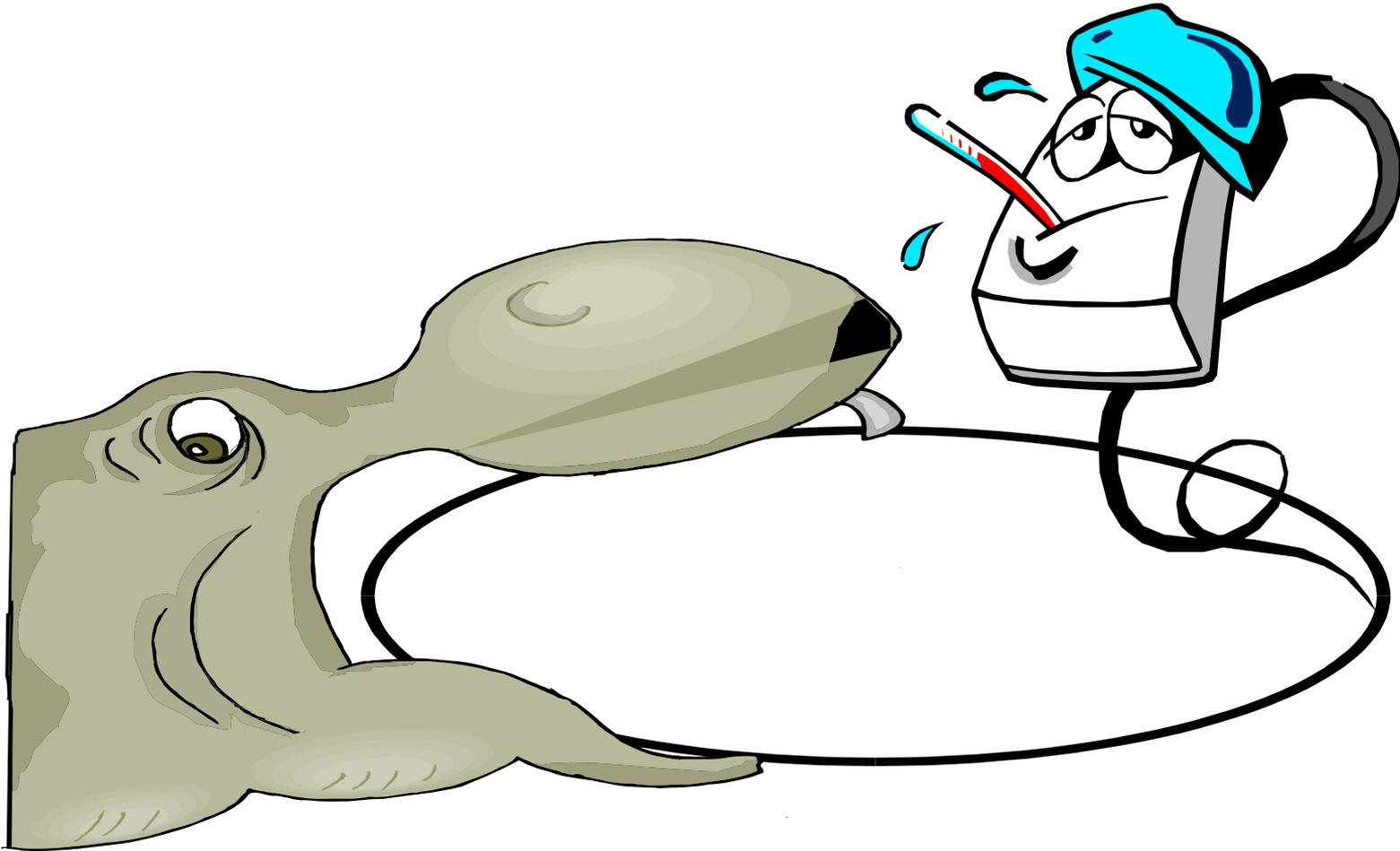


**Please Excuse the Sneezing and
the Wheezing...**



- > Systems Integration.
- > Outsourcing.
- > Infrastructure.
- > Server Technology.
- > Consulting.

2003 CMS HIPAA/MMIS
Conference

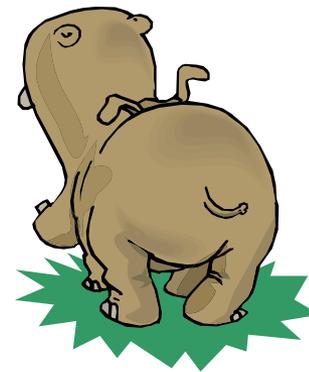
New Orleans, LA

February 12, 2003

unisys

Imagine it. Done.

System Access Controls & other System Security Considerations





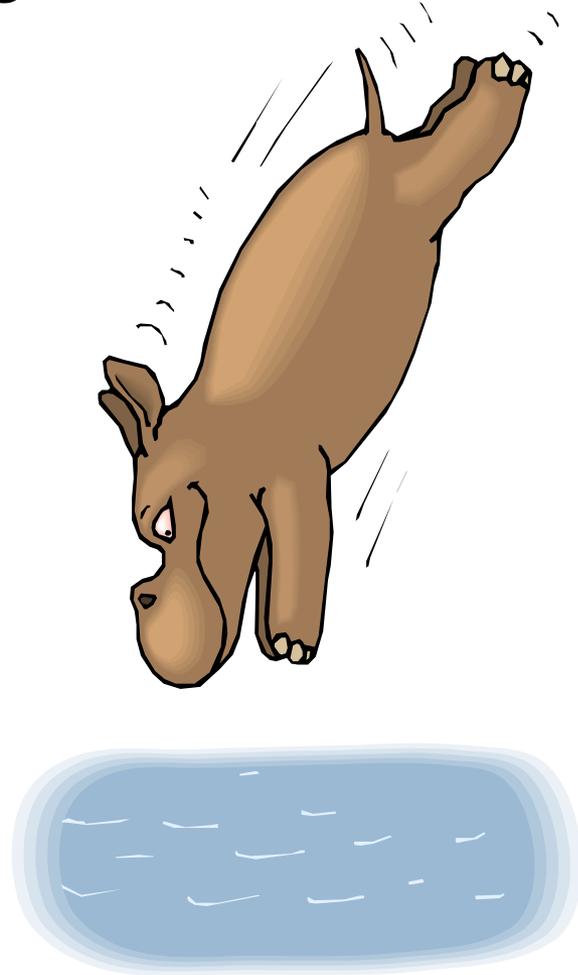
Workshop Agenda

- Brief Security Regulation Overview
- Access Control Basics
- Network Access Controls
- System Security and Access Controls
- Database Controls
- System Access Documentation
- Change Management
- Questions???





