

BITS

FINANCIAL SERVICES
R O U N D T A B L E

BITS KEY CONSIDERATIONS FOR SECURING DATA IN STORAGE AND TRANSPORT

SECURING PHYSICAL MEDIA IN STORAGE, TRANSPORT, AND FOR DATA ERASURE AND DESTRUCTION

FEBRUARY 2006

A PUBLICATION
OF
BITS
1001 PENNSYLVANIA AVENUE NW
SUITE 500 SOUTH
WASHINGTON DC 20004
(202) 289-4322
WWW.BITSINFO.ORG

TABLE OF CONTENTS

I.	Executive Summary	3
II.	Background	5
III.	Policy	6
IV.	Inventory	7
V.	Categorize and Prioritize	9
VI.	Third Party Service Provider Relationships	9
VII.	Controls and Limitations	11
VIII.	Evaluate Residual Risk	16
Appendix I:	Relevant Legal and Regulatory Requirements	17
Appendix II:	Glossary of Terms	18
Appendix III:	About BITS	20

I. Executive Summary

As data security concerns grow in response to data breaches, state legislatures, US Congress, and federal regulators have attempted to address data breach disclosures and customer notification. In early 2005, the BITS Security and Risk Assessment Working Group began to develop a framework to help financial institutions better manage data in storage and transport. The *BITS Key Considerations for Securing Data in Storage and Transport* is the culmination of this effort.

This paper provides financial institutions with a framework to evaluate the risks associated with the transport and storage of physical media and the destruction or erasure of data on various media. This framework is a reference tool that complements individual institutions' risk assessment and risk management policies. The framework helps risk managers and information security professionals by outlining key questions, identifying risks that can (and cannot) be mitigated, educating key vendors about the needs of financial institutions, implementing appropriately secure storage and transport procedures, and developing effective audit procedures. The framework is intended to address transport and storage of information for the purposes of archiving, processing, regulatory reporting, backup and recovery, and customer requirements. As such, the framework does not cover electronic transmissions of information, including e-mail, encryption and other tools for securing data. It also does not address the transport of data using personal storage media, e.g., Personal Digital Assistants (PDAs), USB storage tokens, portable hard drives, digital cameras, and digital audio devices, because it is atypical for institutions to use personal storage media for the purposes noted.

Loss or theft of physical media poses financial and legal risks to a financial institution as well as to its reputation and the confidence of its customers. All financial institutions create and handle media that contains sensitive information. However, each financial institution will apply this framework differently to fit its unique needs. Procedures and controls that may be useful to an institution in some circumstances may not be applicable in others. For example, fewer controls may be deemed necessary where data is being transported between floors of a wholly-owned building with physical security controls that limit public access. Similarly, transporting small amounts of data, such as mailings to individual customers, fall entirely outside the scope of this document. Specific risk thresholds must be determined by individual institutions in light of the totality of their circumstances.

Financial institutions can apply the guidelines in this *BITS Key Considerations* document, based on the institutions' evaluation of the risks, inventory of physical media, available controls and issues relating to managing residual risks. Recognizing that managing this process on an enterprise-wide basis is complex and dynamic, the document is divided into six sections.

Policies: Policies focused on securing data in storage and transport should identify requirements for reasonable and prudent controls that address both preventive and detective measures to safeguard information from loss or theft, and identify when a loss or theft has occurred, as well as provide for response mechanisms to investigate and respond to security incidents pertaining to media. Policies should also: 1) define roles and accountabilities; 2) require robust and ongoing processes for ensuring that the other five elements below remain

current, 3) require documentation for risk monitoring and management; and 4) require testing, verification, validation, or quality assurance of policy compliance.

Inventory: Each business unit should survey the outgoing and incoming physical media that are transported or stored. Based upon survey results, the institution should establish a documented inventory that will provide a complete record of the physical media transported or stored by each business unit. The inventory should be updated as media are added or destroyed. Processes should also be implemented to ensure that changes in business processes affecting media transport or storage result in inventory updates.

