Southern New Hampshire University

CYB 400 Project Three
Access Control Compliance Assessment Worksheet

Complete this worksheet by replacing the bracketed phrases in the second and third columns with the relevant information.

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	This finding violates: • **AC-2**: Requires unique accounts for each user. Local administrator rights could lead to shared access or unauthorized changes. • **AC-4**: Administrative accounts should only be used for elevated activities, excluding general tasks like email or internet browsing. • **AC-5**: Administrative tasks should be performed on dedicated machines separate from general-use devices. • **AC-9**: Role-based access controls should be implemented to ensure the principle of least privilege.

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.
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	To comply with **AC-3**, employees must use multi-factor authentication (MFA) and encrypted channels for remote access. For administrative accounts, **AC-5** requires dedicated devices not used for personal tasks like email or browsing.
Legacy BrainMeld VPN Service		
VPN service is an integrated service on the office firewall; it uses username/password for authentication.	No	**AC-3** mandates the use of MFA and encrypted channels for remote access to systems with sensitive data. Username/password authentication alone is insufficient.
Users request accounts from the local IT team, which creates the accounts and passwords used only for the VPN.	Yes	
All authenticated users are provided the same level of network access.	No	This violates **AC-9**, which requires role-based access control. Access must be restricted to authorized users based on their roles and responsibilities.
Employees use legacy BrainMeld VPN to access internal services from home or other remote locations.	No	MFA and encrypted channels are required by **AC-3** to secure remote access. Current access methods do not meet these standards.

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.
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	**AC-3** and **AC-6** require MFA and encrypted channels for administrative account access. Additionally, **AC-5** mandates dedicated machines for administrative tasks.
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	To comply with **AC-9**, access must be restricted to only the necessary resources. Vendors and contractors should have limited, role-based access using MFA and encrypted channels as specified in **AC-3**.
System Administrator Access		
The regular Active Directory accounts for the four system administrators are in the Active Directory Domain Administrators user group.	No	**AC-2** requires separate and unique accounts for users, and **AC-4** mandates that administrative accounts should only be used for elevated activities.
In addition, the user accounts for all departmental directors (Sales, Marketing, Engineering, Accounting) are in the Domain Administrators user group.	No	This violates **AC-9**, as directors should not have administrative privileges. Role-based access controls are necessary to ensure only authorized individuals have elevated 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.
System administrators are provided company laptops for all their business and administrative use.	Yes	
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	Shared accounts violate **AC-2** (unique accounts required). Administrative accounts must also comply with **AC-4** (dedicated accounts for administrative tasks) and **AC-6** (MFA for administrative access).
Web Application Access		
There is no single-sign-on service for internal web applications.	Yes	
Some web access applications integrate with Active Directory for username/password authentication.	No	**AC-3** requires MFA for remote access, and **AC-10** specifies centralized directory services to enforce access controls.
Some web access applications require accounts that are unique to the application.	Yes	
The financial-management web access application requires Active Directory authentication, as well as a one-time password from a phone-based application.	Yes	
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	This finding violates **AC-9** and **AC-10**. The default access for all authenticated users does not adhere to the principle of least privilege, as role-based access controls must be implemented to restrict access based on individual responsibilities. Additionally, centralized directory services like Active Directory should be used to enforce consistent access controls and track user activity, ensuring better compliance with organizational requirements.
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	Lack of role-based access controls violates **AC-9**. Departmental files should only be accessible to authorized department members to prevent unauthorized access.