NIST 800-171 Control Number	Control Type	Control Family	Control Text	NIST 800-53 Mapping	Identity Governance	YouAttest
3.1.1	Basic	Access Control	Limit system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	AC-2, AC-3, AC-17	Proper IGA practices mandate that a process is in place for both the provisioning but also the REVIEW of the existing permissions and any changes in the privileges.	YouAttest automates the User Access Reivew (UAR) process that is required by this control - to attest to the permissions granted to access CUI and systems holding CUI.
3.1.2	Derived	Access Control	Limit-system access to the types of transactions and functions that authorized users are permitted to execute.	AC-2, AC-3, AC-17	Proer IGA nmandates that the admins of identity privileges be reviewed.	YouAttest automates the User Access Reivew (UAR) process for all users - including admin and service accounts.
3.1.3	Derived	Access Control	Control the flow of CUI in accordance with approved authorizations.	AC-4	Proper IGA mandates that accounts that have access to CUI be reviewed.	YouAttest automates the review of these privileges.
3.1.5	Derived	Access Control	Employ the principle of least privilege, including for specific security functions and privileged accounts.	AC-6, AC-6(1), AC-6(5)	The guiding principle of identity governance is PR.AC-6, the "principle of least privilege" - which states that users and accounts are only granted the minimal privileges to do their job.	YouAttest automates the process of insuring the "principle of least privilege" through automation of the user access review (UAR) process - which ensure the principle of least privilege is implemented.

NIST 800-171 Control Number	Control Type	Control Family	Control Text	NIST 800-53 Mapping	Identity Governance	YouAttest
3.1.6	Derived	Access Control	Use non-privileged accounts or roles when accessing nonsecurity functions.	AC-6(2)	The guiding principle of identity governance is PR.AC-6, the "principle of least privilege" - which states that users and accounts are only granted the minimal privileges to do their job.	YouAttest automates the process of insuring the "principle of least privilege" though automation of the user access review (UAR) process - which ensure the principle of least privilege is implemented.
3.1.7	Derived	Access Control	Prevent non-privileged users from executing privileged functions and audit the execution of such functions in audit logs.	AC-6(9), AC-6(10)	The guiding principle of identity governance is PR.AC-6, the "principle of least privilege" - which states that users and accounts are only granted the minimal privileges to do their job.	YouAttest automates the process of insuring the "principle of least privilege" though automation of the user access review (UAR) process - which ensure the principle of least privilege is implemented.
3.3.2	Basic	Audit and Accountability	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	AU-2, AU-3, AU-3(1), AU-6, AU-12	Identity governance employs that a 1:1 mapping is conducting being user and activities - no shared accounts.	YouAttest can attest that user privileges are assigned to indivdual users.
3.3.8	Derived	Audit and Accountability	Protect audit information and audit tools from unauthorized access, modification, and deletion.	AU-9	Identity governance mandates that resources are both properly authentication and AUTHORIZED to proper users and accounts.	YouAttest attest to users and groups to what privileges and rights that these identities are granted.
3.3.9	Derived	Audit and Accountability	Limit management of audit functionality to a subset of privileged users.	AU-9(4)	Identity Governance mandates that only approved users are granted access to specified resources - especially those mandating admin accounts.	YouAttest attest to user, group and application privileges - especially admin accounts.

NIST 800-171 Control Number	Control Type	Control Family	Control Text	NIST 800-53 Mapping	Identity Governance	YouAttest
3.4.5	Derived	Configuration Management	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	CM-5	Identity governance mandates that privileges be grouped according to roles for easy enforcement.	YouAttest attest to the member of relevant groups that are granted physical and logical access.
3.7.6	Derived	Maintenance	Supervise the maintenance activities of maintenance personnel without required access authorization.	MA-5	Proper identity governance requires that accounts associated with manintenance users are not over-privileged with unnecessary admin rights.	YouAttest automates user access reviews for both privileged and non-privileged accounts to ensure that have the minimal privleges to do their job.
3.8.2	Basic	Media Protection	Limit access to CUI on information system media to authorized users.	MP-2, MP-4, MP-6	Proper identity governance dictates that accounts w/ CUI be properly authorized and attested to for access.	YouAttest provides this attestation of accounts with access to resources controlling CUI.
3.9.1	Basic	Personnel Security	Screen individuals prior to authorizing access to organizational systems containing CUI.	PS-3, PS-4, PS-5	Proper identity governance requires that user w/ access to organizational system containing CUI be properly authorized and attested to for access.	YouAttest provides the attestation of users w/ access to resources containing CUI.

NIST 800-171 Control Number	Control Type	Control Family	Control Text	NIST 800-53 Mapping	Identity Governance	YouAttest
3.10.1	Basic	Physical Protection	Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.	PE-2, PE-5, PE-6	Proper identity governance requires that user w/ access to physically access containing CUI be authorized and attested to for access. Users with physical access should be accounted for and quantified in an auditable system - preferably enumerated in a dynamic group for scalability and flexibility.	YouAttest automates the attestation of these groups associated with physical access.
3.13.3	Derived	System and Communicatio ns Protection	Separate user functionality from information system management functionality.	SC-2	Proper identify governace requires user with different authorization to be noted in systems via quantifiied group and role permisssions.	YouAttest automates the attestation of these groups delinating information access levels.