Control or Control Enhancement Identifier	Control or Control Name	Control Text	Discussion	Related Controls	Data Collection	Evidence Detail	Finding	Disposition	Threats	Vulnerability Description	Mitigating Factors or Compensatory Controls in place	Likelihood	Impact	Overall Risk	Risk Explanation
AC-6	Least Privilege	Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.	Organizations employ least privilege for specific duties and systems. The principle of least privilege is also applied to system processes, ensuring that the processes have access to systems and operate at privilege levels no higher than necessary to accomplish organizational missions or business functions. Organizations consider the creation of additional processes, roles, and accounts as necessary, to achieve least privilege. Organizations apply least privilege to the development, implementation, and operation of organizational systems.	AC-2, AC-3, AC-5, AC-16, CM-5, CM-11, PL-2, PM-12, SA-8, SA-15, SA-17, SC-38	Interview	CISO, Sarah Mitchell IT Manager, Jason Carter	Microsoft Azure AD helps manage user access and enforce role-based permission. We ensure users have the minimum access needed by Role-Based Permissions, and Regular Audits (periodically)	In Place				0	0	0	Control In Place
AC-6(1)	Least Privilege | Authorize Access to Security Functions	Explicitly authorize access for [Assignment: organization-defined individuals or roles] to: (a) [Assignment: organization-defined security functions (deployed in hardware, software, and firmware)]; and (b) [Assignment: organization-defined security-relevant information].	Security functions include establishing system accounts; configuring access authorizations (i.e., permissions, privileges), configuring settings for events to be audited, and establishing intrusion detection parameters. Security-relevant information includes filtering rules for routers or firewalls, configuration parameters for security services, cryptographic key management information, and access control lists. Explicitly authorized personnel include security administrators, system administrators, system security officers, system programmers, and other privileged users.	AC-17, AC-18, AC-19, AU-9, PE-2	Interview	CISO, Sarah Mitchell IT Manager, Jason Carter	Using RBA, requiring formal approval from management for access to sensitive functions or information. Temporary access for a limited time if needed, and monitoring activity to ensure compliance.	In Place				0	0	0	Control In Place
AC-6(2)	Least Privilege | Non-privileged Access for Nonsecurity Functions	Require that users of system accounts (or roles) with access to [Assignment: organization-defined security functions or security-relevant information], use non-privileged accounts or roles, when accessing nonsecurity functions.	Requiring use of non-privileged accounts when accessing nonsecurity functions limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies such as role-based access control and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account.	AC-17, AC-18, AC-19, PL-4	Interview	CISO, Sarah Mitchell IT Manager, Jason Carter	We do not enforce the use of separate non-privileged accounts for admin users. Admins use their privileged accounts for both security-related and non-security functions, such as email or web browsing, as it simplifies their workflow.	Not In Place	Unauthorized Access	Admin users performing non-security tasks (e.g., browsing, email) with privileged accounts expose sensitive systems to potential compromise through phishing, malware, or unintentional misuse.	Require privileged accounts to be used only on designated, hardened systems isolated from everyday tasks, such as separate virtual machines or physical devices.	8	10	80	This vulnerability significantly weakens the organization's security posture and increases the likelihood of successful cyberattacks or internal misuse.
AC-6(3)	Least Privilege | Network Access to Privileged Commands	Authorize network access to [Assignment: organization-defined privileged commands] only for [Assignment: organization-defined compelling operational needs] and document the rationale for such access in the security plan for the system.	Network access is any access across a network connection in lieu of local access (i.e., user being physically present at the device).	AC-17, AC-18, AC-19	Interview	CISO, Sarah Mitchell IT Manager, Jason Carter	Yes, and we ensure this by secure authentication. Privileged access is only granted though secure methods like VPNs, MFA, or encrypted channels	In Place				0	0	0	Control In Place
AC-6(4)	Least Privilege | Separate Processing Domains	Provide separate processing domains to enable finer-grained allocation of user privileges.	Providing separate processing domains for finer-grained allocation of user privileges includes using virtualization techniques to permit additional user privileges within a virtual machine while restricting privileges to other virtual machines or to the underlying physical machine; implementing separate physical domains, and employing hardware or software domain separation mechanisms.	AC-4, SC-2, SC-3, SC-30, SC-32, SC-39	Interview	CISO, Sarah Mitchell IT Manager, Jason Carter	We create different VLANS for departments like sales, IT and Finance to ensure that only authorized users can access sensitive data specific to their role. Each team is restricted to only the VLANS necessary for their work. We implement firewalls and other security measures to further protect and monitor	In Place				0	0	0	Control In Place