Diving in...to HIPAA and System Security Basics

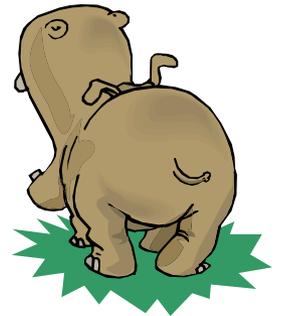




Final Security Rule Status



As of 2/12/2003, the Security final rule is still pending release upon OMB approval. It is anticipated that it will not be largely different from the current NPRM.





Custom Application of Regulations Required

What do you mean you can't tell me EXACTLY what I need to implement in my networks and systems for security????

Overall, the HIPAA Security Standards are very general.
There is NO single checklist of specific requirements for your applications and networks.

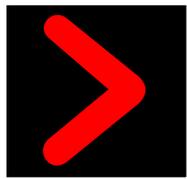
- ***Standards direct compliance based on adhering to described best practice mechanisms for securing data.***
 - ***Example: ISO17799***
 - ***Security compliance means applying appropriate and “reasonable” levels of security standards.***
 - ***Depending on your network, you application, your physical location, and your use of your system, the security rules could apply to your organization in a variety of mechanisms.***



NPRM for HIPAA Security

Implementation Requirements - 4 Basic Categories

- Administrative Procedures to safeguard data integrity, confidentiality, and availability.
- Physical safeguards to guard data integrity, confidentiality and availability.
- **Technical security services to guard data integrity, confidentiality and availability.**
- **Technical security mechanisms to protect data in transit.**



Focusing on Technical Access Controls & Supporting Measures



TECHNICAL SECURITY SERVICES TO GUARD DATA INTEGRITY, CONFIDENTIALITY, AND AVAILABILITY

Requirement	Implementation
Access control (The following implementation feature must be implemented: Procedure for emergency access. In addition, at least one of the following three implementation features must be implemented: Context-based access, Role-based access, User-based access. The use of Encryption is optional).	Context-based access. Encryption. Procedure for emergency access. Role-based access. User-based access.
Audit controls	
Authorization Control (At least one of the listed implementation features must be implemented).	Role-based access. User-based access
Data Authentication	

TECHNICAL SECURITY MECHANISMS TO GUARD AGAINST UNAUTHORIZED ACCESS TO DATA THAT IS TRANSMITTED OVER A COMMUNICATIONS NETWORK

Requirement	Implementation
Communications/network controls (The following implementation features must be implemented: Integrity controls, Message authentication. If communications or networking is employed, one of the following implementation features must be implemented: Access controls, Encryption. In addition, if using a network, the following four implementation features must be implemented: Alarm, Audit trail, Entity authentication, Event reporting).	Access controls. Alarm. Audit trail. Encryption. Entity authentication. Event reporting. Integrity controls. Message authentication.



Regulation Access Controls

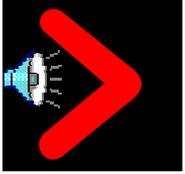
Network and System Controls can largely derived from the Technical Section of the Requirements...

TECHNICAL SECURITY SERVICES TO GUARD DATA INTEGRITY, CONFIDENTIALITY, AND AVAILABILITY

Requirement	Implementation
<p>Access control (The following implementation feature must be implemented: Procedure for emergency access. In addition, at least one of the following three implementation features must be implemented: Context-based access, Roll-based access, User-based access. The use of Encryption is optional).</p> <p>Audit controls</p> <p>Authorization Control (At least one of the listed implementation features must be implemented).</p> <p>Data Authentication</p>	<p>Context-based access.</p> <p>Encryption.</p> <p>Procedure for emergency access.</p> <p>Role-based access.</p> <p>User-based access.</p> <p>Role-based access.</p> <p>User-based access</p>

TECHNICAL SECURITY MECHANISMS TO GUARD AGAINST UNAUTHORIZED ACCESS TO DATA THAT IS TRANSMITTED OVER A COMMUNICATIONS NETWORK

Requirement	Implementation
<p>Communications/network controls (The following implementation features must be implemented: Integrity controls, Message authentication. If communications or networking is employed, one of the following implementation features must be implemented: Access controls, Encryption. In addition, if using a network, the following four implementation features must be implemented: Alarm, Audit trail, Entity authentication, Event reporting).</p>	<p>Access controls.</p> <p>Alarm.</p> <p>Audit trail.</p> <p>Encryption.</p> <p>Entity authentication.</p> <p>Event reporting.</p> <p>Integrity controls.</p> <p>Message authentication.</p>



Technical Access Controls

Network Controls

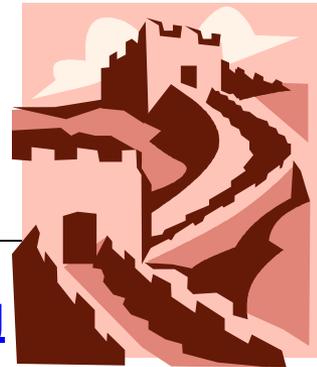
-

The Outer Layer of Defense for a Secure Application





Network Access Controls



Virtual Division of an Organization for Protecting Individual Health Care Data and the Organization

Network Segmentation

- Segment your network where possible to help limit access to network folders.
- Appropriate **network segmentation** between your organization and the rest of the State network can also assist in providing more a **secure, isolated environment** for Medicaid network traffic.
- This also helps to **secure your network data** and any security documentation present in your environment by limiting user access to it.