Categorize and Prioritize: Evaluating the inventory will allow the organization to identify and assess risks, set priorities, and apply appropriate controls based on the specific kinds of information contained on the media, the method of transportation, and the possible effects of unauthorized disclosure, modification, or destruction.

Third Party Service Provider Considerations: Contracts with third party service providers should ensure that there are clear policies, procedures, and escalation processes in place to identify data storage, media handling, and destruction requirements, as well as the loss or theft of the information. Ongoing due diligence is required to determine whether the policies and procedures included in the contract are sufficient to ensure proper data handling and to determine if these practices are being followed by the service provider.

Controls and Limitations: This paper also includes a table of security controls for media within the financial institution, under the control of a service provider, and being transported. The table includes limitations and risk considerations related to these controls; the table assumes that the media contains some level of confidential information. Recognizing that there are risks when disposing of or reusing media if proper procedures are not followed to ensure that information is not disclosed to unauthorized internal or external parties, this paper also includes an analysis of the available methods for the destruction of media.

Evaluate Residual Risks: After applying available controls, the financial institution should evaluate the residual risk that remains after the controls are implemented. The decision on the acceptability of that residual risk is one that can only be made by the individual financial institution. Organizations should document any issues uncovered during the application of controls, evaluation of limitations, and review of residual risks for use in ongoing operations and to be considered if there are changes in regulations, policies, providers or business needs.

The framework includes an appendix of relevant regulatory requirements that may impact a financial institution's assessment of the risk and control requirements necessary to protect information in storage or transport.

II. Background

Loss or theft of physical media can result in damage to a financial institution's reputation and erosion of customer trust. Data security breaches also can lead to operational disruption, unplanned expense, or litigation and may result in the imposition of substantial penalties due to the failure to meet regulatory requirements. It is critical to the integrity of the financial services infrastructure that controls be implemented to reduce the security risks associated with the transport and storage of physical media containing company data.

As indicated by the data security breaches of all organizations—financial institutions, retailers, universities, government agencies, etc.—that took place between January and December 2005, the implementation of security controls to mitigate risks associated with the transport and storage of media goes beyond the application of formulaic solutions. Rather, each business unit and data center of a financial institution must determine appropriate controls consistent with the enterprise policy and risk appetite, depending upon the type of media involved, the kinds of data residing on the media, and the likely risks to both the company and the customer associated with the loss or theft of data.

In 2005, news media and public attention have been focused on security breaches and data losses. Data breach disclosures reflect the breadth of risks and the fact that many types of organizations are required to report security breaches. These are mandated by various state and federal laws and various regulatory or supervisory requirements. (See Appendix I: Relevant Legal and Regulatory Requirements for a list of regulatory requirements that may impact a financial institution's assessment of the risk and control requirements necessary to protect information in storage or transport). Most of the breaches that have occurred are physical breaches or loss of data in transit as it was being shipped from one facility to another. There also have been hacking-related breaches and insider abuse. While news of these breaches sounds alarming, there is not a one-to-one correlation between the exposure of personal information in a breach and an incident of identity theft or fraud.

With increased attention and concern about these risks, the BITS Security and Risk Assessment Working Group formed a Project Team in early 2005 to evaluate risks and controls associated with securing data in storage and transport.¹ The Team has reviewed the elements of a comprehensive analysis of risks, available controls and regulatory requirements. As a result, this framework addresses the following components:

1. **Policy** – What are some of the considerations that financial institutions need to address in their policies given recent breaches?
2. **Inventory** – What should an inventory of electronic and physical data in storage and transport include?
3. **Categorize and Prioritize** – What considerations should be taken into account when setting priorities for what should be done and when it should be

¹ The BITS Security and Risk Assessment (SRA) Working Group is comprised of senior information security officers from 78 BITS member companies. The mission of the BITS SRA is to strengthen the security and resiliency of financial services by sharing and developing best practices to secure infrastructures, products and services; maintaining continued public and private sector confidence; and providing industry input to government agencies and regulators on policies and regulations.

