

Access Control -- Control Type

❖ *DigitalSherlock.com | SafeHack.com*

❖ *Date: 2005/05/27*

❖ *Document Name: access_control_control_type.pdf*

❖ *GNU Free Documentation License*

❖ *Version 1.00, 2005-05-27*

❖ *Copyright © 2005 Adonis, MSc, Eng, CISSP, Security+, CEH, GSec, MCSE, etc.*

❖ *Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation.*

❖ Technical & Detective

➤ Intro

- **Measures intended to reveal the violations of security policy**
- **These measures include**
 - Intrusion Detection Systems
 - Automatically generated violation reports
- **To limit the amount of audit information a "clipping level" can be set**
- **Using clipping levels refers to setting allowable Thresholds on a reported activity.**

➤ Examples

- **Audit trail**
- **automated security monitoring**
- **Bebugging**
- **Check digit**
- **checksum**
- **Cycle checkers**
- **cyclic redundancy check (CRC)**
- **digital signature**
- **Error seeding**
- **HASH total**
- **intrusion detection**
- **Journal**
- **Limit checks**
- **Operating system (Console) log**
- **Parity checking**
- **penetration testing**
- **Reasonability checks**
- **Quality control**
- **Alarms and Alerts**
- **Firewall**
- **Antivirus software**

❖ Technical & Preventive

➤ Intro

- **They are known as Logical controls**
- **They can be built into the Operating system**
- **They can be software controls**
- **They can be hardware controls**

➤ Examples

- Access control Software (System access)
- access control list ACLs
- Access Control Measures
- Access Password
- Authentication Process
- passphrase
- Protocols
- Encryption
- end-to-end encryption
- end-to-end security
- fetch protection
- link encryption
- one-time passwords
- Biometrics
- Constrained user interface
- Menus
- Shells
- Database views
- Virus scanning software
- Limited keypads
- Smart cards
- Disk mirroring
- Disk duplexing
- Firewall
- Audit logs
- Routers
- Network Access, Dial up access, callback systems
- Network Architecture
- Antivirus software
- intrusion detection
- Smart Cards

❖ Control type ?

- § Deterrent/Preventative
 - Use to discourage occurrences
- § Detective
 - Detective Technical Controls warn of technical Access Control violations
 - Used to detect or identify occurrence)
- § Corrective
 - Are used to restore systems that are victims of harmful attacks
- § Recovery
 - Used to restore resources, capabilities, or losses

❖ Which control is what ?

- Control by action include:
 - Preventive

- Detective
- Corrective
- **Control by function include:**
 - Management controls
 - Technical controls
 - Operational controls

❖ **Access control Protect**

- **Integrity**
 - Prevention of the modification of information by unauthorized users
 - Prevention of unauthorized modification of information by authorized users
 - Preservation of internal and external consistency
 - Internal consistency ensures that internal data is consistent
 - External ensures that the data stored in the database is consistent with the real world
 - Information must be accurate, complete and protected from unauthorized modification
- **Confidentiality**
 - Assures that the information is not disclosed to unauthorized persons or processes
 - To protect data's confidentiality you need to identify which information is sensitive
- **Availability**
 - Assures that authorized users have timely uninterrupted access to the system
 - resources need to be available to users in a timely manner
 - Fault tolerance and recovery ensure the continuity of availability

❖ **Physical & Administrative**

- Facility selection or construction
- Facility management
- Personnel controls
- Training
- Emergency Response and procedures

❖ **Physical & Detective**

- **Intro**
 - Require a human to evaluate the input from sensors
- **Examples**
 - Motion detectors
 - Thermal detectors
 - Smoke and fire detectors
 - Sensors and alarms
 - Closed circuit TV monitoring
 - Security guards, Dogs
 - Biometric access controls
 - Closed circuit TV monitoring
 - Backup

❖ **Administrative & Detective**

- **Intro**

- Warn of technical Access Control violations
- Prevent future security policy violations

➤ **Example**

- Organizational policies, Procedures
- Security reviews and audits
- Performance Evaluation
- Organizational Procedures
- Background checks
- Labeling of sensitive material
- Increased supervision
- Security awareness training
- Behavior awareness
- Sharing of responsibilities
- Reviews of audit records
- Background Investigation
- Job rotation
- Required vacations
- functional testing

❖ **Administrative & Preventive**

- Security Policies and procedures
- Draft Inspection Reports
- Accountability
- Acceptance testing
- Quality assurance QA
- Authorization
- certification
- dual control
- Integration test
- functional testing
- Record retention
- Monitoring & Supervising
- Separation of duties
- Job rotation
- Information classification
- Personal Procedures
- Hiring procedures
- Security awareness training
- Work habit checks
- Personal Screening
- Background Investigation
- User Registration for computer access
- Termination of employee policy

- Disaster recovery and contingency plan

❖ **Administrative & Corrective**

- contingency plan
- Security Policy