Network Technical Controls

▪ Network Access Control Groups

▪ Divide access on your LAN into appropriate network groups

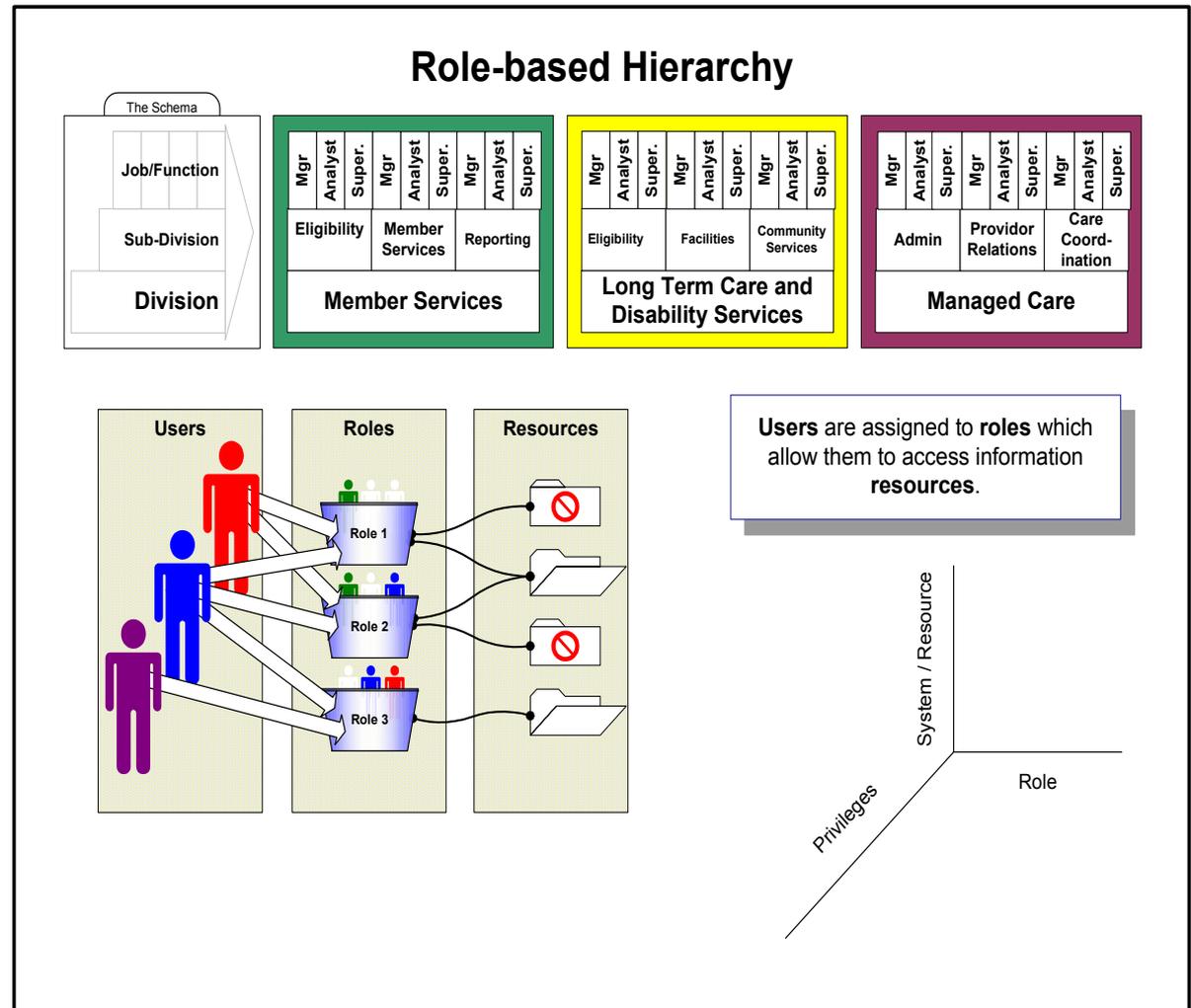
- Area Network Groups can be used to limit recipient and claims-specific data LAN data access to only those members of the groups that require access to data
- ***This helps to meet the Privacy Min Access Requirement since only users that belong to the appropriate network group can access the data.***
 - Claims Dept Users
 - Provider Dept Users
 - Utilization Dept Users
 - Operations Dept User
 - *Users can have specific combined folder areas created for file sharing between different network groups. This allows for needed flow of data without losing control over who may access the data. Read-only access to the area allows for data owners to still maintain control over their own data, while sharing it with other users who require it.*

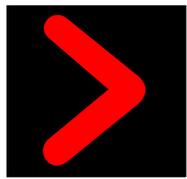


Access Control Assignment

Access to Data on the Network Can also be Controlled through Access Controls based on assigned role and user id.

The diagram to the right shows how this can be applied to accessing network or application resources.

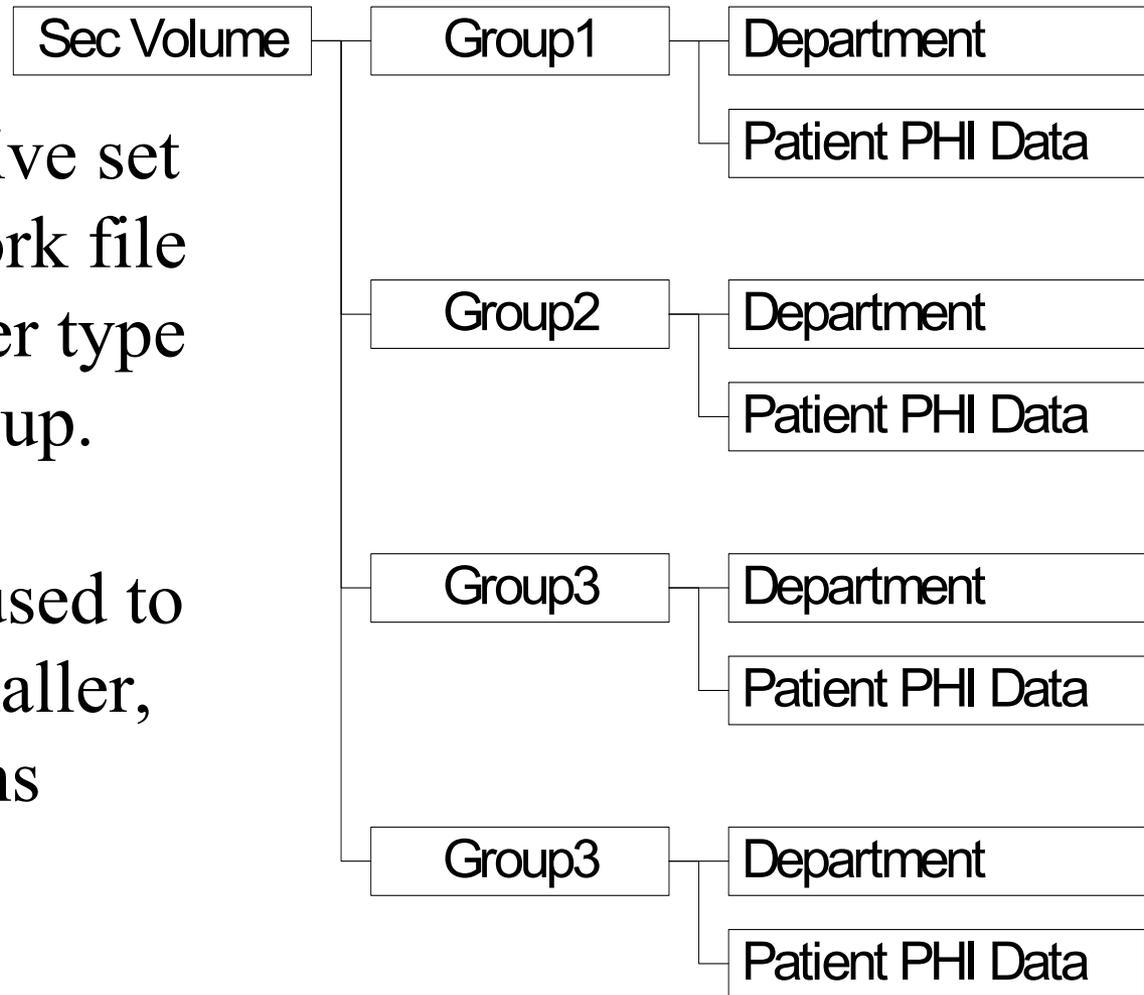




Access Control & Network Groups

Develop a definitive set up for their network file access or any other type of data access group.