- accomplished? How should risk be calculated based upon regulations and risk management requirements?
4. **Third Party Service Provider Relationships** – What should financial institutions consider as requirements for those third parties engaged in transport, storage, processing or destruction of electronic or physical media?
 5. **Controls and Limitations** – What are the available controls and how can they be applied to media in different states? What are the limitations of each control? What controls can be put into place when media will be destroyed?
 6. **Evaluate Residual Risk** – What are the residual risks that have to be monitored?

Consistent with the goals of this paper, these six components provide a strong framework for assessing and ultimately strengthening current data storage and transport practices. However, institutions should be mindful of the fact that this paper is only a portion of the broader and more comprehensive information security program that is necessary to protect sensitive or confidential information and thus maintain safety and soundness requirements.

III. Policy

Financial institutions should have policies in place that establish the framework for a comprehensive program to manage and protect sensitive information on media while in transit and storage.

The following definitions are used to govern the scope of this project:

- **Media is the physical material used to store information.** As used within the scope of this framework, media is distinguished as existing either in electronic (digital) form, as in tapes (reel, cassette), disks, drums, CDs, and DVDs, or in print form, such as paper, microfilm, and microfiche. Each institution should conduct a thorough risk assessment to identify and assess risk and to determine inherent risk. Once inherent risk is identified, institutions can choose and implement appropriate controls to reduce risk to acceptable levels and establish thresholds for residual risk. Appropriate controls and acceptable risk may vary based on the media in question, the location of the storage or distance of transportation, and many other factors. Institutions will reach different conclusions as they assess risk and design controls.
- **Transport is the physical movement of media from its current location to any other location.** This includes delivery of the media to a third party (e.g., client, regulatory agency, service provider). A business-related purpose for this transport may be the storage of back-up or archive data, regulatory reporting, the processing of data offsite by the company or a third party, transfer to a client or customer, the erasure of data and/or the destruction of media. Institutions also should review their inter-office mail systems and transfers to determine whether appropriate controls, such as those outlined in this paper, should be implemented. Electronic transmissions of information, including e-mail, are not within scope of this project.
- **Storage is the retention of media when its data are not actively being used for business-related purposes.** For example, when a form of media (e.g., magnetic tape) is placed into an archive for business continuity or records retention purposes, it is in storage. It could be stored locally in the processing facility (e.g., tape library), offsite at another company facility, or at a third party location.

The institution's policies should address the issues associated with electronic or digital media and print media. The risk assessment process should consider scenarios when the information is under the institution's control and when it is under the control of a third party. Policies should identify requirements for reasonable and prudent controls that address both preventive and detective measures to safeguard information from loss or theft, and identify when a loss or theft has occurred. Policies also should address the need for response mechanisms to investigate and respond to security incidents pertaining to media.

A sound practice is for institutions to establish an overall Data Media Management policy, the purpose of which is to explain the requirements for and the manner in which transport, storage, retention, and destruction are interrelated processes. Following are some additional considerations:

- **Information Classification Standards** – Policies should reference appropriate internal, legal, and regulatory definitions for classifying information. For example, information can be classified as that which is public, company internal, customer confidential/sensitive, and/or restricted. Controls applied to each of these classifications should be commensurate with the perceived risk of unauthorized access or compromise. These classifications can drive the handling of information throughout the enterprise. Stronger controls may be more prudent for sensitive consumer information versus other forms of company data.
- **Transport** – Establish security or control requirements for transport of sensitive information to internal constituents, customers, and third parties. As with data classification, the application of suitable controls should be commensurate with the perceived risk of data loss or exposure.
- **Purpose** – Various scenarios—such as whether the media is for backup or archive purposes, for processing by a third party, or for transmission to a client—may affect the security controls available or necessitate the need for specific controls.
- **Media Destruction Standard** – Establish approved methods for destroying media and erasing data, as well as requirements for securing transport to the destruction facility and documenting and tracking the disposal. The National Institute of Standards and Technology published in February 2006 a public draft of its *Guidelines for Media Sanitization*.² These *Guidelines* provide an excellent overview of sanitization methods and policies. In addition, NIST includes, in its Appendix A, a thorough table of appropriate media sanitization methods for various types of media. Institutions should examine this document and consider integrating it or similar standards into their media erasure and destruction policies.

