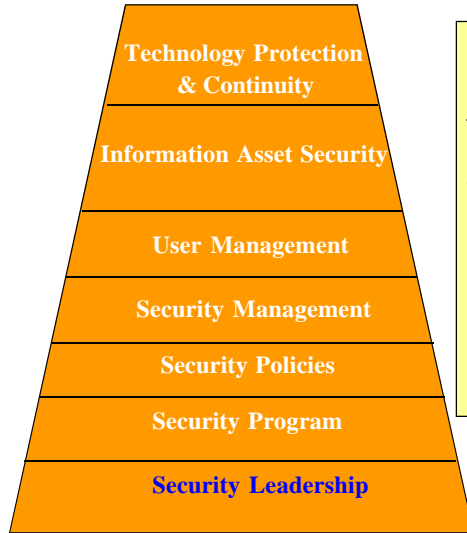


Enterprise Security Capabilities Model

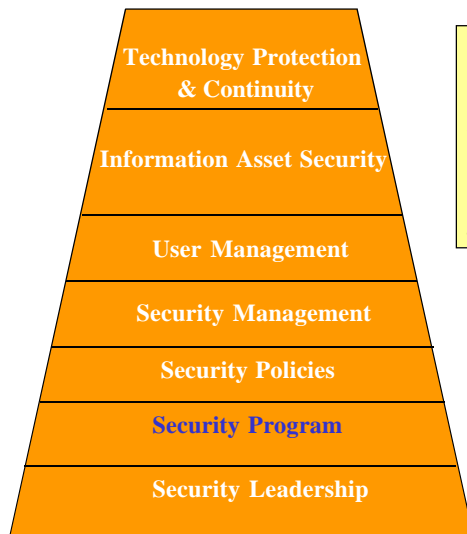


Security Leadership

- Establishes the “chain-of-command” for Information Security from the Board of Directors to the individual employee
- Sets the direction for Information Security at USAA
- Enables resources for Information Security plans and programs
- Performs oversight of Information Security Programs



Enterprise Security Capabilities Model

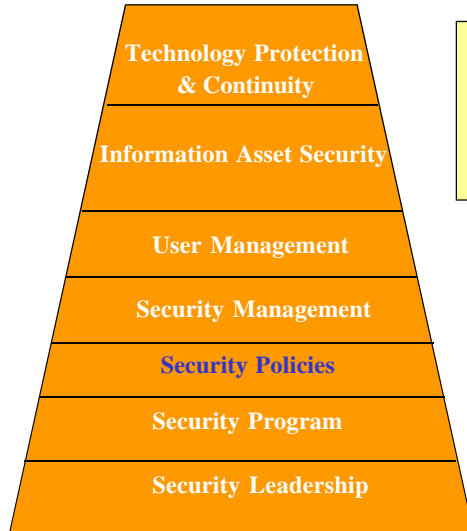


Security Program

- Defines the overall Information Security processes and functions at USAA
- Includes plans, programs, personnel and resources



Enterprise Security Capabilities Model

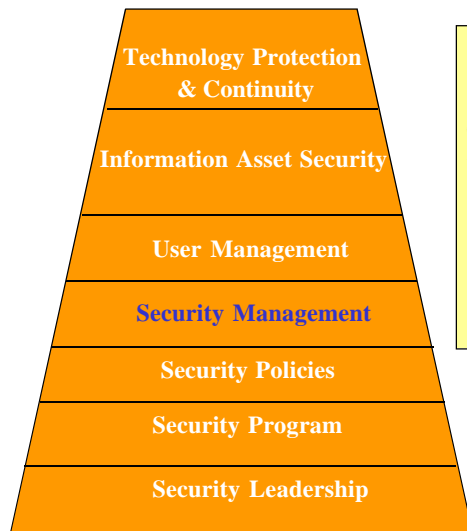


Security Policies

•Policies, standards, guidelines and procedures which codify the Information Security Program at USAA



Enterprise Security Capabilities Model



Security Management

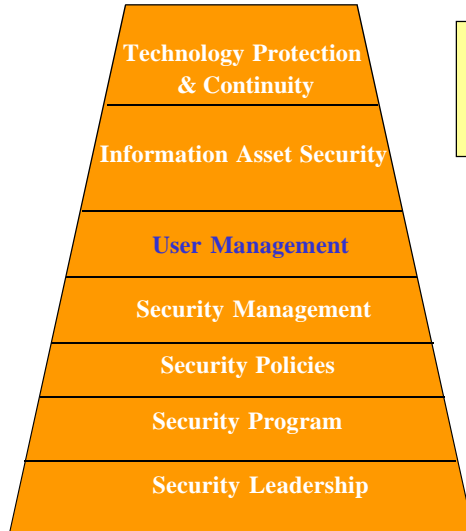
•On-going processes and functions created to ensure Information Security at USAA