This can also be used to limit access to smaller, less robust systems (access dbs etc.)





Network Access Controls

- **Appropriate Network controls for Administrators**
 - **Restriction** of all administrative files on all servers and network components to limited network management personnel
 - **Restriction** of access to all detailed security documentation to network administrators only
 - **Restriction** of control panel and other configuration elements to administrators only
 - If your security systems, **network management groups** and sensitive security documentation is easily compromised then your overall network access controls or other security measures can be easily compromised.



Network Access Controls



■ *Firewalls*

- Firewalls can be used to limit and control access into and out of a network.
 - Limit traffic coming in/out to certain ip addresses, ranges and ports. IP-filtering. This can be an access control to limit users on the network.
- Firewalls can also be used to block/limit internet traffic on user desktops.
 - Limit user ability to install/download dangerous software
 - Limits likelihood of users picking up internet-based viruses
 - Assists in blocking non-authorized intruders from accessing client-server based applications and LAN data.



Intrusion Detection Software



Software and Hardware to Keep OUT unauthorized users!!!!

Install Intrusion Detection Software

- Set up to analyze the data that is incoming and outgoing on your network
- “Sniffs” the inbound and outbound traffic on your network
- IDS Software packages can providing a file integrity checking function.
- IDS Software packages available can identify changes to files and directories and be set to send alerts via email if particular files are altered

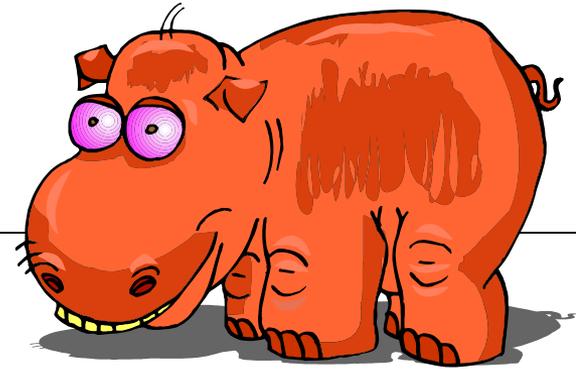


Other Network Considerations

- Limit access by having a single point of entry or exit from the network. 
 - Basic network architecture design – security centric
- Periodically, perform vulnerability scans on your network to detect unnecessary services or open ports that could be exploited
- Run “cracker” tools against your network to simulate a potential attack to determine its resistance to intrusion.



Encryption



- ***A form of access control***
 - **Encryption does not have to be done on:**
 - **Leased line arrangements**
 - **Wide Area Networks and Local Area Networks**
 - **Dial up lines**
 - **This will include many Medicaid's leased line, WAN or dial-up connectivity with switch vendors and other clearinghouses.**



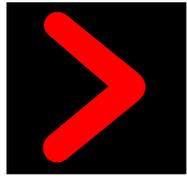
Network and Application Encryption

- ***Encryption is a necessary access control on any unsecure networks:***

- Internet communication
- Untrusted networks (networks that are deemed insecure or are not protected from external access)

Affects:

- Internet Transport of Data. Web submittal of claims, eligibility etc. over the Internet.
- This also **applies to e-mail** of data over the Internet.
 - If your system e-mails data to providers, vendors, recipients, encryption could be a necessity if the transmission includes PHI.



Application Security & Access Controls

The Next Layer...



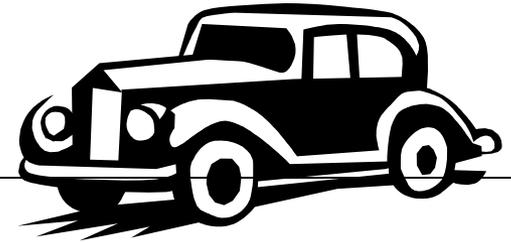
The Application

-

Protecting and Controlling System Data Access



Triple AAA



Authentication

- Authentication provides the mechanism to identify a client that requires access to a system and logically precedes authorization. The mechanism for authentication is typically undertaken through the exchange of username/password combinations, logical keys or certificates between the client and the server.

Authorization

- Authorization follows authentication and entails the process of determining whether the client is allowed to perform and/or request certain tasks or operations.

Accounting

- Accounting is the process of measuring resource consumption, allowing monitoring and reporting of



Password Access Controls

- **Authentication:**

- Applications should utilize user id and passwords, session “tokens,” IP addressing and other combinations of authentication means to validate each user or submitter of data to it prior to allowing the user to update system data or access it.

- **Like Networks, Applications must have:**

- **User-based access**

OR

- **Role-based access**

OR

- **Context based access**

***Best solution is a combination of one or more of the above.
This is generally standard of most applications or networks
that are built.***



Combining Role Based & User Based Controls in an Application

- This allows the ease of role-based access, but also enables the accountability of specific user-based access.
 - **This makes for a strong security assignment and access accountability.**
- Users can be grouped into like roles and their access to an application based on their “roles” functional needs, making it easier on managers and users to determine their system access needs as well as making it easier on system administrators to match users with appropriate access levels.
 - *A Health Care Organization can base its Access Controls on the **functional roles** or **organizational roles** within the organization as the primary criteria for granting access to networks and applications.*





Access Controls – Role Based

- ***Role Based Access Controls to Application Data***
 - **System needs ability to have field, screen, role and user based security access to system functionality and data**
 - **All users of a particular group are given access to an application or network file area**
 - **Role-based access groups are excellent for grouping like access needs together for a particular functional area.**
 - **Medicaid Claims Manager**
 - **Can perform delete and override functions on claims.**
 - **Has update access to Claims Screens**
 - **Has read access to all Claims Screens**
 - **Has access to Claims Network Folders**
 - **Has access to Claims Management Folder**
 - **Medicaid Claims Analyst**
 - **Has update access to all Claims screens**
 - **Has read access to all Claims Screens**
 - **Has access to Claims Network Folders**





Role-Based Access Controls

Ease of Maintenance

- Easy to maintain appropriate access to systems and network since users/managers do not need to report specific application and network changes.
 - But instead indicate they have moved from one **ROLE** to another **ROLE** and inherit the network rights and system access associated with that functional **ROLE**.





Application User IDs



■ USER IDs

- SPECIFIC USER ID to the application or user
 - NO GENERIC USER ids
 - USER ids must be associated with individual user or an application (background/automated processing)
 - StankisS
 - IMAGSYS01
- Access requires user id and password to access
 - Complex Passwords to Protect
 - Letters, Number, Upper-Case/Lower Case, Symbols
 - CompleX8#
- If possible, applications should force users to use complex passwords and to change them on a frequent basis.
- Need to establish user-specific ids to help establish appropriate audit trails and ability to determine WHO has access to PHI systems
 - If generic ids are used, no determination of list of users can be performed.