IV. Inventory

Sound policy and practical considerations typically necessitate business unit involvement in the risk management process. An initial survey of all business units should be taken to identify where media is being created, where it is being sent, what it contains, and its intended purpose. Once the survey is complete, responses can be assessed to identify where additional risk assessment and mitigation is necessary, including the need for comprehensive

² NIST Special Publication 800-88, *Guidelines for Media Sanitization*, Public Draft is available at http://csrc.nist.gov/publications/drafts/DRAFT-sp800-88-Feb3_2006.pdf.

monitoring and tracking of transport and storage of media. Where appropriate, business units should be responsible for documenting procedures for the development and maintenance of the inventory, for tracking and monitoring the transport and storage of sensitive data, and for reporting the loss or theft of data.

Individual business units frequently are a logical component of an inventory process that surveys to identify physical media (both print and electronic such as tapes, CDs, disks) that are periodically transported or are placed into storage for archival or other purposes. The results of the survey might contain the information such as:

- Origin of data (e.g., paper forms, data generated from specific applications).
 - Owner of data
 - Technical contact of data creation
- Destination (the location to which the physical media will be transported).
- Frequency of transport (e.g., *ad hoc*, daily, weekly, monthly).
- If the data is consumed or created for storage.
- If the media is to be returned or held/destroyed. If the media is returned, then the return trip should also be included in the inventory.
- Media type (e.g., tape, disk, CD, paper).
- Data type (e.g., “unrestricted information,” “sensitive customer information,” customer confidential,” “company internal,” “restricted”).
- Number of customers’ records contained in the media.
- Size of data on media (e.g., 100 MB, 3 GB).
- Number of items typically included in the shipment.
- Data protection measures in place including security controls implemented to protect data against loss, theft, unauthorized disclosure.
- Description of shipping method and level of service (e.g., national carrier, overnight mail, hand delivered, local courier).
- Description of storage method (e.g., third-party off-site storage service, secure room, desk, vault, cabinet, secure tape room).
- Risk (e.g., no impact, minor, significant, tangible, serious, grave).

Based upon the results of the survey, the institution should identify where additional risk assessment and mitigation is needed and where it might be appropriate to establish a documented inventory of physical media (both electronic and print) containing sensitive information that are transported or which are placed into storage. This inventory should include the information described above, as well as the following:

- Tracking or other identification number associated with shipment or storage item.
- Date media are shipped to designated destination.
- Date media are received at destination or placed into storage.
- Date media are returned, destroyed or the data erased.

This inventory should represent a complete record of physical media (both electronic, e.g., tape, CD, disk and print) that the business unit or data center has shipped or placed into storage. The inventory should be updated when new media are added or old data are erased

or destroyed. Also, the accuracy of this record should be verified periodically. It is especially important to verify that stored media are properly accounted for.

Once an initial inventory of media is completed, financial institutions should consider the need for and the requirements of an inventory tracking system. Such a system will better enable institutions to discover weaknesses in their processes as data requirements, media, and processes evolve over time. An institution may consider a number of potential approaches to an inventory tracking system (e.g., information lifecycle approach) before settling on one that best meets an institution's needs.

V. Categorize and Prioritize

Evaluating survey results and the inventory will allow the organization to identify risks, set priorities, and apply appropriate controls. Business units must assess risk based upon the specific kinds of information contained on media, the method of transportation, and the possible effects of unauthorized disclosure, modification, or destruction. Impact assessment should consider the risk to the financial institution and the client, the consumers to whom the information may ultimately apply, legal implications, and regulatory requirements. Issues highlighted in this document should be taken into consideration in impact and risk assessments. Where non-electronic data is concerned, the protection of the data relies strongly on physical security. Sensitive electronic data requires at least the same level of physical protection, and may also require additional electronic measures such as encryption.

