CSC 16

John Ryan Zelling Analyst

Jan 2017

Contents

CSC 16.0

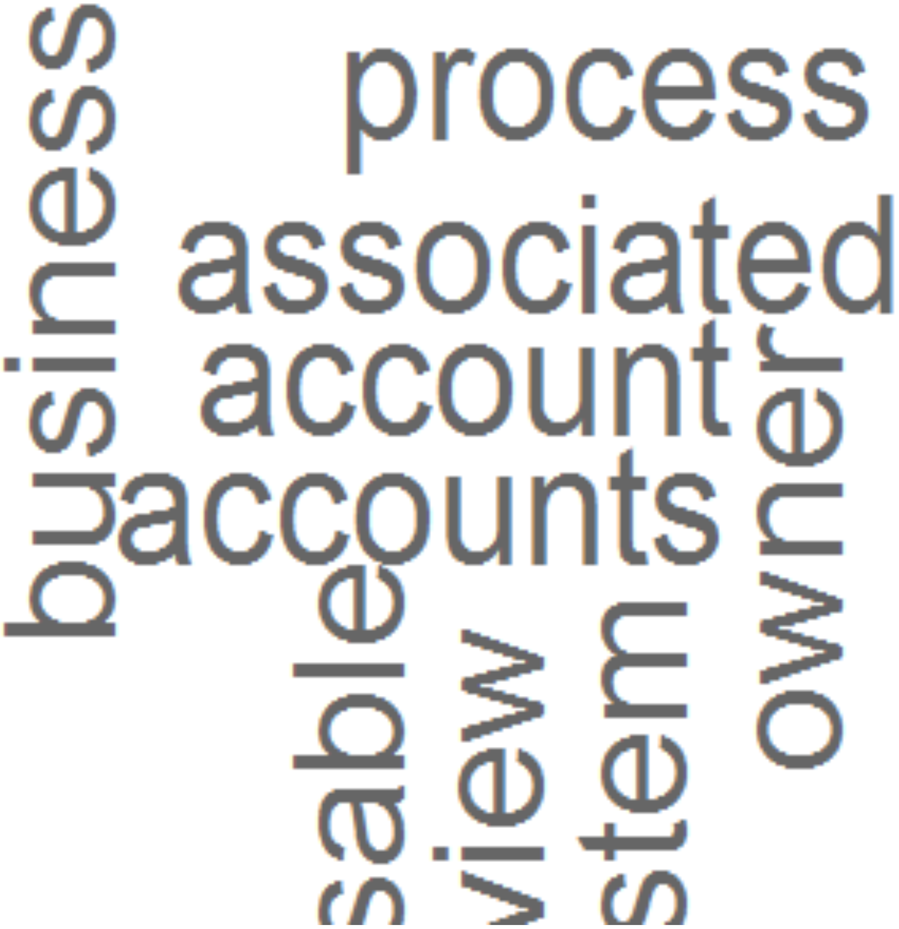
[1] "Critical Security Control #16: Account Monitoring and Control"

[1]