System Password Recommendations



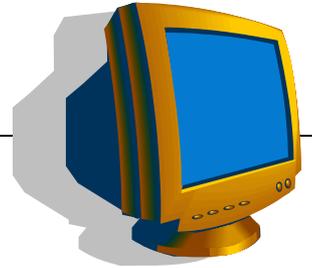
- **System Access Controls**

- *Recommendations:*

- **Default User Ids and/or Passwords should be deleted or their Passwords Modified**
 - *Examples*
 - *GUEST on a PC...is a default account that should be suspended and its password should be set as complex password to help prevent intrusions*
 - *Routers often have a default admin password of "password"*
 - **Passwords should be encrypted within databases if possible as an added precaution**
 - **User should not be able to use the same password as used previously when their password expires**



System Session Expiration

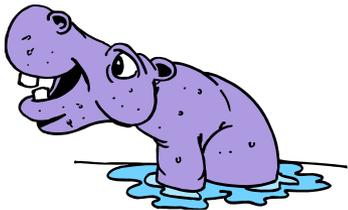


■ System Session Expiration

- Application sessions should expire
 - Set a low time limit for expiration that is both practical for operations while at the same time is short to keep intrusion and session stealing at a minimum

If this is not possible for your application to expire, then users should have desktop screen savers that cut on after a short period of inactivity.

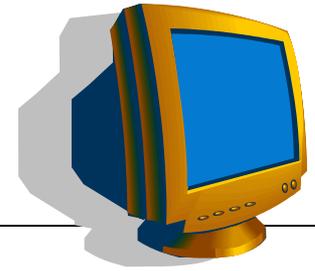
- Example: 15 minutes



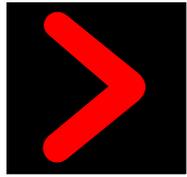
Either of these solutions can be used to meet the **REQUIREMENT** for session controls within the HIPAA regulations. This will allow some of your older systems or smaller COTS products to meet the session time out requirements.



Multiple Logins



- User caution when allowing multiple logins...
- Unless necessary, systems should not allow for multiple logins from the same user id simultaneously.
- Users will abuse multiple logins and share ids instead of requesting individual access authority.
- Applications should also be set to lock user accounts when passwords are entered incorrectly.
 - This will help to stave off attackers trying to break into your system by guessing passwords using a found or uncovered user name.
 - Recommendations:
 - Lock user after 3 bad login attempts or less
 - Lock out can also be done on network controls, although this lockout should probably be set to expire for operational practicality

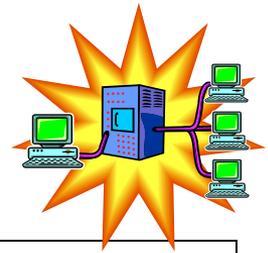


Application Security Suggestions and Requirements

- Application Security Suggestions and Requirements:
 - **Require Encryption for any Internet Transmission of data**
 - Encryption for all login of username and passwords during upload to system to prevent use ids and passwords from being read.
 - Application must prevent the user from making malicious SQL calls to the database through browser.
 - Do not store decrypted passwords in the security system database.
 - Set the file and folder permissions to the minimum set required for accessing the application. Do not allow Everyone, Users, or Domain Users access to files and folders.



Web-Specific Application Security



- Do not allow users to change web address during a secure session. Remove browser toolbar from application and limit user ability to “back out” of a secured application to the general internet while logged in.
- Keep useful information out of cookies. If useful information is stored in a cookie, a malicious user can modify the cookie values before returning the page to the server.
- Keep useful information out of hidden code “tags”. If useful information is stored in a hidden tag, a malicious user can modify the tag value before returning the page to the server.
- Do not run your web servers with administrator or root privileges. Most web servers can be configured to run with a less privileged account such as “nobody.”
- Adhere to input buffer length checking where possible to prevent non-secure traffic from entering system
- Code secure applications using stateless “tokens” to exchange for system and user authentication to help prevent session stealing.



Application Security Setting

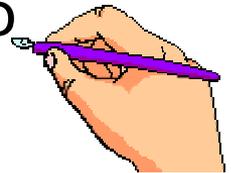
Other Considerations:

- Use of private, non-routable IP addresses within the application to protect databases
- Prevent show code commands
- Work to Block hostile inputs from users or intruders by limiting field length inputs and preventing input of characters such as @!#\$%*()
- Restricted access to system utilities and operation software. Ability should be selectively assigned to administrator user levels.
- Remove user access to any system or applications tools, OS set up, dlls and other executables of the application or its platform.



Audit Logging & Event Reporting

- Audit logging on all database updates and system access
 - Help detect/document unwanted access into a system.
 - System should also log all major events within the system in terms of errors or updates
- Automated event reporting must be enabled within the application if at all possible. This should include security alarms.
 - Alerts should be sent to a single console for operations monitoring and review if possible.
- Produce error responses to users when attempts to exceed authority are made

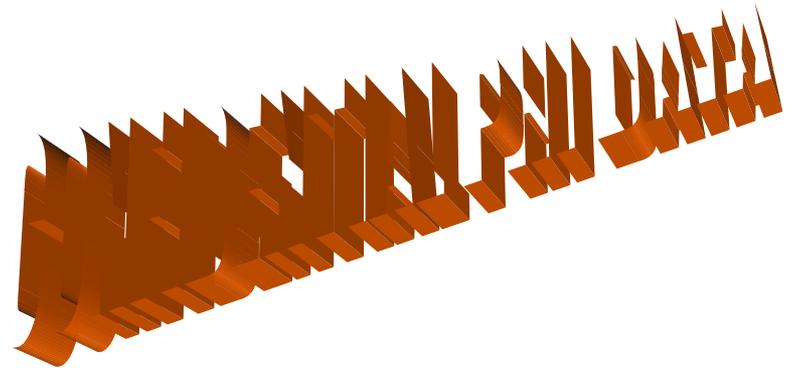




Access Control Assignment

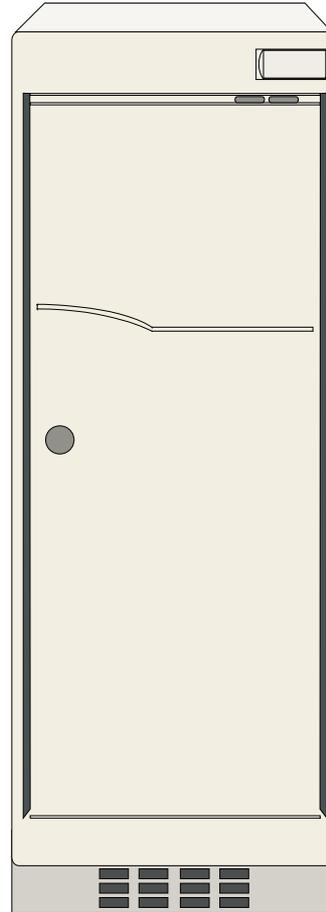
Access Control Through Appropriate Data Labeling