VI. Third Party Service Provider Relationships

Financial institutions utilize third party service providers to provide a wide range of services. For the purposes of this framework, BITS considered two high level categories of third party service providers: 1) those that provide processing services to the financial institution; and 2) those that are engaged in the transportation, back-up, storage, or archiving of the physical media.

Requirements established by the institution to protect media need to take into account the purpose for which the service provider handles the information, the way the third party service provider handles the information, and whether the service provider's controls are adequate based upon the services provided. Contracts with third party service providers should ensure that the service provider has clear policies, procedures and escalation processes in place regarding media handling and destruction requirements, as well as the loss or theft of the information. Ongoing due diligence is required to determine whether the policies and procedures included in the contract are sufficient to ensure proper data handling and to determine if these practices are being followed by the service provider.³

³ See the *BITS Framework for Managing Technology Risk for IT Service Provider Relationships*, November 2003, and the *BITS Expectations Matrix*, January 2004, for further details on selecting and managing service provider relationships.

Contracts should communicate to the service provider the financial institution's requirements for the safe handling of information as they apply to storage and transport, including access controls, copying, authentication systems, or encryption. The institution should define the necessary service provider procedures commensurate with the risk and sensitivity of the information, including but not limited to:

- **Media Storage:** Procedures for safe storage of both electronic and print media, including requirements for the copying of archived data should that media deteriorate.
- **Media Destruction:** Procedures for securely erasing data from media or physically destroying media, as well as any requirements for securing transport to facilities for erasure or destruction.
- **Media Transport:** Information-handling procedures for storage, packaging for internal messenger, packaging for external mail or courier services, shipping, tracking, and destruction.
- **Audit:** Requirements for validating transport and storage controls, data erasure and media destruction methods, and requirements for timing for destruction.
- **Incident Management and Escalation:** Clear definition around what would constitute "lost" media and the timeline according to which an item would be considered "lost," procedures for notifying the financial institutions that an incident has occurred, and specification of what recourse the financial institution has in cases of lost items.
- **Dependent Service Providers:** Notice and control requirements should be included in the contract relative to the use of dependent service providers to provide any aspect of the contracted service.

VII. Controls and Limitations

The following is a list of available controls. Each organization should assign its own level of risk and appropriate controls during the Categorization and Prioritization process described earlier. Not every control can be implemented as some controls would override or contradict a lesser control. For the purposes of the following matrix, the assumption is that the media contains some level of confidential information.

Please note that this framework does not cover electronic transmissions of information, including e-mail, or the transport of data using personal storage media. It also does not cover encryption and other tools for securing data. Encryption of information on removable media and computer devices using widely recognized and accepted standards can significantly mitigate risk associated with loss or theft of the device containing the information. Use of encrypted electronic transmissions in place of physical transport of the media can be utilized to mitigate this risk.

Purpose of the Media	Potential Controls	Risk Considerations	Limitations
Storage: Media Within the Financial Institution (e.g. available for processing or in tape library)			
Created for internal use	<ul style="list-style-type: none"> • Encrypt the media – file level • Encrypt the media – media level • Log access to sensitive data, etc. • Log addition of external recordable devices. • Environmental Controls • Storage/Library Management System • Physical Security (access controls matching production hardware environment) • Logical Security (access controls matching production) • Biometric identification 	<p>Notification requirements for loss of confidential information.</p> <p>Regulatory/compliance requirements concerning record retention.</p> <p>Service level and other contractual agreements</p>	<p>Encryption Key management</p> <p>Encryption Key length / Strength</p> <p>User management / Administration</p> <p>People</p>

