

Access Control

“Access control is the process of granting or denying requests to use information, use information processing services, and enter company facilities.”

(Sec. 3.1 NIST Handbook 162)

C001 Establish system access requirements



AC.1.001 Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems)



A screenshot of a 'Member login' form. It features a user icon at the top, followed by the text 'Member login'. Below this are two input fields: 'Username' and 'Password'. There is a 'Remember me' checkbox and a 'Forgot password?' link. At the bottom is an orange 'Login' button.



Audit
Objective

Acceptable
Evidence

Interviews

Evaluate/
Test

AC.2.005 Provide privacy and security notices consistent with applicable CUI rules

```
WARNING: There is no expectation of privacy when using this system
-----
Use of this system should only be for official purposes only and
Unauthorised access or use of this equipment is prohibited
and constitutes an offence under the Computer Misuse Act 1990.
If you are not authorized to access this system, terminate
this session immediately.
All those who are accessing this device are subject to having
their activities monitored and recorded, any abuse or criminal activity
may be turned over to law enforcement or other appropriate officials.
-----
If you gain access to this device, you are accepting all conditions laid
out above
-----
Using keyboard-interactive authentication.
Password: █
```



Audit
Objective

Acceptable
Evidence

Interviews

Evaluate/
Test

AC.2.006 Limit use of portable storage devices on external systems



Audit
Objective

Acceptable
Evidence

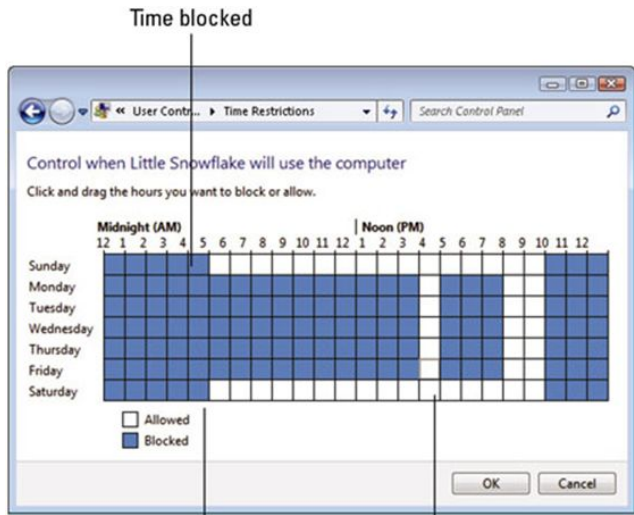
Interviews

Evaluate/
Test

C002 Control Internal system access



AC.1.002 Limit system access to the types of transactions and functions that authorized users are permitted to execute



Purchase - Good



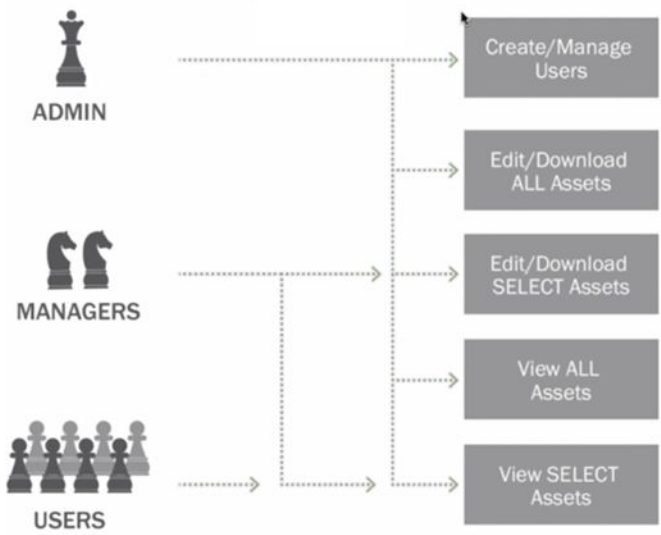
Audit
Objective

Acceptable
Evidence

Interviews

Evaluate/
Test

AC.2.007 Employ the principle of least privilege, including for specific security functions and privileged accounts