- **Work to Label sensitive screens, reports in your application with **CONFIDENTIAL** to alert users and operators to the sensitive nature of the data accessed.**
- **Help with security/privacy for printouts of reports and screens.**





Database Controls





Database Protections

- **Do Not Allow ODBC connections to database without appropriate authority.**
- **Do Not allow all users to utilize tools, such as enterprise manager, to view tables in an application database.**



Database Access Measures

- Close default SQL ports
- Use windows authentication on SQL server access to add additional security authentication to user access
- Establish a series of user access roles within enterprise manager to limit access
- Do not use default SA account's for administrator access. Eliminate account or disable and use a complex password.
- Used stored procedures in your applications to limit user access into the database. Stored procedures can help to only allow approved calls to be used in a database.
- Limit ability to grant security access to databases



Access Control Maintenance





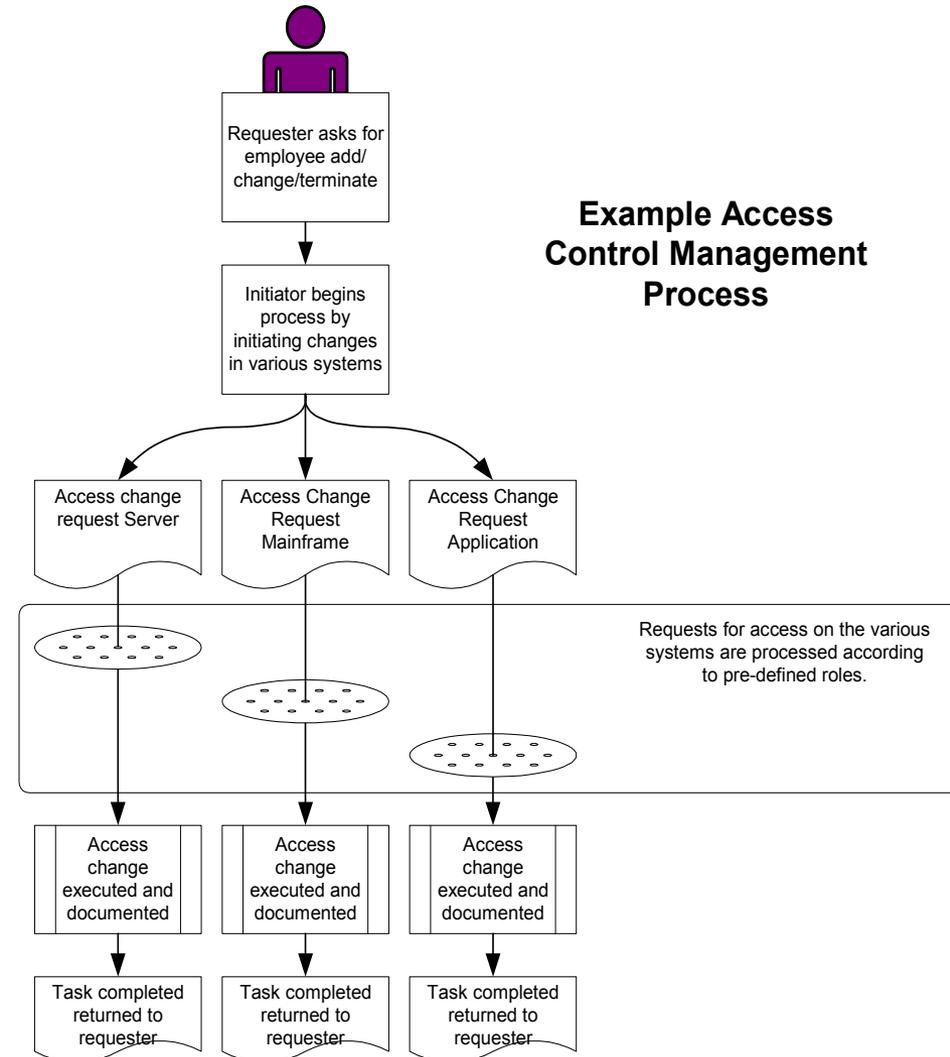
Access Control Maintenance

Importance of Process and Documentation:

A single process and POC for adding, updating, deleting and documenting changes in user access from all critical systems and network within an organization.

Unless you have a single application or a LDAP or other single sign on solution, you need to have a central location to document system access, unless you feel it is simple to pull system's access tables easily.

unisys



Imagine it. Done. 41



Access Control Documentation

Role-based Access across Multiple Systems

USER ID	Role 1	Role 2	Role 3	Role 4	Role 5	Role 6	Role 7
ACF2							
Dec UNIX							
MS Active Directory							
DSS							
Physical Access							

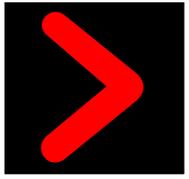
A Table, Database or Log should be kept to reflect the access levels granted to individuals and groups accross applications, networks, facilities etc.



Access Request Documentation

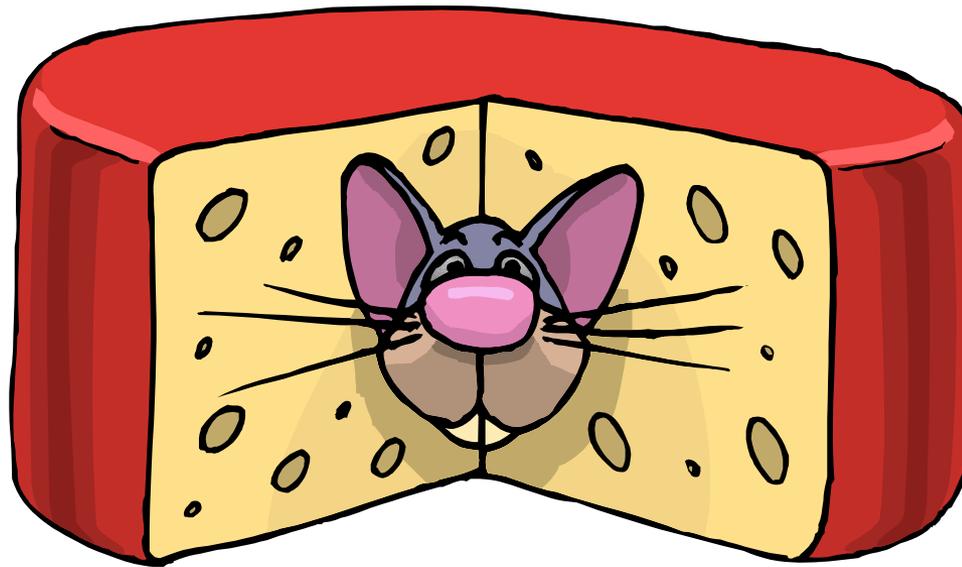
Benefits to Access Request Documentation