Purpose of the Media	Potential Controls	Risk Considerations	Limitations
Received from outside organization	<ul style="list-style-type: none"> • Obtain a receipt from courier to indicate receipt • Entered into tracking system to log receipt of tape • Use a centralized center for receipt of outside information • Provide positive acknowledgement to the sender, confirming receipt • Encrypt the media – file level • Encrypt the media – media level 	<p>Notification requirements for loss of confidential information.</p> <p>Regulatory/compliance requirements concerning record retention.</p> <p>Service level and other contractual agreements</p>	<p>Media may be sent in a manner which is not secured.</p> <p>Ownership of liability in the event of a loss needs to be established.</p>
Created for outbound users	<ul style="list-style-type: none"> • Encrypt the media – file level • Encrypt the media – media level • Entered into tracking system to log receipt of tape • Positive acknowledgement from the recipient confirming receipt • Logical security (access controls matching production) • Biometric identification 	<p>Notification requirements for loss of confidential information.</p> <p>Service level and other contractual agreements</p> <p>Regulatory/compliance requirements concerning record retention.</p>	<p>Regulators may not accept encrypted media.</p> <p>Key management</p> <p>Key distribution</p> <p>Key escrow</p> <p>Key recovery</p> <p>Software interoperability (algorithms, protocols)</p> <p>Performance impacts</p>
Storage: Media is Under the Control of a Third Party Provider			
Third party service provider	<ul style="list-style-type: none"> • Contract • Due Diligence • Service Level Agreements (SLAs) • Logging of access to sensitive data, etc. • Logging of adding external recordable devices. • Annual reviews of controls • Logical access controls • Physical access controls 	<p>Possible use of unknown downstream service provider</p> <p>Procedures not followed</p> <p>Criminal or accidental breach</p> <p>Regulatory/compliance requirements concerning record retention.</p>	<p>Third party may change procedures without approval from client.</p> <p>Contract may not have sufficient protections written into it.</p> <p>Frequency of moving data increases risk.</p> <p>Validation</p> <p>Audit</p>

Purpose of the Media	Potential Controls	Risk Considerations	Limitations
		<p>Service level and other contractual agreements</p> <p>Notification requirements for loss of information</p> <p>Business interruption resulting from manmade or natural disasters.</p> <p>Liability of loss/damage resulting from financial viability of provider.</p>	
<p>Third party provider performs a service using the contents of the container (e.g. backup, storage or archiving)</p>	<ul style="list-style-type: none"> • Logging of access to sensitive data, etc. • Logging of adding external recordable devices. • Due Diligence • Annual reviews of controls • Contract • Service Level Agreements (SLAs) • Logical access controls • Physical access controls 	<p>Possible use of unknown downstream service provider</p> <p>Procedures not followed</p> <p>Criminal or accidental breach</p> <p>Regulatory/compliance requirements concerning record retention.</p> <p>Service level and other contractual agreements</p> <p>Notification requirements for loss of information</p> <p>Business interruption resulting from manmade or natural disasters.</p> <p>Liability of loss/damage resulting from financial viability of provider.</p>	<p>Third party may change procedures without approval from client.</p> <p>Contract may not have sufficient protections written into it.</p> <p>Frequency of moving data increases risk.</p> <p>Validation</p> <p>Audit</p>