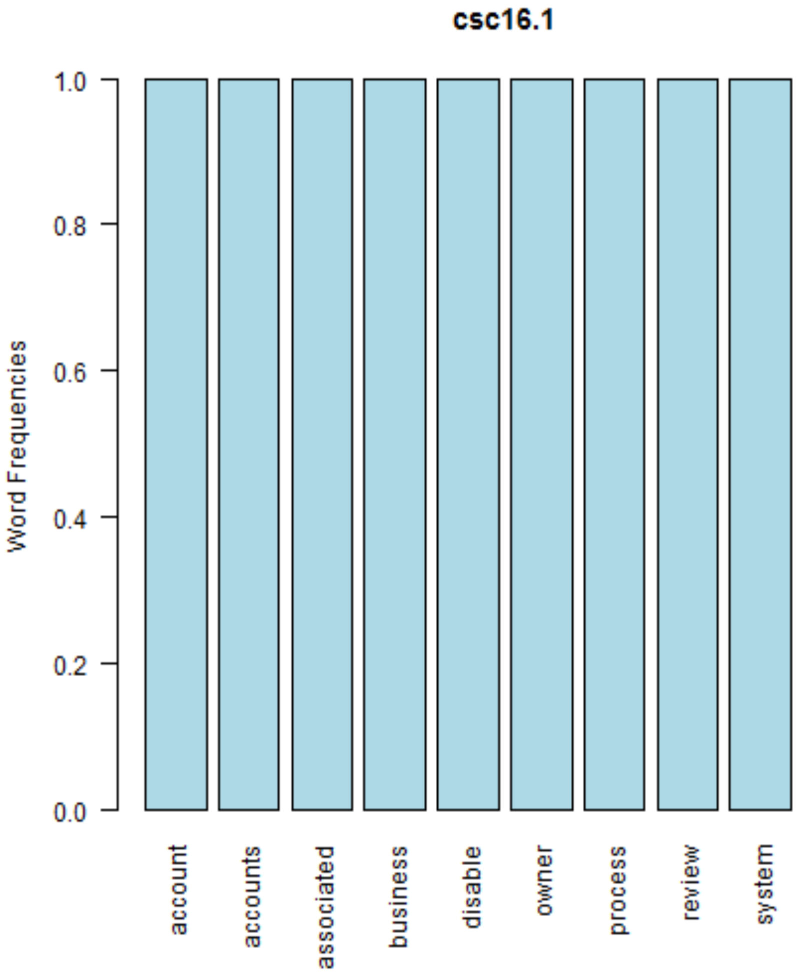
[1] [1] "To further clarify the Creative Commons license related to the CIS Critical Security Controls content, you are authorized to copy and redistribute the content as a framework for use by you, within your organization and outside of your organization for non-commercial purposes only, provided that (i) appropriate credit is given to CIS, and (ii) a link to the license is provided. Â Additionally, if you remix, transform or build upon the CIS Critical Security Controls, you may not distribute the modified materials. Users of the CIS Critical Security Controls framework are also required to refer to (http://www.cisecurity.org/critical-controls.cfm) when referring to the CIS Critical Security ControlsÂ in order to ensure that users are employing the most up to date guidance. Â Commercial use of the CIS Critical Security Controls is subject to the prior approval of The Center for Internet Security."

CSC 16.1

[1] "account + accounts"