For example:

- Access controls
- Anti-virus measures
- E-Security



Enterprise Security Capabilities Model

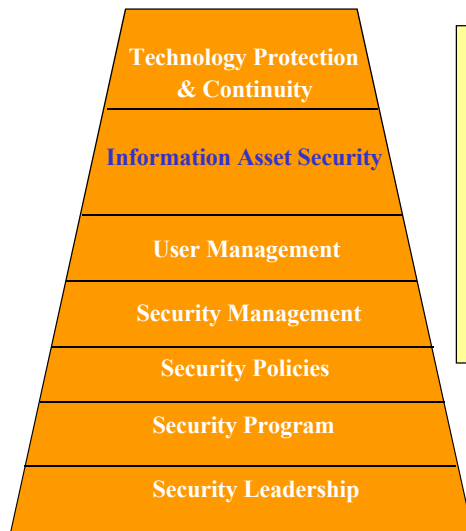


User Management

- Management of system user access
- User awareness functions



Enterprise Security Capabilities Model



Information Asset Security

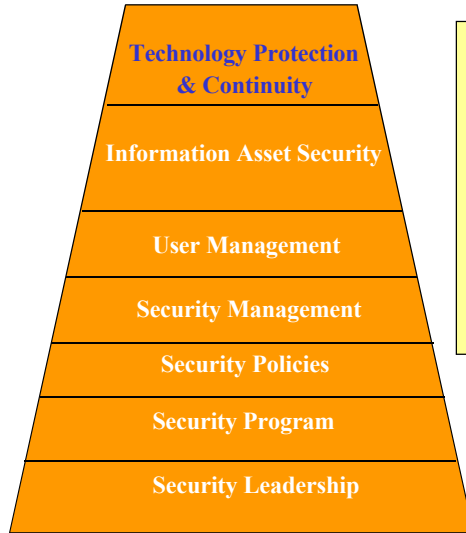
- Management of security controls related to specific technologies

For example:

- Network access
- Mainframe access
- Database access
- Desktop security



Enterprise Security Capabilities Model



Technology Protection & Continuity

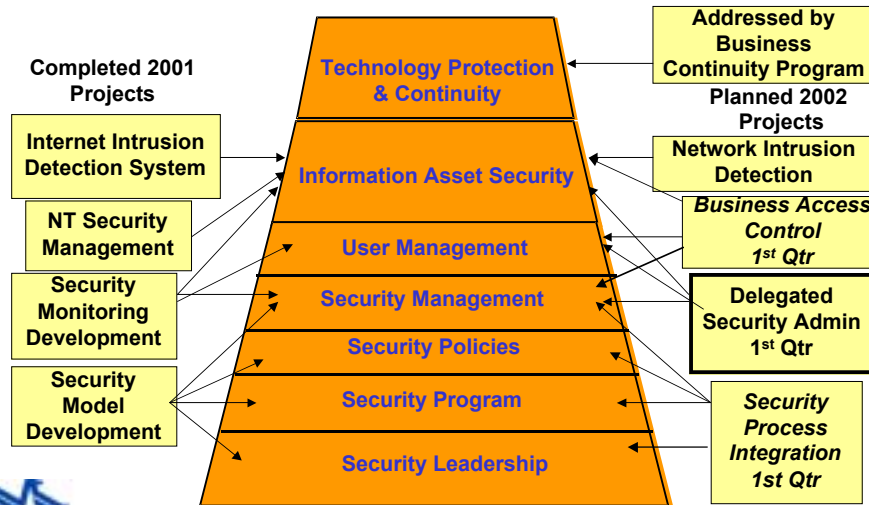
•Management of security controls related to the physical environment

For example:

- Access to computer rooms
- Plans for emergency power
- Disaster recovery plans



Integrated Security Program Project Linkages to Enterprise Security Model



Information Security Policy & Standards Hierarchy

The relationship...



- A single, very high-level document that states USAA's Information Security policy



Information Security Policy & Standards Hierarchy

The relationship...



- Fourteen high-level standards that define USAA's complete Information Security environment

For example:

- Physical Security (e.g. Visitor access must be controlled.)
- Environmental Security (e.g. Uninterruptible Power Supplies (UPS) must be installed for mission critical devices .)
- Et cetera



Information Security Policy & Standards Hierarchy

The relationship...



