allow for wanding or coding the new media into the tracking software system.
- Staging areas should be clean and environmentally controlled.
- Staging space should clearly delineate the media moving into the vault as well as the media out of the vault during back ups or removal of tape from service.

Imaging Area

- Due to the equipment utilized, the air circulation from this area should not be on the same zone as the vault or the staging areas
- Special electrical circuits will be required due to the electrical draw for imaging equipment
  - Special breakers are required for this equipment
- Staging areas for the paper document which are being scanned must be provided
  - Staging areas for document in and documents out should be clearly marked to avoid destructing records prior to imaging
- Output from the imaging system whether microfilm or computer media must be immediately be entered into the software tracking system with bar codes and identifiers.

Microfilming Zones

- Due to the equipment utilized, the air circulation from this area should not be on the same zone as the vault or the staging areas
- Special electrical circuits will be required due to the electrical draw for imaging equipment
  - Special breakers are required for this equipment
- Staging areas for the paper document which are being scanned must be provided
  - Staging areas for document in and documents out should be clearly marked to avoid destructing records prior to imaging
- Output from the microfilming department must be immediately be entered into the software tracking system with bar codes and identifiers.
- An inspection program must be part of this process to verify quality.

Destruction Areas

- Shredding areas require separation from the records storage area
  - Dust and debris pose a threat to records center
  - Special detectors should be considered for this area
- This area should be treated as a high security area
- Special care should be taken to provide proper staging areas
  - Avoid wrongful destruction of records
  - Insure that scheduled destruction files are destroyed
  - Special coding should be used for identified records
- Third party destruction should have a special bay for this function
- Certification statements on all destructed records

Author's note:

This is a special area of concern as case history after case history has shown that records shown as destructed have continued to exist in the offsite records storage facility. A constant complaint of corporations changing records storage vendors, is that records certified as destructed remain in storage and the company has been paying the storage costs. This impacts the litigants position in a civil action when records reported as destructed are found on discovery.

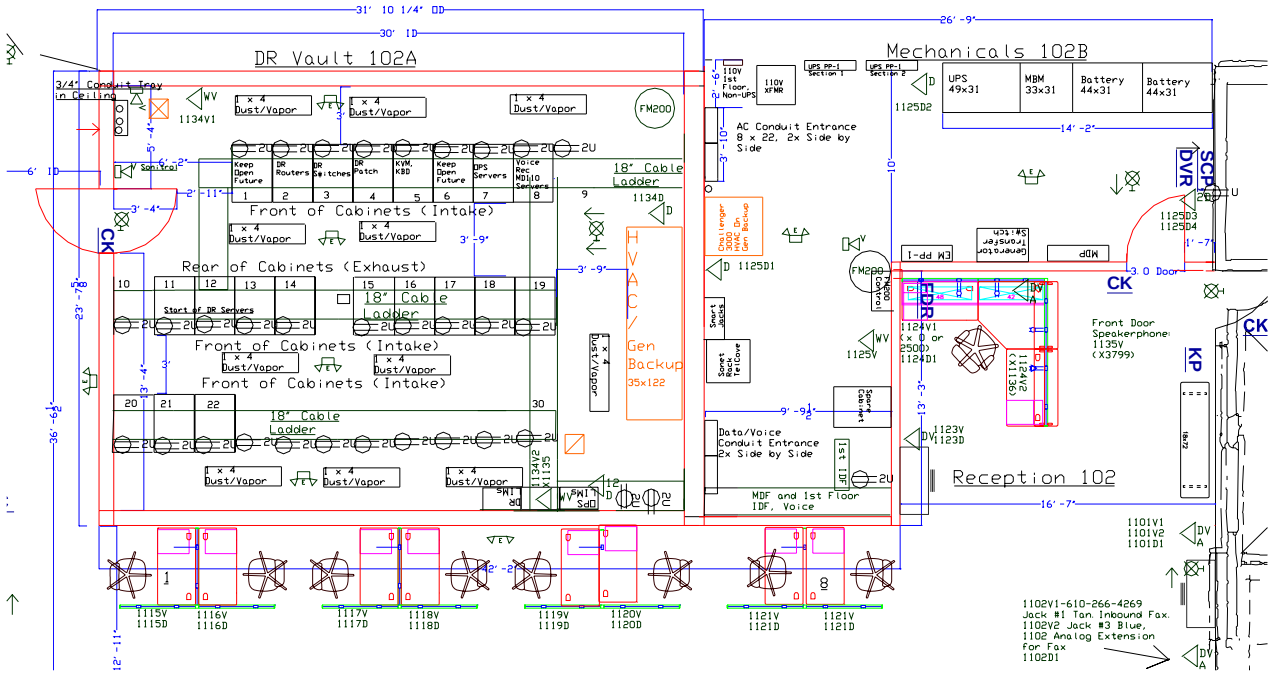
Business Continuity Centre

The role of the Business Continuity Centre can have many versions but the primary purpose is to insure that the organization can continue it mission critical functions. Depending on the investment the organization is willing to commit, this can take various forms.

In our discussion of a Records Center of the Future, the center will have as part of its function a business continuity platform. This new type facility will provide the greatest security and flexibility to the organization. In the event of a disaster at the main data processing facility, the platform at the records center is up and running and can, at any time, take over the processing function from the prime processing center.

Depending on the size of the organization, a number of servers may be required in the network which have SAN units attached which provide for a large volume of information asset and data storage. This provides a redundancy of data and backups that are not tied to any one server or application. The Storage Area Network (SAN) can be shared across many servers. The Storage Area Network will typically employ Redundant Arrays of Inexpensive Disks (RAID) to provide fault tolerance to the system. If there is a defect or loss in some data asset, the RAID has fault tolerance that will rebuild the damaged or missing data. In addition these units then improve the performance of the entire system.

