



COMPLIANCE COMPONENT

DEFINITION	
<i>Name</i>	Access Controls
<i>Description</i>	Access Controls prescribe who or what is to have access to a specific system resource and the type of access permitted.
<i>Rationale</i>	Requirements for using (and prohibitions against the use of) various computer resources can vary considerably. Some resources must be accessible to all users, some by several groups or departments, and some resources should be limited to only a few individuals. Users must have access to the resources they need to do their jobs. However, it is also required to deny access to non-job-related information. Access restrictions enforce policy and help ensure that unauthorized actions are not permitted.
<i>Benefits</i>	<p>Access controls:</p> <ul style="list-style-type: none"> ▪ Prescribe who or what is to have access to a specific system resource ▪ Prescribe type of access that is permitted ▪ Can be built into the operating system or incorporated into: <ul style="list-style-type: none"> ○ Applications programs ○ Major utilities ○ Add-on security packages ▪ Protect operating systems and other system software from unauthorized modification or manipulation ▪ Protect the integrity and availability of information by restricting the number of users and processes with access ▪ Protect confidential information from being disclosed to unauthorized individuals
ASSOCIATED ARCHITECTURE LEVELS	
<i>Specify the Domain Name</i>	Security
<i>Specify the Discipline Name</i>	Technical Controls
<i>Specify the Technology Area Name</i>	Logical Access Controls
<i>Specify the Product Component Name</i>	
COMPLIANCE COMPONENT TYPE	
<i>Document the Compliance Component Type</i>	Guideline
<i>Component Sub-type</i>	
COMPLIANCE DETAIL	
<i>State the Guideline, Standard or Legislation</i>	<p>In deciding whether to permit someone to use a system resource, access controls examine whether the user is authorized for the type of access requested. The system uses various criteria to determine if a request for access will be granted. They are typically used in some combination.</p> <p>The following are various criteria to control access.</p>

- Identity – The majority of access controls are based upon the identity of the user (either human or processes) which is usually obtained through identification and authentication. The identity is usually unique to support individual accountability but can be a group identification.
- Roles – Access to information may also be controlled by the job assignment or function of the user or account seeking access. The process of defining roles should be based on a thorough analysis of how an organization operates.
- Location - Access to particular system resources may also be based upon physical or logical location, i.e. subnet.
- Time – Time of day or day of week restrictions are common limitations on access.
- Transaction Type - Another approach to access control can be used by transactions, i.e. account inquiries. This means that users have no choice in which resources they have access to. Access is limited by the type of transaction being requested.
- Service Constraints - Restrictions that depend upon the parameters that arise during use of the application or that are pre-established by the resource owner or manager. For example, a particular software package may only be licensed by the agency for five users at a time. Access would be denied for a sixth user, even if the user were otherwise authorized to use the application.
- Common Access Modes - In addition to considering criteria for when access should occur, it is also necessary to consider the types of access modes. Common access modes can be used in either operating or application systems, and include the following:
 - Read access provides users with the capability to view information
 - Write access allows users to add, modify, or delete information
 - Execute privilege allows users to run programs
 - Delete access allows users to erase information

Technical Implementation Mechanisms

Many mechanisms have been developed to provide internal and external access controls, and vary significantly in terms of precision, sophistication, and cost. These methods are not mutually exclusive and are often employed in combination. Managers need to analyze their organization's protection requirements to select the most appropriate, cost effective logical access controls.

- Internal Access Controls - Logical means of separating what defined users (or user groups) can or cannot do with system resources.
 - Passwords - Most often associated with user authentication, they are also used to protect data and applications on many systems.
 - Encryption - Is especially useful if strong physical access controls

cannot be provided, such as for laptops or external media.

- Access Control Lists (ACL) - A register of users (including groups, machines and processes) who have been given permission to use a particular system resource, and the types of access they have been permitted.
 - Elementary ACLs. A short, predefined list of the access rights to files or other system resources typically based on the concepts of owner, group, and world.
 - Advanced ACLs. Provide a great deal of flexibility in implementing system-specific policy and allow for customization to meet the security requirements of functional managers.
- Constrained User Interfaces - Restrict users' access to specific functions by never allowing them to request the use of information, functions, or other specific system resources for which they do not have access. Constrained user interfaces can provide a form of access control that closely models how an organization operates. Three major types of constrained user interfaces exist:
 - Menus - Users can only execute commands that are available on the screen.
 - Database views – A means of restricting access to data fields in a database.
 - Physically – Constraining access by limiting the physical means of interacting with the system. For example, a kiosk physically limits access by providing predefined buttons to perform tasks.
- Security Labels - A designation assigned to a resource for the purpose of controlling access, specifying protective measures, or indicating additional handling instructions.
- External Access Controls - A means of controlling interactions between networks and outside entities, systems and services. External access controls use a wide variety of methods, including separate physical devices, i.e. firewalls, between the system being protected and another network.
 - Port Protection Devices (PPD) - Fitted to a communications port of a host computer, a PPD authorizes access to the port itself, prior to and independent of the computer's own access control functions. A PPD can be a separate device in the communications stream, or it may be incorporated into a communications device (e.g., a modem). PPDs typically require a separate authenticator, such as a password, in order to access the communications port.
 - Secure Gateways and Firewalls - Blocks or filters access between two networks, often between a private network and a larger, more public network such as the Internet. Secure gateways allow internal users to connect to external networks and at the same

time prevent compromising the internal systems. For additional information on gateways and firewalls see the Secure Gateways and Firewalls Technology Area and associated Compliance Components.