Potential Controls	Risk Considerations	Limitations
Media Being Transported		
<ul style="list-style-type: none"> • Encrypt media/data. <p>Associates</p> <ul style="list-style-type: none"> • Training on handling procedures and control requirements. • Awareness of privacy laws and regulations and their business implications. <p>Vendor</p> <ul style="list-style-type: none"> • Only approved vendors shall be used. Evaluation of potential vendors may include such factors as whether the vendor possesses the financial ability to meet liability obligations through bonding, insurance, self insurance, etc. • Contracts with approved vendor shall be in place. • Contract must specify chain of custody information. • Background checks. • Non-Disclosure Agreement (NDA). <p>Transportation\Tracking</p> <ul style="list-style-type: none"> • Media cannot be transported through a major distribution hub (i.e. no mass handling or automated sorting). • Point to Point monitoring and/or chain of custody package location tracking (e.g., signatures designating any change of custody - sender, courier or receiver, bar code scanning; delivery control numbers, logging, position control). • The materials or items must not be left unattended or in an unsecured vehicle. • Manifests are required and must include shipper, receiver, and driver signatures with delivery time and pickup. • Inventory control and escalation procedures. • Certified Mail Receipt. • Global Positioning System (GPS) Tracking of very large shipments 	<p>Notification requirements for loss of confidential information.</p> <p>Procedures not followed.</p> <p>Criminal or accidental breach or loss of package.</p> <p>Service level and other contractual agreements.</p> <p>Damage to financial institution with respect to reputation, laws and regulations, and/or fraud if media is compromised in transit.</p> <p>Business interruption resulting from manmade or natural disasters.</p> <p>Liability of loss/damage resulting from financial viability of provider.</p>	<p>Frequency of moving data increases risk.</p> <p>Reliance on third parties to conduct background checks on their employees.</p> <p>Key management issues associated with data encryption.</p> <p>Encryption key length/strength.</p> <p>Encryption key management for locking mechanisms.</p> <p>Tracking of missing shipments may be more difficult than when using conventional couriers.</p> <p>Options may be subject to postal regulations.</p>

Potential Controls	Risk Considerations	Limitations
Media Being Transported		
<p>Access Control</p> <ul style="list-style-type: none"> • Media is stored in a locked room or cabinet. • Access to storage areas is limited and restricted to those with a need to enter. • Access to storage areas is monitored, where appropriate, by CCTV or onsite security guards, and logged. • Removal of media is recorded, including identification of the handler, purpose, date, time, intended disposition, and expected return date if applicable. • Return of media is recorded. • A process is established to identify media that has not been returned beyond its expected return date. <p>Packaging</p> <ul style="list-style-type: none"> • Metal container(s) with a locking mechanism or a sealed container. • Locking mechanisms should be Air Transportation Association of America (ATA)-compliant padlocks if the containers are to be air freighted. • Containers must be locked or sealed before leaving the secure premises. • Key/combination management processes which ensure key/combinations are only available to authorized personnel. • Enclose the media in bubble wrap for shipment. • Use only hard cardboard boxing material, no envelopes. • Double box the package in the event that the outer container or seal is broken. • Tape the package with 2" pressure sensitive adhesive tape, reinforce the box at the four corner points, and place tape across the box. • Do not mark the outside of the box with information pertaining to its contents or classification. 		

VIII. Evaluate Residual Risk

After applying available controls, the financial institution should evaluate the residual risk that remains after the controls are implemented. The decision on the acceptability of that residual risk is one that can only be made by the individual financial institution based upon those decisions made in the categorization and prioritization process. Organizations should document any issues uncovered during the application of controls, evaluation of limitations, and review of residual risks for use in ongoing operations and to be considered if there are changes in regulations, policies, providers, or business needs.

Appendix I: Relevant Legal and Regulatory Requirements

Financial institutions should carefully examine the legal and regulatory requirements of all jurisdictions in which they serve customers. Requirements vary widely between countries and between states or other jurisdictions within the same country. The following is a list of some of the potential regulatory requirements which may impact a financial institution's assessment of the risk and control requirements necessary to protect information in storage or transport.

