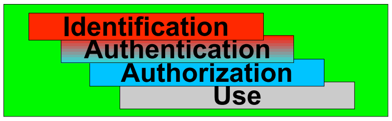
8.5 Access process



Rate each issue from 0-10.

Issue	*Rate*
The access process is designed based on the notion that the utility of the overall information capability of the enterprise depends on the ability to legitimately access the information resources with minimal friction while still assuring the continuing value of the information in light of the hostilities of the environment in which it works.	
The access process architecture defines how identified subjects demonstrate their identities through authentication, and how the properly authenticated identified subjects can then use the content through an authorization mechanism.	
TOTAL (total and divide by 2)	

8.5.1 Identification

Rate each issue from 0-10.

Issue	*Rate*
Identity of people and things, including programs and processes are unique tags that allow individuals to be associated with other properties.	
An identification system is used to track identities and associate them with these other properties.	
Initialization of identification processes are designed to meet the needs of the clearances and classifications of the identified entities.	
For low surety situations, nominal background checks and standard government identities are considered adequate for initial identification.	
Clearance processes with background checks and detailed life reviews are invoked for situations in which people have to be identified with higher surety upon entry to a system of identification.	
For externally mandated clearance processes, the external mandates for initial identification are used in addition to internal requirements.	
Pedigrees for hardware and software are considered in determining suitability for trust in high risk situations.	
TOTAL (total and divide by 7)	

8.5.2 Authentication

Rate each issue from 0-10.

Issue	*Rate*
Authentication is used to verify the authenticity of identity to a level of surety based on testing that identity against its known properties in the identification system.	

Issue	*Rate*
The surety of the authenticity of an identification is tied to the available properties in the identification system and the ability to present and verify those factors as present or absent in the individual in question.	
For higher risk, higher surety is desired, and sequential authentications are used to increase the certainty with which authenticity of an identity is believed.	
Different properties have different defined surety levels based on their ability to withstand different threats more or less successfully.	
The surety of authentication is not trusted beyond the surety of the identification system used to authenticate the properties.	
Threat capabilities and intents are considered in evaluating the surety of authentication techniques.	
TOTAL (total and divide by 6)	

8.5.3 Authorization

Rate each issue from 0-10.

Issue	*Rate*
Subjects are only authorized to uses after the subject's identity has been authenticated to an adequate level for the access decision process to be completed.	
Based on a requested use, the identity, and the surety of authentication, use is treated in one or more of a set of pre-defined ways.	
TOTAL (total and divide by 2)	

8.5.4 Use

Rate each issue from 0-10.

Issue	*Rate*
The whole process as as transparent and automatic to the user relative to the utility associated with that use as feasible for the surety required and the applicable costs constraints.	
The effort and surety for simple low-risk operations is minimal.	
The effort required to perform the process never exceeds the business value granted by that use.	
Authentication allows use of a set of capabilities for a period of time so that a single authenticated identity is authorized for sets of activities which are performed without additional authentication at every step.	
The time and set of activities permitted are limited by risk management determined factors.	
For high valued transactions, like large financial transfers or setting off explosive devices, additional authentication is warranted and applied.	

Issue	*Rate*
Additional authentication associated with that high valued transaction is leveraged to allow uninhibited subsequent use for a period of time and to a set of functions where feasible.	
Where feasible, use in excess of least privilege is not granted.	
Where additional access is granted, risk management approval is required prior to implementation of the system and at periodic intervals over the life cycle of its use.	
When additional access is granted, audit mechanisms associated with use are used to provide additional checks on that use and to limit the effects of illicit use.	
In all cases, use is audited if the value of the operation exceeds the threshold of risk requiring audit or if there are regulatory or other drivers that mandate auditing of use.	
TOTAL (total and divide by 11)	

8.5.5 Roll-up

Issue	*Rate*
Access process	
Identification	
Authentication	
Authorization	
Use	
TOTAL (total and divide by 5)	

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
2	5	3	7	9