Audit
Objective

Acceptable
Evidence

Interviews

Evaluate/
Test

AC.2.008 Use non-privileged accounts or roles when accessing non-security functions



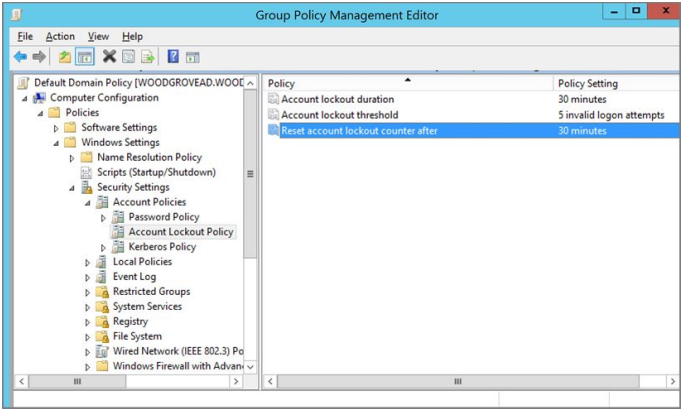
Audit
Objective

Acceptable
Evidence

Interviews

Evaluate/
Test

AC.2.009 Limit unsuccessful logon attempts



Audit
Objective

Acceptable
Evidence

Interviews

Evaluate/
Test

AC.2.010 Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity

Information is hiding or blurred out.



User is locked out.