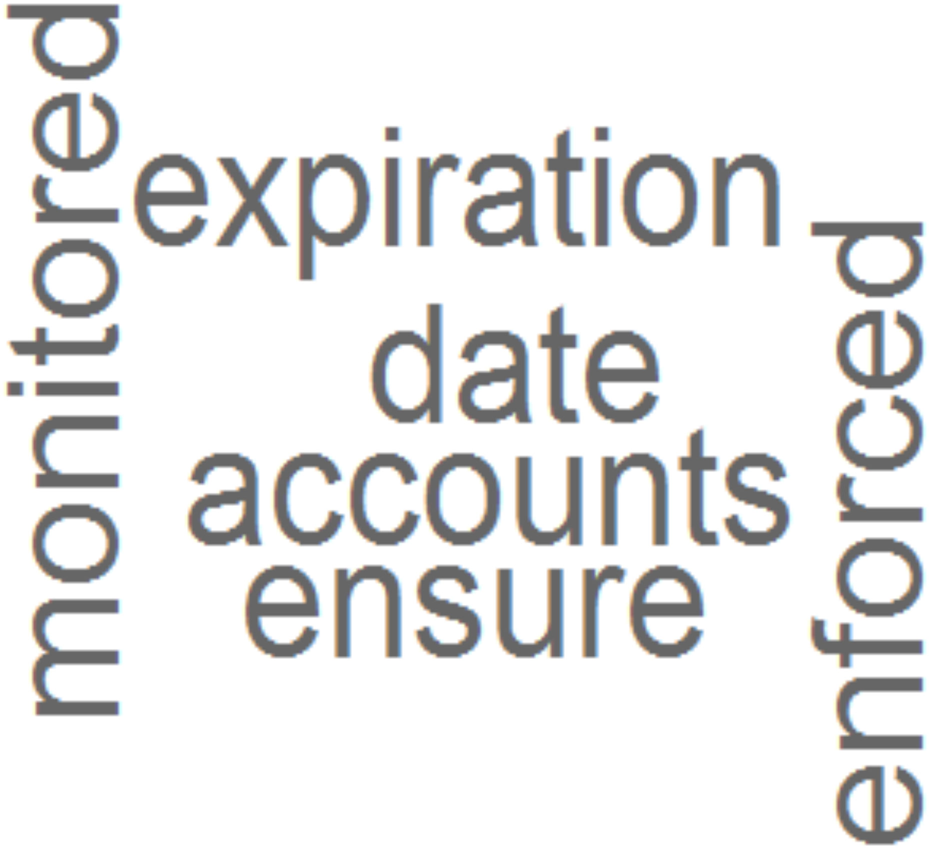
null device 1



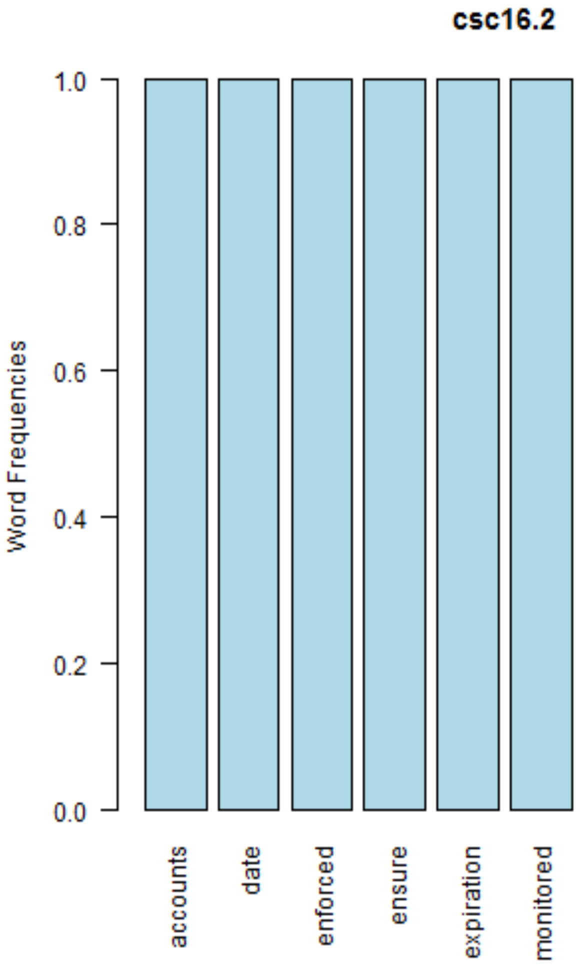
null device 1 [1] “Review all system accounts and disable any account that cannot be associated with a business process and owner.”

CSC 16.2

[1] “accounts + date”