Business Continuity and Disaster Recovery Centre



The routers, servers, DR servers, RAID and SAN along with the switch equipment units must all be protected within a secure environment equipped with specialized environmental control equipment. All of this computer equipment and the HVAC

System must be attached to a generator system that can maintain operation in a power loss. This area must also be protected from intrusion by means of card access control, security type locks, security type doors, surveillance cameras and digital recorders.

Tape drive output is often part of this center and the ability to have a recovery center located in the same facility as the tape vault is an advantage in a full-scale recovery. Tapes are immediately removed from the tape drives and stored within the vital records vault. The fact that the records center is manned during the day offers an extra level of protection to this redundant processing center. In the event of a virus attack, the back up tapes are immediately available for loading back the system to pre-virus condition.

The fact that the tapes are outside the control of the IT staff offers a dual level of security, as these back up tapes must be accessed through records management.

There are real estate savings by combining the functions of records center and business continuity into one secure site.

The new trend is vaulting of the business continuity center due to the fact that when the main platform suffers a catastrophic event, then the redundant center is the only functioning center and as such should be protected with the highest level of protection available.

Establishing The Legal Authority That Controls The Design Of The Records Center Of The Future?

International Standard 15489.1 Records Management Standard

"Appropriate storage environment and media, physical protective materials, handling procedures and storage systems should be considered when designing the records system, knowing how long the records will need to be kept and maintained will affect decisions on storage media. The records system should address disaster preparedness to ensure that risks are identified and mitigated. Integrity should be demonstrably maintained during and after recovery from disaster."
(**ISO 15489.1 Records Management - 8.3.3 Physical storage medium and protection)**

"Records should be stored on media that ensure their usability, reliability, authenticity and preservation for as long as they are needed (see 8.2). Issues relating to the maintenance, handling and storage of records arise throughout their existence, not only when they become inactive."

"Records require storage conditions and handling processes that take into account their specific physical and chemical properties. Records of continuing value, irrespective of format, require higher quality storage and handling to preserve them for as long as that value exists. Storage conditions and handling processes should be designed to protect records from unauthorized access, loss or destruction, and from theft and disaster."

"Organizations should have policies and guidelines for converting or migrating records from one records system to another. Systems for electronic records should be designed so that records will remain accessible, authentic, reliable and useable through any kind of system change, for the entire period of their retention. This may include migration to different software, re-presentation in emulation formats or any other future ways of re-presenting records. Where such processes occur, evidence of these should be kept, along with details of any variation in records design and format."
(**ISO 15489.1 Records Management -9.6 Storage and Handling)**

"To ensure the authenticity of records, organizations should implement and document policies and procedures which control the creation, receipt, transmission, maintenance and disposition of records to ensure that records creators are authorized and identified and that records are protected against unauthorized addition, deletion, alteration, use and concealment."
(**ISO 15489.1 Records Management 7.2.2 Authenticity)**

"The integrity of a record refers to its being complete and unaltered. It is necessary that a record be protected against unauthorized alteration. Records

management policies and procedures should specify what additions or annotations may be made to a record after it is created, under what circumstances additions or annotations may be authorized, and who is authorized to make them. Any authorized annotation, addition or deletion to a record should be explicitly indicated and traceable."
(**ISO 15489.1 Records Management 7.2.4 Integrity)**

8.0 Records Center Software
Any system deployed to manage records should be capable of continuous and regular operation in accordance with responsible procedures.
A records system should
a) routinely capture all records within the scope of the business activities it covers,
b) organize the records in a way that reflects the business processes of the records' creator,
c) protect the records from unauthorized alteration or disposition,
d) routinely function as the primary source of information about actions that are documented in the records, and
e) provide ready access to all relevant records and related metadata.
The reliability of the system should be documented by creating and maintaining records of systems operation.
These records should demonstrate that the system satisfied the criteria listed above.
(**ISO 15489.1 Records Management - 8.2.2 Reliability)**

Historical Manuscripts Commission
HMC Standard for Records Repositories
Third Edition, 2001

British Standard
BS 5454:2000 Recommendations for the Storage and Exhibition of Archival Documents

5.5.1 "Fire Protection - Strong-rooms, including their doors, walls and ceilings, should offer 4-hour fire resistance."
5.5.2 "Smoke Detectors, preferably capable of detecting fire in its incipient phase, with automatic fire alarms connected to the fire station or security agency should be fitted to strong-rooms, plant rooms, and adjacent areas and preferably throughout the repository."

5.9 ***Environment and storage: Magnetic Tape***

5.9.1 "Magnetic tape should be stored in an environment as close as possible to that in which it will be consulted."

Canadian Standard
FC 311 (M), Standard for Records Storage

This Standard describes the Fire Protection Requirements for the storage and handling of records of the Government of Canada.

*"**Fire Rated Vault**" means a vault of an approved design and construction having a fire resistance rating.*
*"**Fire Resistance Rating**" means the time that a material or assembly of materials will resist the effects of fire as determined by ULC Standards S101 "Standard Methods of Fire Endurance Tests of Building Construction and Materials." U.S. Equivalent ASTM E-119.*
"Fire Rated Vaults"
1) A fire rated vault shall be of an approved design and of noncombustible construction having a fire resistance rating of not less than two hours.

> *NOTE: A vault designed in accordance with NFPA 232. "Standard for the Protection of Records" shall be considered to meet the design requirements of this Clause.*

Canadian Physical Security Standard
"Access Control should be used to progressively handle traffic within the Centre. Some evaluation such as a Threat Risk Assessment should guide the determination of the security methods employed."

- *"Public Zone*
- *Reception Zone*
- *Operations Zone*
- *Security Zone*
- *High Security Zone"*