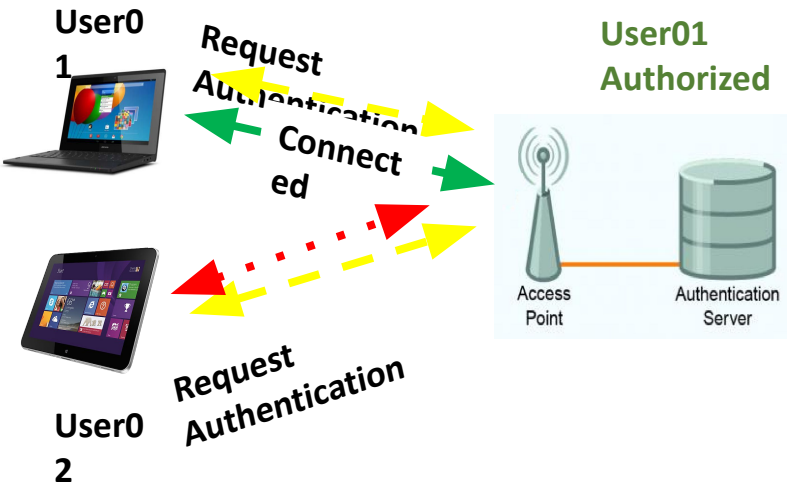
Audit
Objective

Acceptable
Evidence

Interviews

Evaluate/
Test

AC.2.011 Authorize wireless access prior to allowing such connections



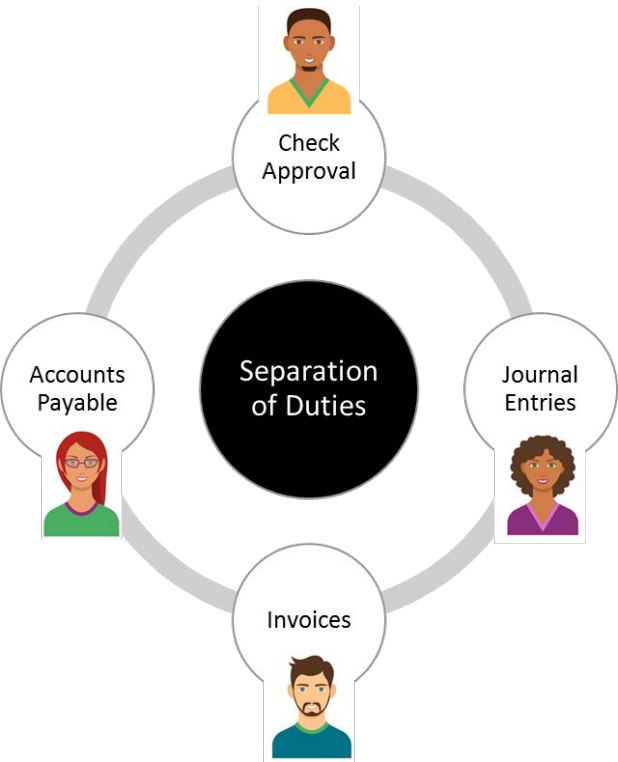
Audit
Objective

Acceptable
Evidence

Interviews

Evaluate/
Test

AC.3.017 Separate the duties of individuals to reduce the risk of malevolent activity without collusion



Audit
Objective

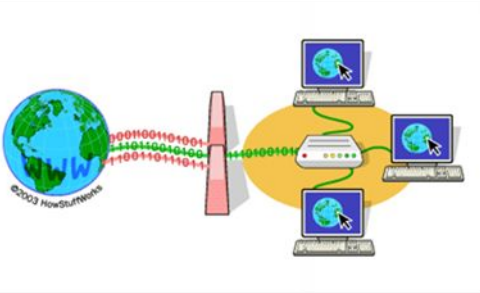
Acceptable
Evidence

Interviews

Evaluate/
Test

AC.3.018 Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs

Cannot execute privileged functions



Non-privileged access

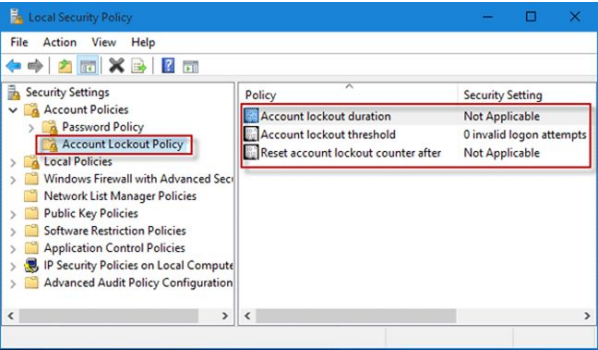
Audit
Objective

Acceptable
Evidence

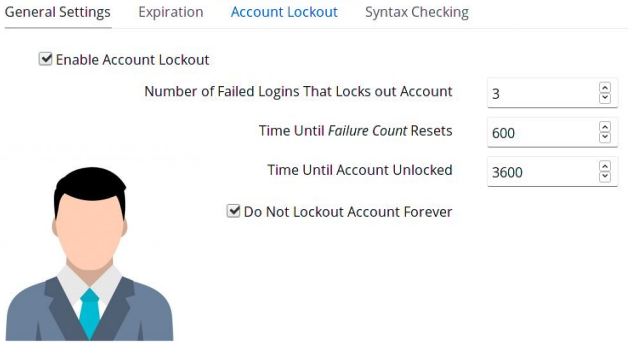
Interviews

Evaluate/
Test

AC.3.019 Terminate (automatically) a user session after a defined condition



Policy	Security Setting
Account lockout duration	Not Applicable
Account lockout threshold	0 invalid logon attempts
Reset account lockout counter after	Not Applicable