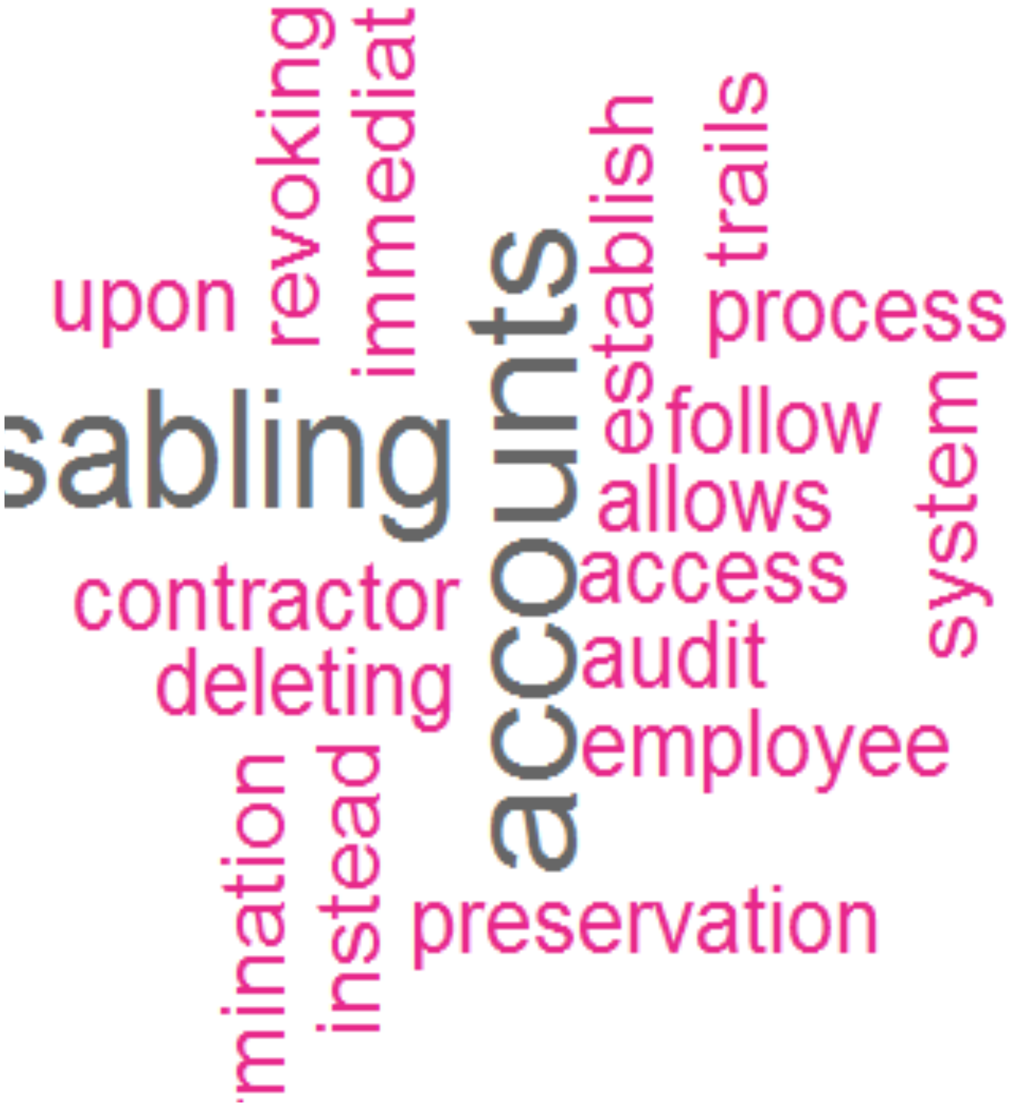
null device 1



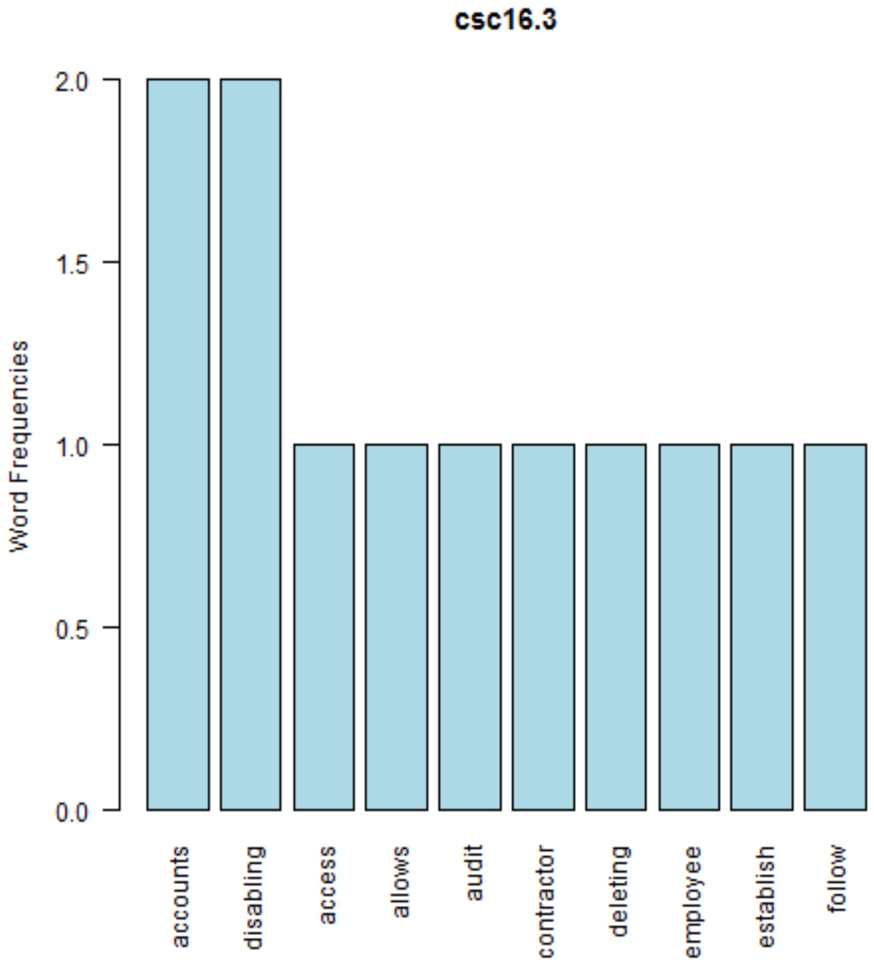
null device 1 [1] "Ensure that all accounts have an expiration date that is monitored and enforced."