- Gramm-Leach-Bliley Act of 1999 (GLBA) (otherwise known as “The Financial Services Modernization Act.”) GLBA includes security guidelines containing a range of risk management obligations focused on implementing the Congressional policy of protecting customer data. A significant component of the GLBA legislation is the affirmative and continuing obligation for a financial institution to “respect the privacy of its customers.” As part of this privacy-related obligation, GLBA explicitly includes a responsibility to protect certain data—namely the “security and confidentiality of customers’ nonpublic personal information.”
- Economic Espionage Act 1996 (export of sensitive information)
- Federal Privacy Act of 1974
- Health Insurance Portability and Accountability Act of 1996 (HIPAA) (mandates privacy of medical information)
- Computer Security Act of 1987
- Family Education Rights and Privacy Act of 1974 (FERPA)
- Fair and Accurate Credit Transaction Act of 2003 (FACTA)
- USA PATRIOT Act, Title V (privacy of educational, financial information)
- Sarbanes-Oxley Act of 2002 (officially, the Public Company Accounting Reform and Investor Protection Act of 2002. Section 404 of Sarbanes-Oxley requires an institution to assess and then report on its internal controls over financial reporting. It also requires external auditors to certify and report on management’s report on internal controls.)
- International Traffic in Arms Act (ITAR)
- Government Information Security Reform Act (GISRA) (Federal agencies protecting information)
- DoD Information Technology Security Certification and Accreditation Process (DoD security of information)
- European Union Data Protection Directive (EUDPD)
- State data breach notification requirements
- SEC rules 17a-3 and 17a-4; NASD conduct rule 3110; and NYSE Exchange rule 440 (email retention requirements)

Appendix II: Glossary of Terms

Access: The ability to physically or logically enter or make use of a system or area (secured or unsecured); the process of interacting with a system.

Access Control: A mechanism to allow, deny, or limit access to a resource, whether to individuals or remote machines; typically based on the authenticated identity of the individual or remote machine requesting access. Access controls prevent unauthorized access to a resource, including prevention of the use of a resource in an unauthorized manner.

Classification: Categorization (e.g., “confidential,” “sensitive,” “public”) of the information processed by the financial institution.

Confidentiality: Assuring information will be kept secret, with access limited to appropriate persons on a need to know basis.

Control Requirements: Process used to document and/or track internal procedures to determine that those documented procedures and/or physical security policies are being followed.

Data Integrity: A fundamental element of information security that exists where data has not been accessed, altered, or destroyed without intent or authority.

Encrypt: To scramble information so that only someone with the appropriate “key” can access the original information (through decryption).

Physical media will refer to any portable device or substance (e.g., paper) used to store data for specific and legitimate purposes. The following types of devices are examples of physical media:

- Magnetic tapes and disks
- Cartridges, including 9-track, DAT, and VHS
- Optical disks in CD and DVD format
- Microfilm/fiche
- Paper (e.g., computer-generated reports and other printouts)
- Static memory devices, such as USB “memory sticks”

Policy: Organization-level rules governing acceptable use of computing resources, security practices, and operational procedures.

Retention Requirement: Requirement established by a company or by regulation for the length of time and/or for the amount of information that should be retained.

Threat event: An occurrence or circumstance with the potential to have an undesirable impact on an asset.

Threat: The potential for a threat agent or source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.

Threat agent: The source of a threat, which can be human-made or natural. Human threats can be further categorized as intentional or unintentional.

Threat factor: A subjective value assigned to reflect the likelihood that a vulnerability will be exploited by a threat, assuming that there are no controls in place.

Vulnerability: A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

APPENDIX III: ABOUT BITS

BITS was created in 1996 to foster the growth and development of electronic financial services and e-commerce for the benefit of financial institutions and their customers. A nonprofit industry consortium of 100 of the nation's largest financial institutions that shares membership with The Financial Services Roundtable, BITS seeks to sustain consumer confidence and trust by ensuring the security, privacy and integrity of financial transactions. BITS works as a strategic brain trust to provide intellectual capital and address emerging issues where financial services, technology and commerce intersect, acting quickly to address problems and galvanize the industry. BITS' activities are driven by the CEOs and their appointees—CIOs, CTOs, Vice Chairmen and Executive Vice Presidents—who make up the BITS Advisory Board and BITS Advisory Council. For more information, go to www.bitsinfo.org.

BITS
1001 PENNSYLVANIA AVENUE, NW
SUITE 500 SOUTH
WASHINGTON, DC 20004
202-289-4322
WWW.BITSINFO.ORG

This *BITS Key Considerations* document was developed by a dedicated team of professionals from the BITS Security & Risk Assessment Working Group and BITS staff. BITS also vetted the draft framework with other experts from non-BITS members and from regulatory agencies. BITS appreciates their time and contributions in developing this framework.