- **Accountability**
 - **Retain copies of system requests**
 - **Formalize requests for all systems/networks**
 - **Users do not get access to system without the appropriate authority and a paper trail of approval exists.**
 - **Users who no longer require access to a system or particular system function can be more readily identified in a single report and more easily removed from the system.**
 - **Support managers and HR reporting removal of access.**



Change Management and Risk Analysis

- Proper Change Management is a Key Security Measure

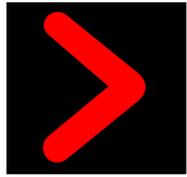




Keeping it Secure...

So you have
designed a secure
system and system
architecture...how
does it stay
secure???



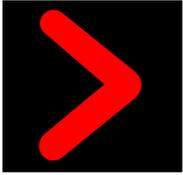


Access Control & Change Management



Appropriate Change Control can be another method of Access Control to system files and data that can protect system security.

- System users, system owners and network administrators need to be controlled by a single mandatory process for making changes to production applications, overall production network design, critical system and technical design documents and documentation.
- Appropriate Change Management can make sure that changes are not made without considering the impact to a system's overall security capabilities, HIPAA compliance, core business functionality, availability etc.



Security Risk Analysis

- A security analyst should be involved in the construction, development and deployment of any new application so as to BUILD strong security into the structure and design of the application from the beginning.



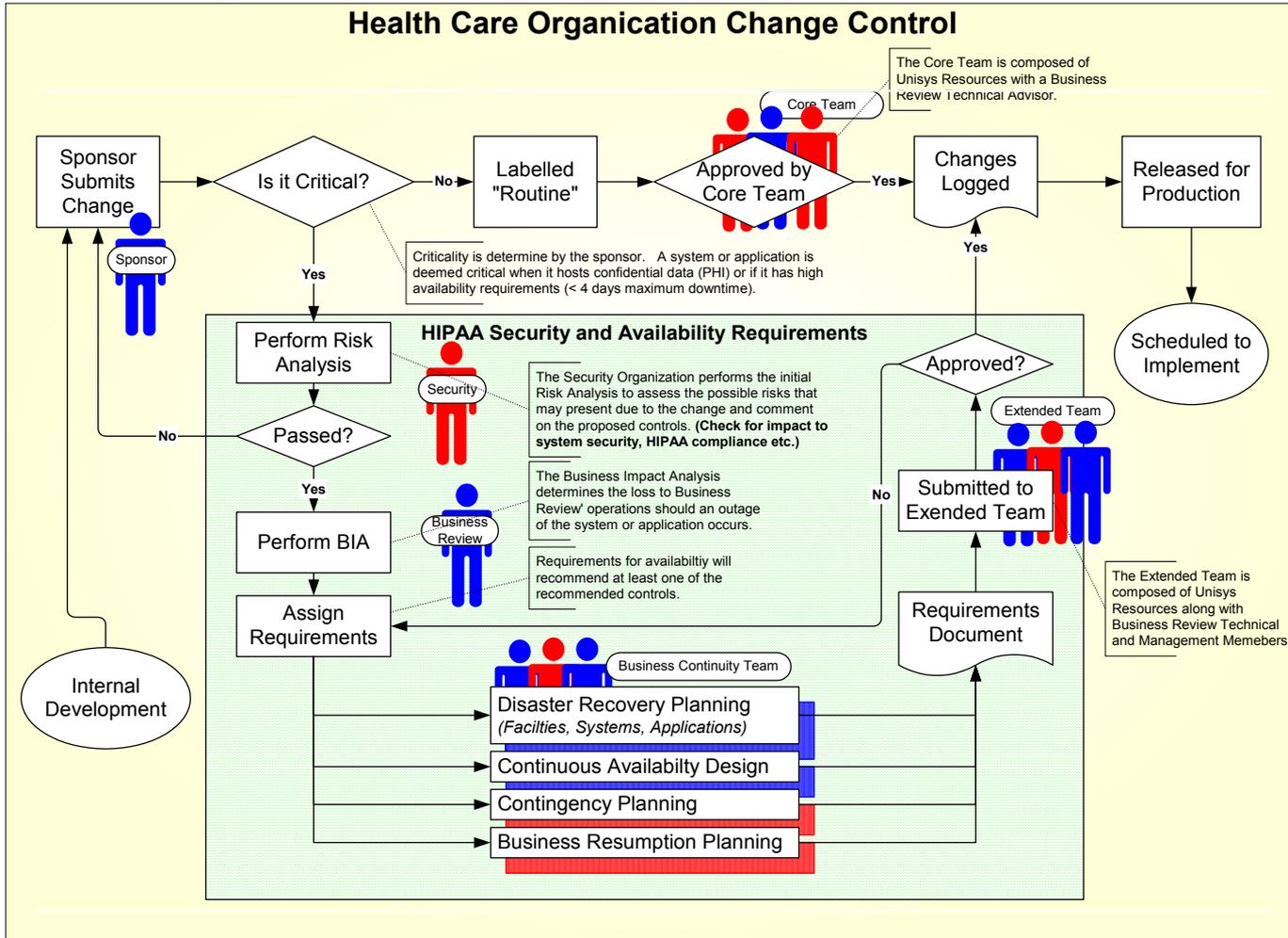


Security Risk Analysis

- A Security Risk Analysis should be invoked whenever a major change is involved in a system or network such as:
 - A new system, application or database is commissioned
 - A change has been submitted that would affect a system, application or database security set up that is deemed business critical or hosts PHI.
 - A security risk analysis should be used to prevent any weakening of your current security set up through any unreviewed institution of changes.
 - By being a part of CM, security analysis keeps security considerations for systems and networks in the minds of business users, programmers and network managers.