- A single, comprehensive document which defines the do's and don'ts of Information Security at USAA
- Details the specific requirements needed to comply with the Enterprise Standards

For example:

“Ensure that entry points (doors, windows, ceilings, floors, etc.) to secure areas are monitored at all times, locked when unattended, and routinely checked.”



Information Security Policy & Standards Hierarchy

The relationship...



- Standards that define how to adequately secure a specific technology (e.g. IBM OS390, Oracle, etc.)
- Details the specific requirements needed to comply with the Enterprise Standards and Guidelines

For example:

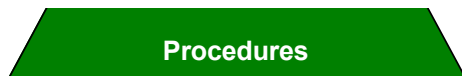
“Will remove all unneeded or vulnerable scripts, certificates, sample applications, paths, directories, services, or code as part of the Oracle DBMS installation / configuration process.” (Oracle Standard)



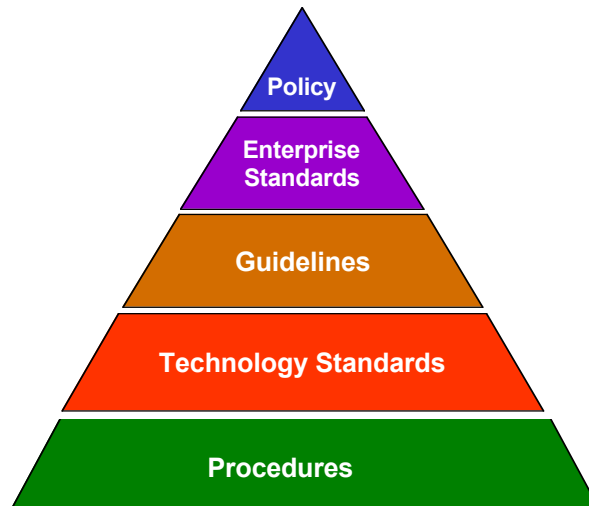
Information Security Policy & Standards Hierarchy

The relationship...

•Step-by-step “cookbook” procedures for performing the requirements defined in the Technology Standards



Information Security Policy & Standards Hierarchy



Customer Data Security & Privacy

- Be prepared for a different kind of exam
 - SEC / Department of Insurance Partnership
 - Enlarged scope
 - Increased coordination effort
 - Privacy inquiry more like a holding company exam
 - Don't expect a lot of feedback...
“We do not have any written comments at this time.”



SEC / TDI Exam – How it Played Out

- SEC was lead for Security & Privacy
 - SEC Team was senior, including one individual who helped author the rules.
 - Requested & reviewed many documents early.
 - Second on-site visit included 2 days of our presentations on Security & Privacy.
 - More documents requested.
 - Two week site visit reviewed many areas, and went into great detail on selected topics (e.g., **Firewalls**).



SEC / TDI Exam – How it Played Out

- Privacy and Security began together, then addressed in parallel.
 - Especially in Privacy, examiners wanted to view our policies and procedures in practice.
 - Privacy records and privacy complaints reviewed.
 - Lots of interest in why we made decisions we did on both Privacy and Security.



Looking Ahead

- Major Concerns Ahead
 - FCRA Preemption expires January 2004
 - Regulatory environment not favorable for extension
 - 2003 will be watershed year for Privacy at the Federal Level
 - Wireless is a major risk – wireless products (with rare exception) do not yet include mature security
 - Instant Messaging is another technology that is not yet security mature





Jurisdiction

- **HIPPA**
 - Secretary Health & Human Services
- **Privacy (GLB)**
 - OTS, FDIC, SEC, FDIC
 - Dept of Insurance (within State GLB)



Safeguarding Customer Information

- **Passwords**

- Passwords can be your weakest link
- Ensure passwords are strong
 - Combination of letters, numbers and special characters
 - Never use dictionary words, or easily guessed dates/numbers
 - Run “cracker” programs to find out how strong passwords actually are <http://www.l0phtcrack.com/>
 - Pay special attention to passwords accessing your most critical systems or with administrator privileges



Safeguarding Customer Information

- **Information Security Training**

- Training for all new employees and contractors / consultants
- Annual Refresher Training
- Frequent communications regarding importance of sound practices
- Identify Theft as a major concern – employee awareness can really pay off



Safeguarding Customer Information

- Disaster Recovery / Business Resumption
 - Our Plans changed after 9-11
 - Assumption we could fly people and data to alternate location proved invalid
 - USAA utilizes our own DR / BR site, within Driving Distance
 - Have held multiple exercises of Infrastructure, then full Line of Business Recoveries
 - Business a very active participant

