DFARS

Assessment Summary

NIST 800-171 Key areas

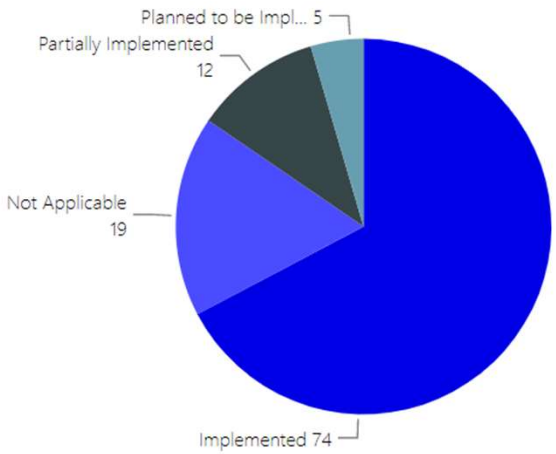
- Access Control
- Audit and Accountability
- Awareness and Training
- Configuration Management
- Identification and Authentica...
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical Protection
- Risk Assessment
- Security Assessment
- System and Communication...
- System and Information Inte...

Risk Level

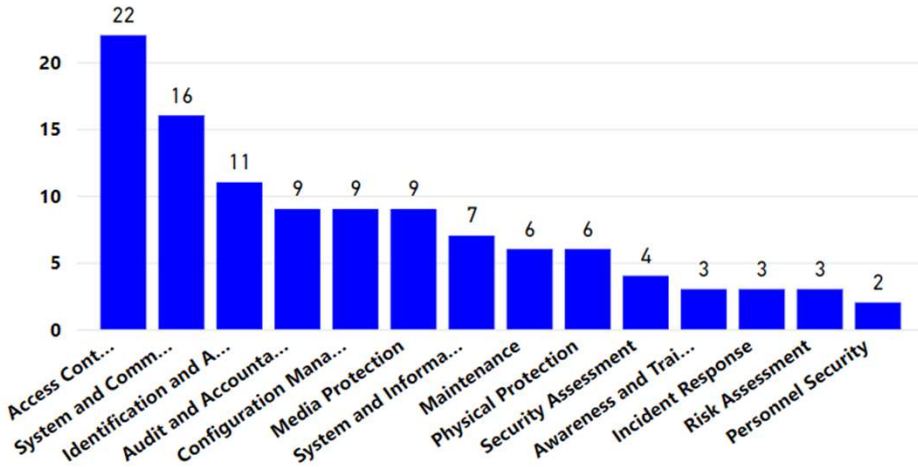
High

Medium

Count of Status of Domains



Control measures



Control	Domain	Control Text
3.3.4	Audit and Accountability	Alert in the event of an audit process failure.
3.5.9	Identification and Authentication	Allow temporary password use for system logons with an immediate change to a permanent password.
3.4.4	Configuration Management	Analyze the security impact of changes prior to implementation.
3.4.8	Configuration Management	Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.
3.5.2	Identification and Authentication	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite

DFARS

Assessment Summary

Domain	Actual	Target	Implemented	Gap
Access Control	22	20	17	3
Audit and Accountability	9	6	3	3
Awareness and Training	3	3		3
Configuration Management	9	7	5	2
Identification and Authentication	11	9	9	
Incident Response	3	2		2
Maintenance	6	5	4	1
Media Protection	9	6	6	
Personnel Security	2	2	2	
Physical Protection	6	5	3	2
Risk Assessment	3	3	2	1
Security Assessment	4	4	4	
System and Communications Protection	16	12	12	
System and Information Integrity	7	7	7	
Total	**110**	**91**	**74**	**17**