- Host-Based Authentication - Grants access based upon the identity of the host originating the request, instead of the identity of the user making the request. Many network applications use host-based authentication to determine whether access is allowed.

Under certain circumstances it is fairly easy to masquerade as the legitimate host, especially if the masquerading host is physically located close to the host being impersonated.

Administration of Access Controls

One of the most complex and challenging aspects of access control, administration involves implementing, monitoring, modifying, testing, and terminating user accesses on the system. Decisions regarding accesses should be guided by agency policy, employee job descriptions and tasks, information sensitivity, user need-to-know determinations or other factors. There are three basic approaches to administering access controls: centralized, decentralized, or a combination of these. Each has relative advantages and disadvantages. Which is most appropriate in a given situation will depend upon the particular agency and its circumstances.

- Centralized Administration - One office or individual is responsible for configuring access controls. As users' information processing needs change, their accesses can be modified only through the central office, usually after requests have been approved by the appropriate official. This allows very strict control over information, because the ability to make changes resides with very few individuals. Each user's account can be centrally monitored, and closing all accesses for any user can be easily accomplished if that individual leaves the organization. Since relatively few individuals oversee the process, consistent and uniform procedures and criteria are usually not difficult to enforce. However, when changes are needed quickly, going through a central administration office can be time consuming.
- Decentralized Administration - Access is directly controlled by the owners or creators of the files, often the functional manager. This keeps control in the hands of those most accountable for the information, most familiar with it and its uses, and best able to judge who needs what kind of access. This may lead, however, to a lack of consistency among owners and creators as to procedures and criteria for granting user accesses and capabilities. Also, when requests are not processed centrally, it may be much more difficult to form a system-wide composite view of all user accesses on the system at any given time. Different application or data owners may inadvertently implement combinations of accesses that introduce conflicts of interest or that are in some other way not in the agency's best interest. It may also be difficult to ensure that all accesses are properly terminated when an employee transfers internally or leaves an agency.
- Hybrid Approach - Combines centralized and decentralized administration. One typical arrangement is that central administration is responsible for the broadest and most basic accesses, and the owners or creators of files control types of accesses or changes in users' abilities for the files under their control. The main disadvantage to a hybrid approach is adequately

	<p>defining which accesses should be assigned locally and which should be assigned centrally.</p> <p>It is vital that access controls protecting a system work together. The development of an access control policy may not be an easy endeavor. It requires balancing the often-competing interests of security, operational requirements, and user friendliness.</p> <p>Access controls are a means of implementing policy decisions. Policy is made by management responsible for a system, application or group of systems. Once these policy decisions have been made, they will be implemented through access controls. In doing so, it is important to realize that the capabilities of various types of mechanisms vary greatly.</p>		
<i>Document Source Reference #</i>	NIST SP 800-12		
Compliance Sources			
<i>Name</i>	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	<i>Website</i>	http://csrc.nist.gov
<i>Contact Information</i>			
<i>Name</i>		<i>Website</i>	
<i>Contact Information</i>			
KEYWORDS			
<i>List Keywords</i>	Access Control Lists, ACL, logic, physical, port, interface, password, encryption, menu, constrained, database, file, field, labels, host, protection, access.		
COMPONENT CLASSIFICATION			
<i>Provide the Classification</i>	<input type="checkbox"/> <i>Emerging</i> <input checked="" type="checkbox"/> <i>Current</i> <input type="checkbox"/> <i>Twilight</i> <input type="checkbox"/> <i>Sunset</i>		
<i>Sunset Date</i>			
COMPONENT SUB-CLASSIFICATION			
<i>Sub-Classification</i>	<i>Date</i>	<i>Additional Sub-Classification Information</i>	
<input type="checkbox"/> <i>Technology Watch</i>			
<input type="checkbox"/> <i>Variance</i>			
<input type="checkbox"/> <i>Conditional Use</i>			
Rationale for Component Classification			
<i>Document the Rationale for Component Classification</i>			
Migration Strategy			
<i>Document the Migration Strategy</i>			
Impact Position Statement			
<i>Document the Position Statement on Impact</i>			

CURRENT STATUS

Provide the Current Status

In Development

Under Review

Approved

Rejected

AUDIT TRAIL

Creation Date

02/01/2007

Date Approved / Rejected

03/23/2007

Reason for Rejection

Last Date Reviewed

Last Date Updated

Reason for Update