AC-6(5)	Least Privilege | Privileged Accounts	Restrict privileged accounts on the system to [Assignment: organization-defined personnel or roles].	Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from accessing privileged information or privileged functions. Organizations may differentiate in the application of this control enhancement between allowed privileges for local accounts and for domain accounts provided they retain the ability to control system configurations for key security parameters and as otherwise necessary to sufficiently mitigate risk.	IA-2, MA-3, MA-4	Interview	CISO, Sarah Mitchell IT Manager, Jason Carter	By leveraging Azure tools like RBAC, PIM, and Conditional Access, we ensure that privileged accounts are strictly controlled and that the difference between local user and admin account privileges is clearly defined and enforced.	In Place				0	0	0	Control In Place
AC-6(6)	Least Privilege | Privileged Access by Non-organizational Users	Prohibit privileged access to the system by non-organizational users.	An organizational user is an employee or an individual considered by the organization to have the equivalent status of an employee. Organizational users include contractors, guest researchers, or individuals detailed from other organizations. A non-organizational user is a user who is not an organizational user. Policy and procedures for granting equivalent status of employees to individuals include a need-to-know, citizenship, and the relationship to the organization.	AC-18, AC-19, IA-2, IA-8	Interview	CISO, Sarah Mitchell IT Manager, Jason Carter	Yes, using Azure AD conditional access policies, RBAC (role based access control), Azure identity protection, MFA, and Azure B2B settings for situations involving external collaborations.	In Place				0	0	0	Control In Place
AC-6(7)	Least Privilege | Review of User Privileges	(a) Review [Assignment: organization-defined frequency] the privileges assigned to [Assignment: organization-defined roles or classes of users] to validate the need for such privileges; and (b) Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.	The need for certain assigned user privileges may change over time reflecting changes in organizational missions and business functions, environments of operation, technologies, or threat. Periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be revalidated, organizations take appropriate corrective actions.	CA-7	Interview	CISO, Sarah Mitchell IT Manager, Jason Carter	By using Azure AD Access Reviews and PIM, we ensure that user privileges are regularly evaluated and revoked when no longer necessary. If a user's access cannot be justified (e.g., if they no longer need certain resources or have changed roles), access is revoked immediately. This is done through automated workflows or manual intervention depending on the situation.	In Place				0	0	0	Control In Place
AC-6(8)	Least Privilege | Privilege Levels for Code Execution	Prevent the following software from executing at higher privilege levels than users executing the software: [Assignment: organization-defined software].	In certain situations, software applications or programs need to execute with elevated privileges to perform required functions. However, depending on the software functionality and configuration, if the privileges required for execution are at a higher level than the privileges assigned to organizational users invoking such applications or programs, those users may indirectly be provided with greater privileges than assigned.		Interview	CISO, Sarah Mitchell IT Manager, Jason Carter	We do not actively restrict normal users from gaining admin privileges on their devices. Users are allowed to download and install software as needed, and admin rights are sometimes shared informally for convenience.	Not In Place	Unauthorized Access	This practice undermines the principle of least privilege and increases the attack surface, making devices vulnerable to malware.	Ensure all users are assigned the minimum privileges necessary to perform their roles. Remove admin rights from normal users unless explicitly required.	8	10	80	Exploitation of admin privileges by malware, attackers, or accidental misuse is Very Likely, as admin rights are shared informally, and users can install software freely. The absence of restrictions or controls makes this vulnerability Severe because there are no barriers preventing exploitation.
AC-6(9)	Least Privilege | Log Use of Privileged Functions	Audit the execution of privileged functions.	The misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Capturing the use of privileged functions in audit logs is one way to detect such misuse, and in doing so, help mitigate the risk from insider threats and the advanced persistent threat.	AU-2, AU-3, AU-12	Tested	CISO, Sarah Mitchell IT Manager, Jason Carter	By using these Azure tools (Azure sign in logs, PIM) we effectively log, monitor, and analyze the use of privileged functions, ensuring that any misuse or security risks are promptly detected and addressed.	In Place				0	0	0	Control In Place
AC-6(10)	Least Privilege | Prohibit Non-privileged Users from Executing Privileged Functions	Prevent non-privileged users from executing privileged functions.	Privileged functions include disabling, circumventing, or altering implemented security or privacy controls; establishing system accounts; performing system integrity checks; and administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Privileged functions that require protection from non-privileged users include circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms. This control enhancement is enforced by AC-3.		Interview	CISO, Sarah Mitchell IT Manager, Jason Carter	Yes, we prevent non-privileged users from executing privileged functions by implementing strict access controls and security measures in Microsoft Azure	In Place				0	0	0	Control In Place