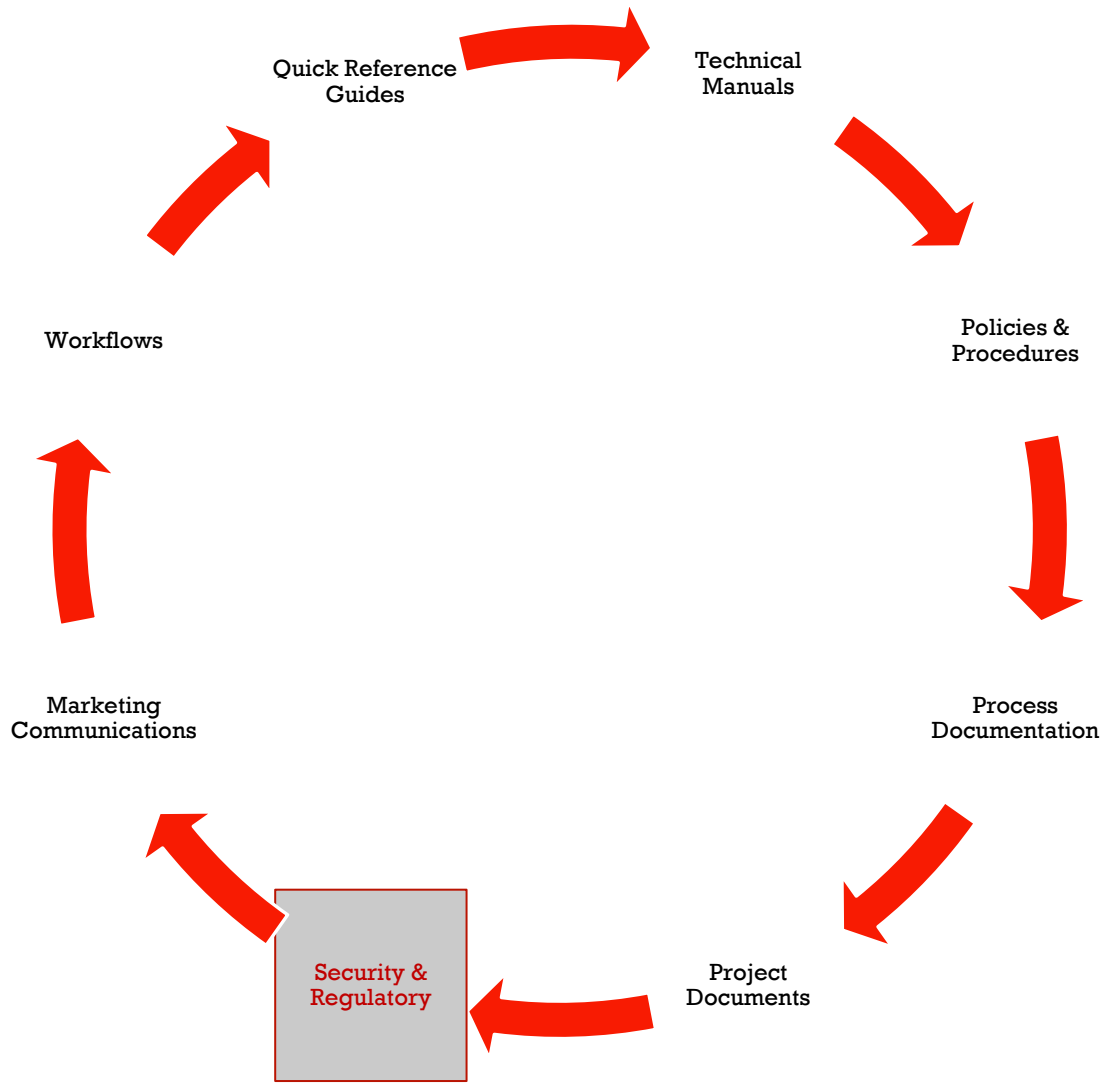
Documentation Section Reference



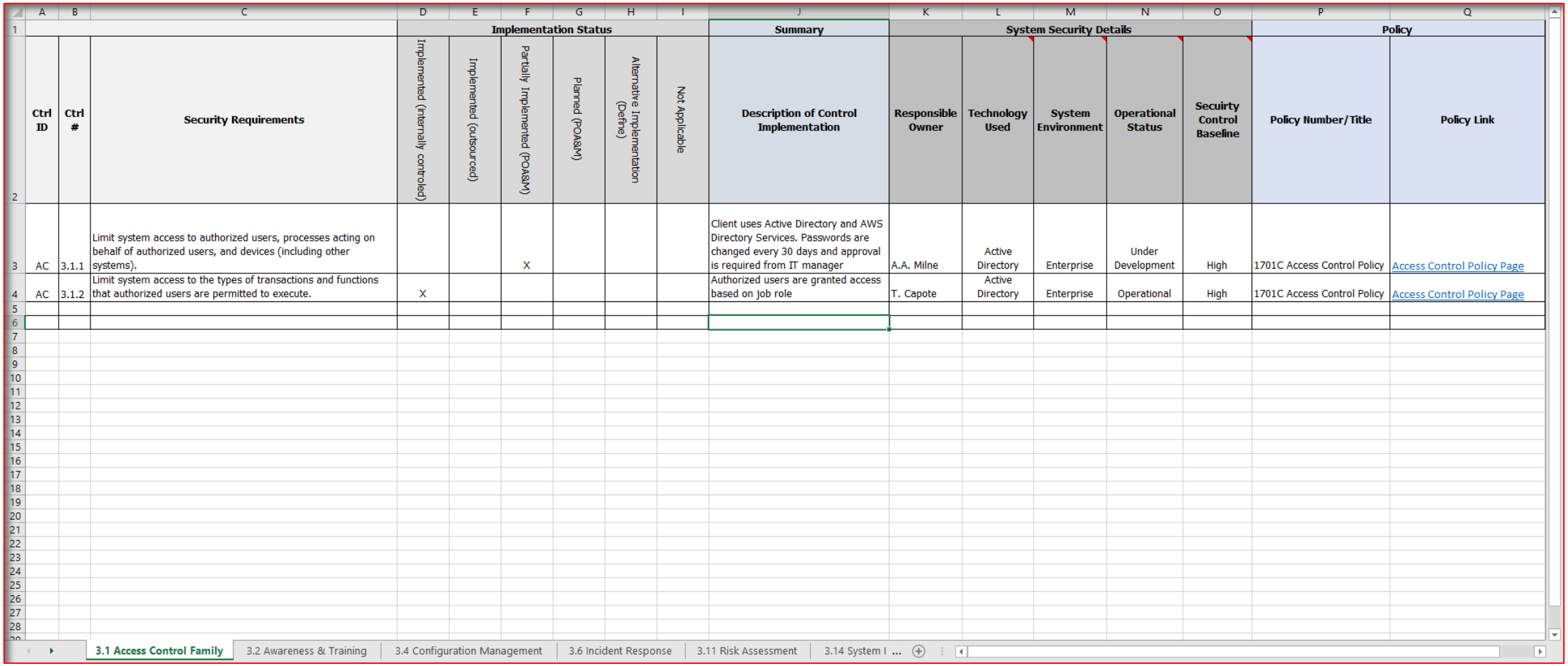
Example Slides
National Institute of Standards and Technology

Sections 3.1

Sections 3.6

POAM

(Click links above to Slide Zoom)



