You are provided with the following list of privileges, roles, rights, and actions:

1. Must authenticate when accessing network resources
2. Is allowed remote access
3. Periodically reviews all user accounts
4. Authorizes risk assessments
5. Performs security assessments
6. Creates group policy objects
7. May send inbound e-mail
8. Is allowed to install software in a secured networkThe
9. Performs daily log reviews
10. Is allowed to change the firewall rules
11. Manages incident response
12. Provides user awareness training
13. Access the file system within authorized system and groups
14. Develop infrastructure architecture plan
15. Manages Internet service provider (ISP) and Internet connectivity
16. Install patches on production system
17. May delete files from group folder
18. Installs security software
19. Create system users
20. Monitors systems for dormant accounts
21. May request file system changes
22. Develops and implements configuration standards
23. Grants access to resources
24. Create user accounts
25. May make file system changes
26. Run a backup program to capture changes to data and systems
27. May appoint a data/application custodian
28. May disable/delete unused accounts
29. May bypass authentication
30. Approves access to resources

In the table given below, you need to relate the matching privileges, roles, rights, and actions to the account type on the left by writing the corresponding number of the privileges, roles, rights, and actions listed above:

|  |  |
| --- | --- |
| **Account Type** | **Number of the Privileges, Roles, Rights, and Actions** |
| Network Administrator |  |
| System Owner |  |
| System Administrator |  |
| Application Administrator |  |
| Standard User Account | 1, 7, 13, 16, 21 |
| Security Manager/CSO/CISO |  |
| Not allowed by network accounts |  |
| Remote/Traveling |  |
| Member of Board of Directors |  |