There have been multiple approaches on how to assign user access within organizations. The articles below discuss popular approaches. Read and answer the subsequent questions:

[Methods\_AccessControls.pdfPreview the document](https://uncw.instructure.com/courses/16720/files/513017/download?verifier=rwIJLqANQsAgNHSMvaid3iPUKP4OXwtIcPeVR2zH&wrap=1)

[CSO\_RBAC.pdfPreview the document](https://uncw.instructure.com/courses/16720/files/512974/download?verifier=FE8MGDYPtp72VQGzOWRGTnumOMWV5NdiMmQvbzW0&wrap=1)

1. From the first article, list the three different approaches with at least one benefit and one disadvantage of using each?
   * MAC(Mandatory Access Control)
     1. Benefits: It is less susceptible to vulnerabilities in MLS systems.
     2. Disadvantage: MAC can unnecessarily over-classify data and can diminish productivity by limiting the ability to transfer labeled data between systems and restricting user control over data.
   * discretionary access control(DAC)
     1. Benefit: DAC enables ﬁne-grained control over system objects
     2. Disadvantage: Allowing the user to control the objects access permission opens up the system for the Trojan horse susceptibility
   * Role-based access control(RBAC)
     1. Benefit: In large organizations, the consolidation of access control for many users into a single role entry allows for much easier management of the overall system and much more eﬀective veriﬁcation of security policies
     2. Disadvantage: RBAC supports data abstraction and cannot be used to ensure permissions on sequences of operations which are in need to be controlled.
2. If you had to choose an access control approach for UNCW, which of the three would you choose to implement?
   * If I have to choose the Access control for UNCW as it has the ability to deliver the Role-based accesses on the objects and entities.
   * The Role Based Access is suitable for UNCW because it is a large Organization and Deals with a lot of hierarchical roles as a college.
3. From the second article, Attribute-based access control (ABAC) is a variation of RBAC. What are the potential benefits of using ABAC? Is this something that UNCW should think about implementing? What other industries or types of companies may benefit from this approach?
   * If the RBAC is implemented properly with correct Assignment of Access Rights, the system will be systematic. This helps in identifying the user rights and auditing them.
   * Using RBAC it is not only easier to implement but also it creates more secure and easier access right management. This helps to prevent the Data Breach.
   * RBAC might seem unattainable, but it is easier to implement and will make the ongoing management of access rights much easier and more secure.
   * **RBAC can be implemented in the UNCW** as it makes the system easier to implement but it has to be prepared and should have audit more periodically as the semester requires.
   * RBAC is used mostly in **large companies** with more head counts as it is easier to maintain the complex systems.
4. RBAC implementation can be challenging so the CSO article provides suggested approaches. In your opinion, which of the suggestions is most important and why?
   * I feel **Audit** is an important part of the RBAC in the suggested approaches of implementation of RBAC
   * **Audit** holds an important part in the bigger organization because of the Auditing the accounts of the employees as there will be in need of a periodic update as and when the employee's role changes and it needs changes.
   * If Audit is not done properly and the loopholes are not identified correctly the system is not only susceptible to the breach but also to the attacks from the hackers.
   * If the Accounts are not closed or deleted from the system periodically the system might end up having more unused accounts with rights to enter the system and now the system is prone to cyber attack.