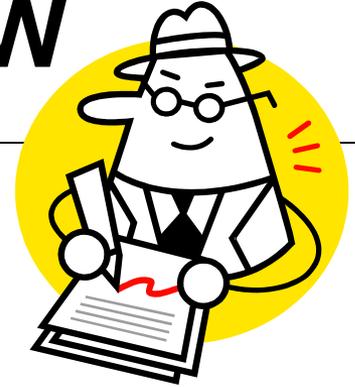


Change Control and Risk Analysis Example Process:

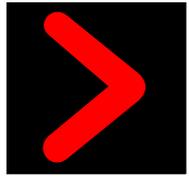




Review...Review...REVIEW



- Review audit logs
- Review system access documentation
- Review intrusion attempts or successes
- Review procedures and modify as needed!!
Processes and needs change!!!
- Keep up with technology changes in security
- “Know thy enemy” ...Security/network staff should become familiar with hacker/cracker tools.
- Encourage a network staff member or your security officer to obtain their CISSP certification



System's Security & Disaster Recovery





Disaster Recovery – Questions to Ask

Overall, when it comes to security and disaster recovery, senior management should be able to answer these questions:

- **Do DR plans involve a review of documentation storage in the event of a disaster?**
- **Are there plans to remove access to systems from backup sites and retrieve data once regular systems are back on line?**
- **Does a return to normal business also signal a return of all electronic data where no longer needed?**
- **Is the transport of data for DR purposes done in a secure manner?**
- **Is the storage of PCs, servers and any other equipment normally used to conduct business stored in a secure manner if removed from site in the event of a disaster?**
- **Are replacement machines, servers etc. wiped before put back into service outside your office's DR support?**
- **Are all paper reports, files that are used to support the office during the disaster destroyed or securely stored once there is a return to normal business?**



Overall Physical Assessment Check List for Servers:

Physical Security Sample Questions:

- Are any Servers, routers and telecommunications located in non-locked publicly accessible or department-wide accessible locations?
- Are all distributions of badges and passkeys recorded on a paper log or database?
- Is all public traffic in and out of the facility controlled and monitored by a security guard, receptionist or video surveillance?
- Are administrator passwords commonly known in an office setting?





Helpful Security Resources

- **ISO17799 Security Guidelines**
- **CMS Information Systems Security, Policy, Standards and Guidelines Handbook(*The Handbook*) Feb, 2002**
- **NSA - The 60 Minute Network Security Guide -(First Steps Towards a Secure Network Environment)**
- **NSA - Guide to the Secure Configuration and Administration of Microsoft.SQL Server. 2000**
- **NSA - Microsoft Windows 2000 -IPsec Guide**
- **NSA - Guide to the Secure Configuration and Administration of Microsoft Internet Information Server 4.0 (Checklist Format)**



HIPAA Security & Privacy

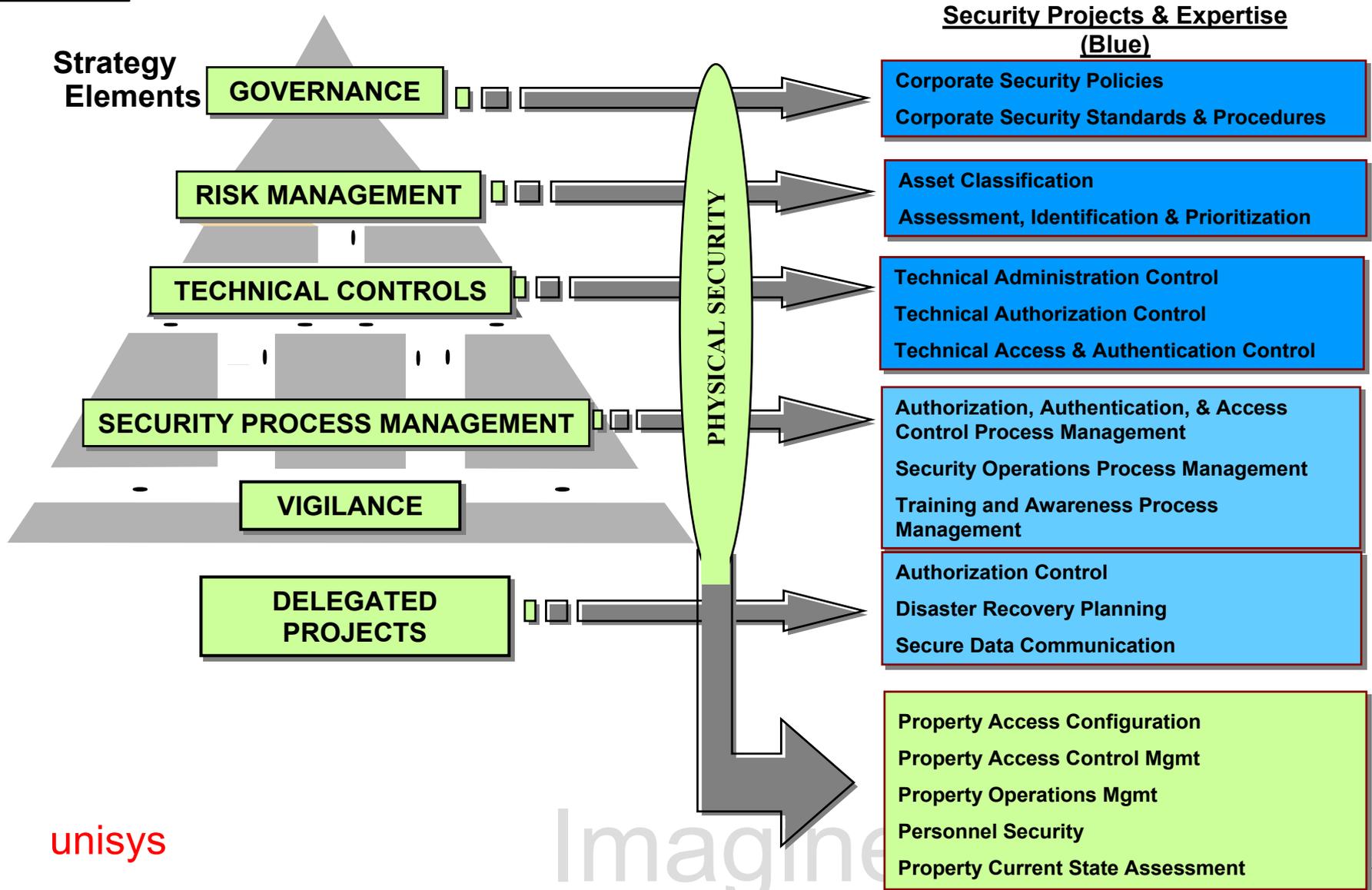


REMEMBER!!!!

- Data that is not Secure either physically or electronically is open to possible violations of the Privacy Rule's "Minimum Necessity" and proper Use and Disclosure regulations.



Minimum HIPAA Security Projects Required for Privacy Compliance



- > Systems Integration.
- > Outsourcing.
- > Infrastructure.
- > Server Technology.
- > Consulting.

2003 CMS HIPAA/MMIS
Conference

New Orleans, LA

February 12, 2003

unisys

Imagine it. Done.



- > Systems Integration.
- > Outsourcing.
- > Infrastructure.
- > Server Technology.
- > Consulting.

2003 CMS HIPAA/MMIS
Conference

New Orleans, LA

February 12, 2003

unisys

Imagine it. Done.