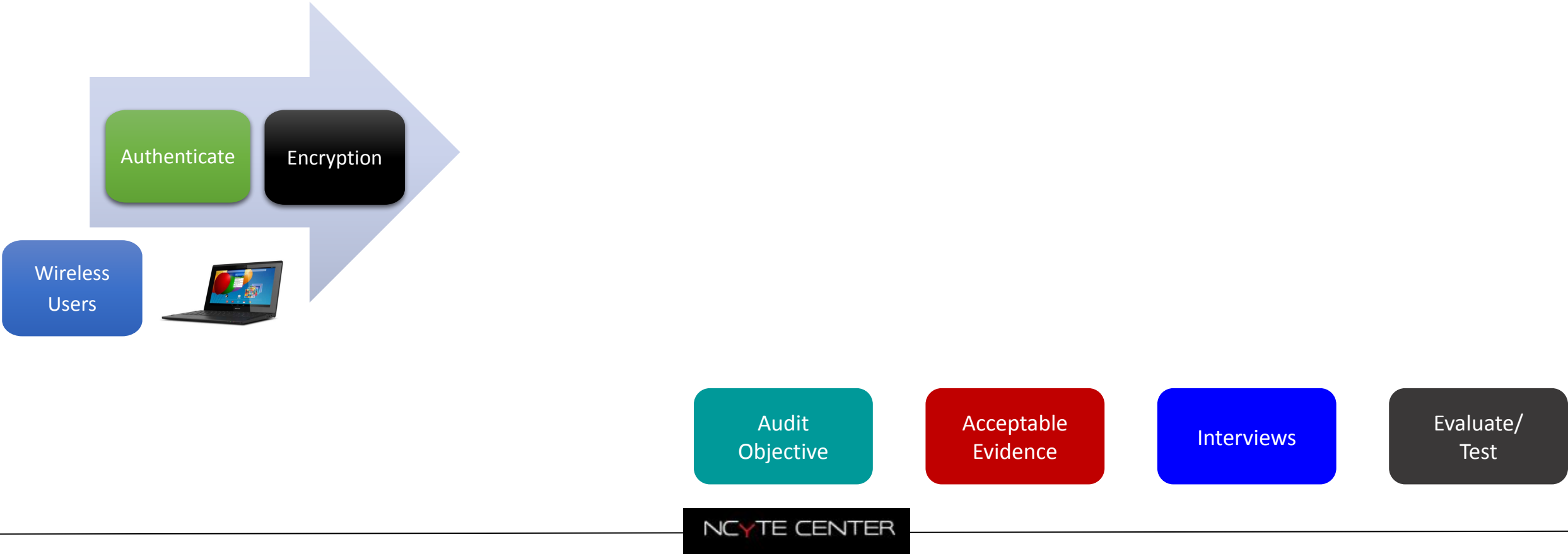
Audit
Objective

Acceptable
Evidence

Interviews

Evaluate/
Test

AC.3.012 Protect wireless access using authentication and encryption





Audit
Objective

Acceptable
Evidence

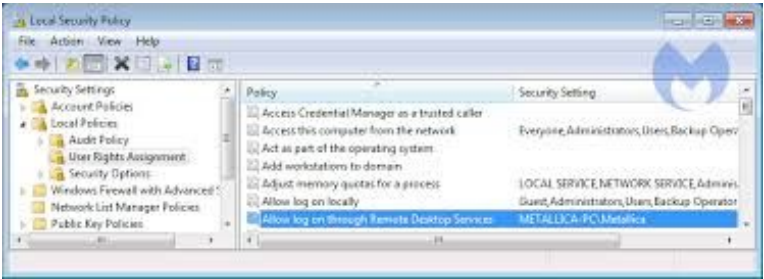
Interviews

Evaluate/
Test

C003 Control remote system access



AC.2.013 Monitor and control remote access sessions



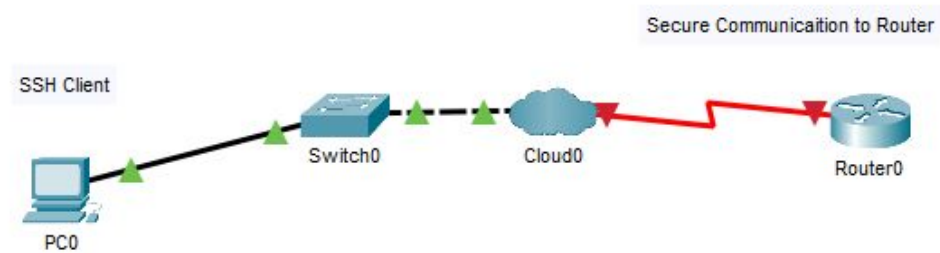
Audit
Objective

Acceptable
Evidence

Interviews

