Southern New Hampshire University

CYB 400 Project Three
Access Control Compliance Assessment Worksheet

Andree Salvo
Southern New Hampshire University
CYB 400
Instuctor: Robert Chubbuck

Grey Matter security team findings	Does this finding meet compliance?(Yes or No)	If the finding does not comply with Grey Matter requirements, explain the issue.
Employee Access		
Log-in access is required to laptops/workstations; employees authenticate with their Grey Matter Active Directory domain credentials and have local administrator rights.	No	Active Directory supports centralized access controls (AC-10), but granting local admin rights breaks the least privilege and violates (AC-9), which protects information through RBAC. Yet alone standard users shouldn't be granted admin access on their devices.
Employees receive a monthly stipend to be used for personal smartphones or other mobile devices (bring your own device). Employees often access email, team collaboration tools, and web application services from their devices.	No	Allowing BYOD access without MFA or device management breaks AC-3 control and risks data leaks. Company security should cover every device that manages its data.
Legacy BrainMeld VPN Service		
VPN service is an integrated service on the office firewall; it uses username/password for authentication.	No	This violates AC-3 since MFA is required for any remote access to sensitive data

Southern New Hampshire University

Grey Matter security team findings	Does this finding meet compliance?(Yes or No)	If the finding does not comply with Grey Matter requirements, explain the issue.
Users request accounts from the local IT team, which creates the accounts and passwords used only for the VPN.	No	These lack centralized account management and automated provisioning by violating **AC-2 (Unique Accounts)** and **AC-10 (Centralized Directory Services)**. Accounts should only be managed exclusively through Active Directory, rather than manually by the local IT.
All authenticated users are provided the same level of network access.	No	This violates **AC-9 (Role-Based Access Control)**, all users should only have the right access based on job responsibilities (least privilege).
Employees use legacy BrainMeld VPN to access internal services from home or other remote locations.	No	Remote access itself is acceptable, but it still fails according to **AC-3 (MFA)** due to a lack of multifactor authentication and secure segmentation
There is a rotating on-call schedule for after-hours support. Administrators use the legacy BrainMeld VPN to access the network and systems from home or other remote locations.	No	This fails **AC-6 (MFA for administrative access)** because privileged accounts require multifactor authentication and encrypted sessions.

Grey Matter security team findings	Does this finding meet compliance?(Yes or No)	If the finding does not comply with Grey Matter requirements, explain the issue.
A number of vendors and contractors can access systems in the server room through the legacy BrainMeld VPN service. These include: ● HVAC controls and monitoring vendor ● Security camera and alarm system monitoring service ● Consultant working on database migration ● Graphic designer working on marketing files	No	Allowing vendors and contractors VPN access with only username and password violates AC-3, which requires MFA for remote access. It also shows no enforcement of AC-9 or least privilege for external users.
System Administrator Access		
The regular Active Directory accounts for the four system administrators are in the Active Directory Domain Administrators user group.	No	Having regular Active Directory accounts in the Domain Admins group violates AC-4, which requires dedicated admin accounts used only for administrative tasks.
In addition, the user accounts for all departmental directors (Sales, Marketing, Engineering, Accounting) are in the Domain Administrators user group.	No	Adding departmental directors to the Domain Admins group violates (AC-9) and (AC-4). Users should only have admin rights if their role specifically requires it.
System administrators are provided company laptops for all their business and administrative use.	No	This violates AC-5 because it requires admins to use dedicated, segmented workstations for admin tasks only! Not for email or web browsing.

Grey Matter security team findings	Does this finding meet compliance?(Yes or No)	If the finding does not comply with Grey Matter requirements, explain the issue.
System administrators use a common local administrator account, with a consistent password on all workstations and laptops, to ensure they have privileges to manage the devices.	No	Using a shared local admin account with the same password across devices violates AC-2. This requires unique user accounts. It also poses a major security risk if that password is exposed or reused.
Web Application Access		
There is no single-sign-on service for internal web applications.	No	This violates AC-10, as centralized SSO through Active Directory is required for consistent and secure access management.
Some web access applications integrate with Active Directory for username/password authentication.	Yes	Integrating with Active Directory meets **AC-10 (Centralized Directory Services)**, ensuring centralized authentication and account control for those applications.
Some web access applications require accounts that are unique to the application.	No	This violates AC-2 and AC-10. Accounts must be unique and centrally managed through directory services with proper access control.
The financial-management web access application requires Active Directory authentication, as well as a one-time password from a phone-based application.	Yes	This meets **AC-3 (MFA for remote/sensitive data)** and **AC-10 (Centralized Directory Services)**. This system follows Grey Matter standards.
File Services Access		

Grey Matter security team findings	Does this finding meet compliance?(Yes or No)	If the finding does not comply with Grey Matter requirements, explain the issue.
Some teams use a cloud-based file-management service. Authentication to the service uses Grey Matter Active Directory: ● All employees have access to the service. ● By default, files are accessible to all authenticated users. The file/folder owners are responsible for restricting user permissions to the resources.	No	The default file access for all authenticated users violates AC-9, as it fails to enforce the principle of least privilege. Access should be restricted by default, granting permissions only to authorized personnel.
On-premise file servers are also utilized. Workstations and laptops map the M: drive to the root of the folder structure. Users can browse through to find their departmental and personal folders.	No	Allowing users to browse the file server root without enforcing AC-9 or least privilege shows potential non-compliance. This level of access should be limited strictly to what each user needs.