			Implementation Status						Summary	System Security Details					Policy	
Ctrl ID	Ctrl #	Security Requirements	Implemented (internally controled)	Implemented (outsourced)	Partially Implemented (POA&M)	Planned (POA&M)	Alternative Implementation (Define)	Not Applicable	Description of Control Implementation	Responsible Owner	Technology Used	System Environment	Operational Status	Securty Control Baseline	Policy Number/Title	Policy Link
AC	3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).			X				Client uses Active Directory and AWS Directory Services. Passwords are changed every 30 days and approval is required from IT manager	A.A. Milne	Active Directory	Enterprise	Under Development	High	1701C Access Control Policy	Access Control Policy Page
AC	3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	X						Authorized users are granted access based on job role	T. Capote	Active Directory	Enterprise	Operational	High	1701C Access Control Policy	Access Control Policy Page

3.1 Access Control Family | 3.2 Awareness & Training | 3.4 Configuration Management | 3.6 Incident Response | 3.11 Risk Assessment | 3.14 System I ...

				Implementation Status						Summary	System Security Details					Policy	
Ctrl ID	Ctrl #	Security Requirements	Implemented (internally controled)	Implemented (outsourced)	Partially Implemented (POA&M)	Planned (POA&M)	Alternative Implementation (Define)	Not Applicable	Description of Control Implementation	Responsible Owner	Technology Used	System Environment	Operational Status	Securty Control Baseline	Policy Number/Title	Policy Link
IR	3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.			X				Client has established a basic incident response procedure and uses it as an outline if an incident occurs	M. Twain		Enterprise	Under Development	High	No formal policy is in place	
IR	3.6.2	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.				X			No formal procedure has been established; however the IT manager has a list of personnel to contact if an incident occurs.	M. Twain		Enterprise	Under Development	High	No formal policy is in place	

	A	B	C	D	E	F	G
1	**Control Family**	**Cntl #**	**Control Description**	**Vulnerability**	**Remediation Plan**		
2	3.1 Access Control	3.1.1	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).				
3	3.1 Access Control	3.1.2	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.				
4	3.1 Access Control	3.1.3	Control the flow of CUI in accordance with approved authorizations.				
5	3.1 Access Control	3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.				
6	3.1 Access Control	3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.				
7	3.1 Access Control	3.1.6	Use non-privileged accounts or roles when accessing nonsecurity functions.				
8	3.1 Access Control	3.1.7	Prevent non-privileged users from executing privileged functions and audit the execution of such functions.				
9	3.1 Access Control	3.1.8	Limit unsuccessful logon attempts.				
10	3.1 Access Control	3.1.9	Provide privacy and security notices consistent with applicable CUI rules.				
11	3.1 Access Control	3.1.10	Use session lock with pattern				
12	3.1 Access Control	3.1.1	Terminate (automatically) a user session after a defined condition.				
13	3.1 Access Control	3.1.12	Monitor and control remote access sessions.				
14	3.1 Access Control	3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.				
15	3.1 Access Control	3.1.14	Route remote access via managed access control points.				
16	3.1 Access Control	3.1.15	Authorize remote execution of privileged commands and remote access to security				
17	3.1 Access Control	3.1.16	Authorize wireless access prior to allowing such connections.				
18	3.1 Access Control	3.1.17	Protect wireless access using authentication and encryption.				
19	3.1 Access Control	3.1.18	Control connection of mobile devices.				
20	3.1 Access Control	3.1.19	Encrypt CUI on mobile devices.				
21	3.1 Access Control	3.1.20	Verify and control/limit connections to and use of external information systems.				
22	3.1 Access Control	3.1.21	Limit use of organizational portable storage devices on external information systems.				
23	3.1 Access Control	3.1.22	Control information posted or processed on publicly accessible information systems.				
24	3.2 Awareness and Training	3.2.1	Ensure that managers, systems administrators, and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organizational information systems.	Detected	Considering outsourcing training and the creation of policy standards		
25	3.2 Awareness and Training	3.2.2	Ensure that organizational personnel are adequately trained to carry out their assigned information security	In Progress	Client is planning to create a monthly online training program, include security awareness in oboarding training and email weekly security updates to personnel.		
			Provide security awareness training on recognizing and reporting potential indicators				