Evaluate/
Test

AC.2.015 Route remote access via managed access control points



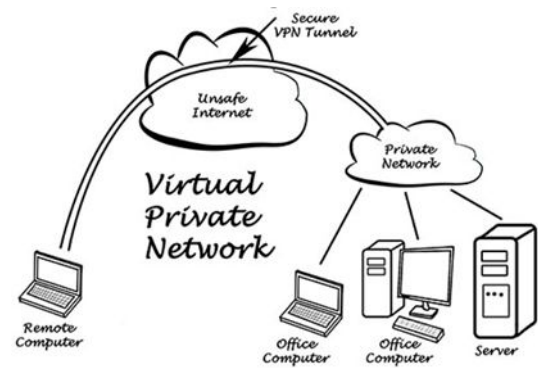
Audit
Objective

Acceptable
Evidence

Interviews

Evaluate/
Test

AC.3.014 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions



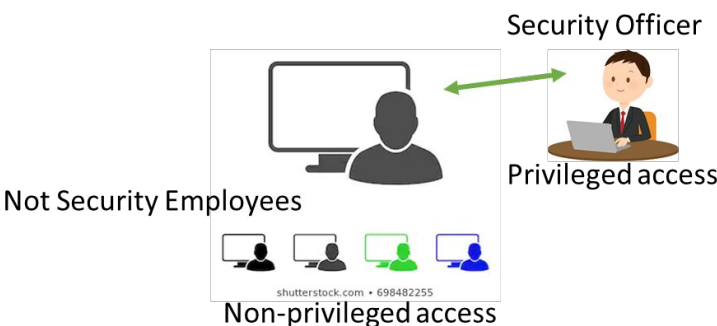
Audit
Objective

Acceptable
Evidence

Interviews

Evaluate/
Test

AC.3.021 Authorize remote execution of privileged commands and remote access to security-relevant information



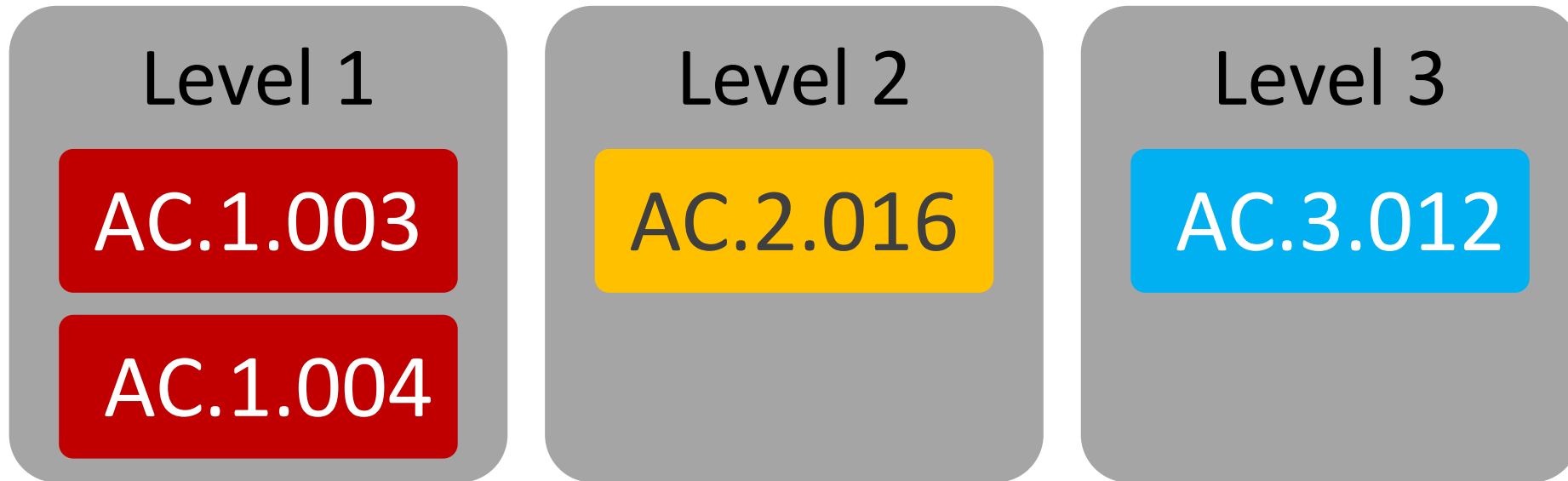
Audit
Objective

Acceptable
Evidence

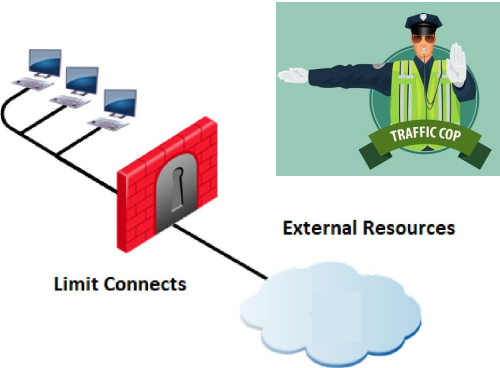
Interviews

Evaluate/
Test

C004 Limit data access to authorized users and processes



AC.1.003 Verify and control/limit connections to and use of external systems



Audit
Objective

Acceptable
Evidence

Interviews

Evaluate/
Test

AC.1.004 Control CUI posted or processed on publicly accessible systems

Posting company data on social media NOT allowed!!



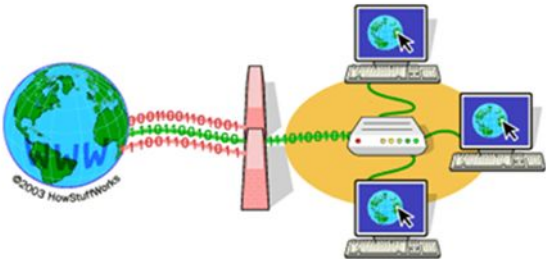
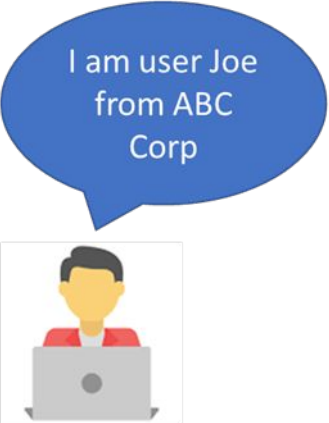
Audit
Objective

Acceptable
Evidence

Interviews

Evaluate/
Test

AC.2.016 Control the flow of CUI in accordance with approved authorizations



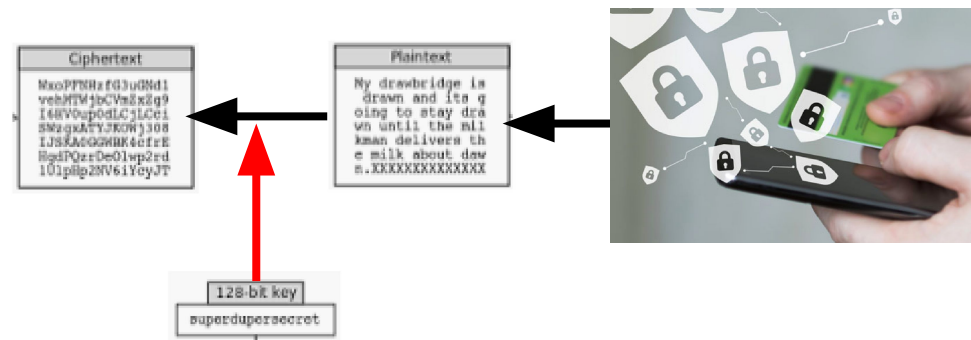
Audit
Objective

Acceptable
Evidence

Interviews

Evaluate/
Test

AC.3.022 Encrypt CUI on mobile devices and mobile computing platforms



Assessment Documentation and Methods

- Access control policy and all other related documents and records
- Procedures addressing access control for mobile devices
- System security plan and design documentation
- System configuration settings and associated documentation
- Encryption mechanisms and associated configuration documentation
- System audit logs and records

Audit Objective

Acceptable Evidence

Interviews

Evaluate/ Test