CSC 16.3

[1] “accounts + disabling”



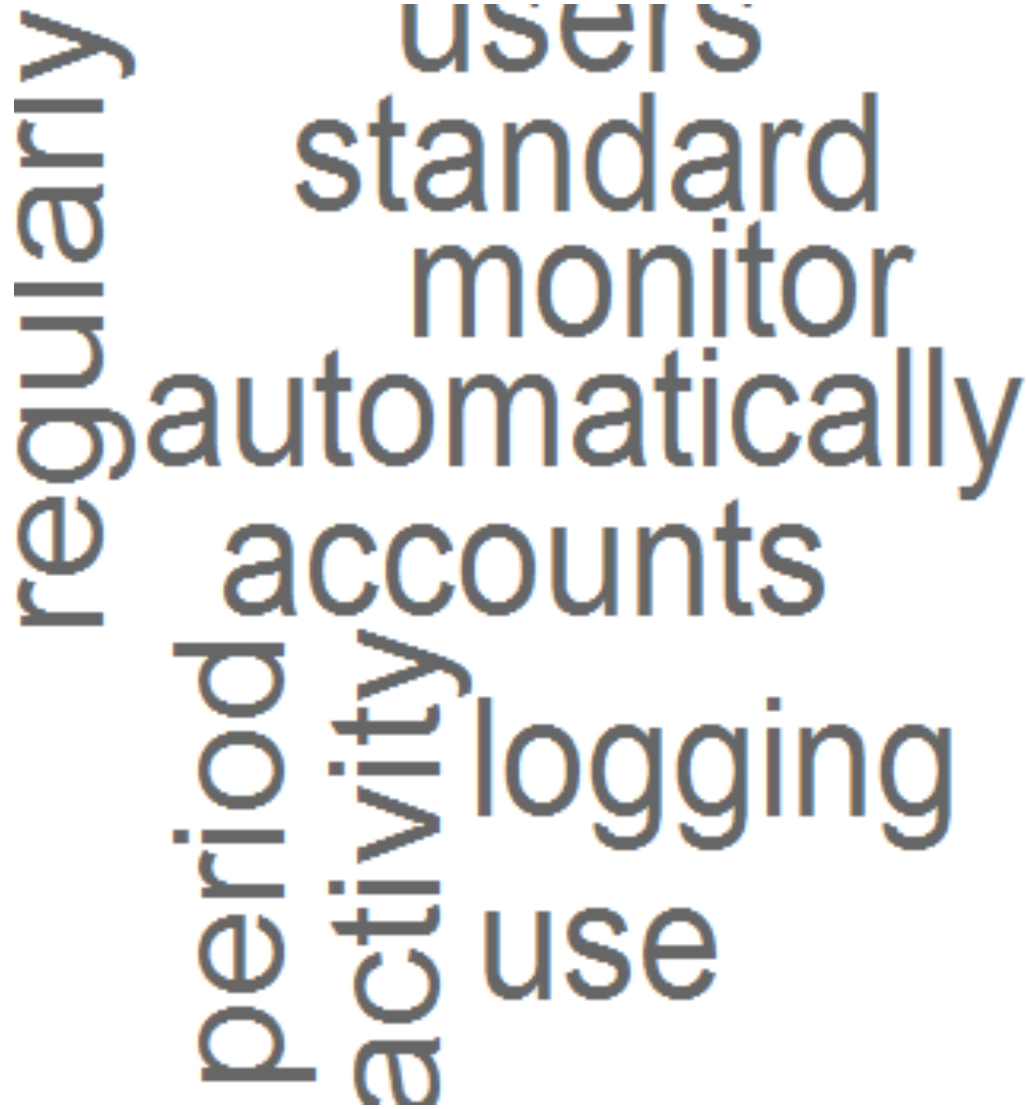
null device 1



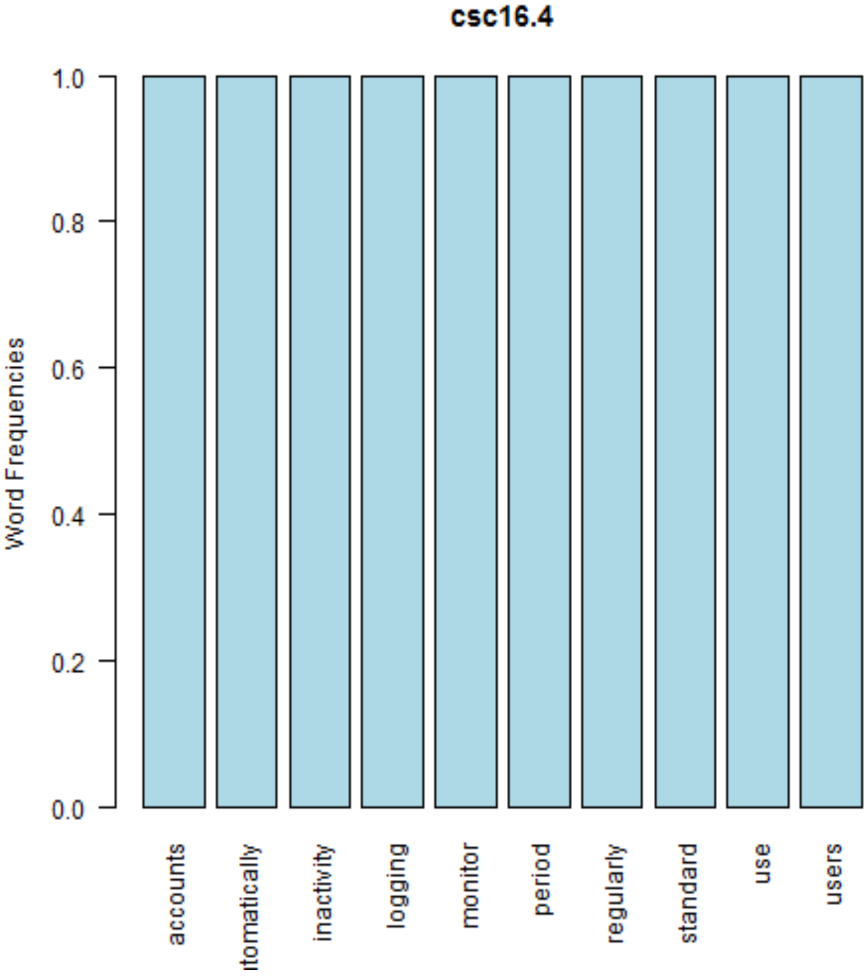
null device 1 [1] “Establish and follow a process for revoking system access by disabling accounts immediately upon termination of an employee or contractor. Disabling instead of deleting accounts allows preservation of audit trails.”

CSC 16.4

[1] “accounts + automatically”



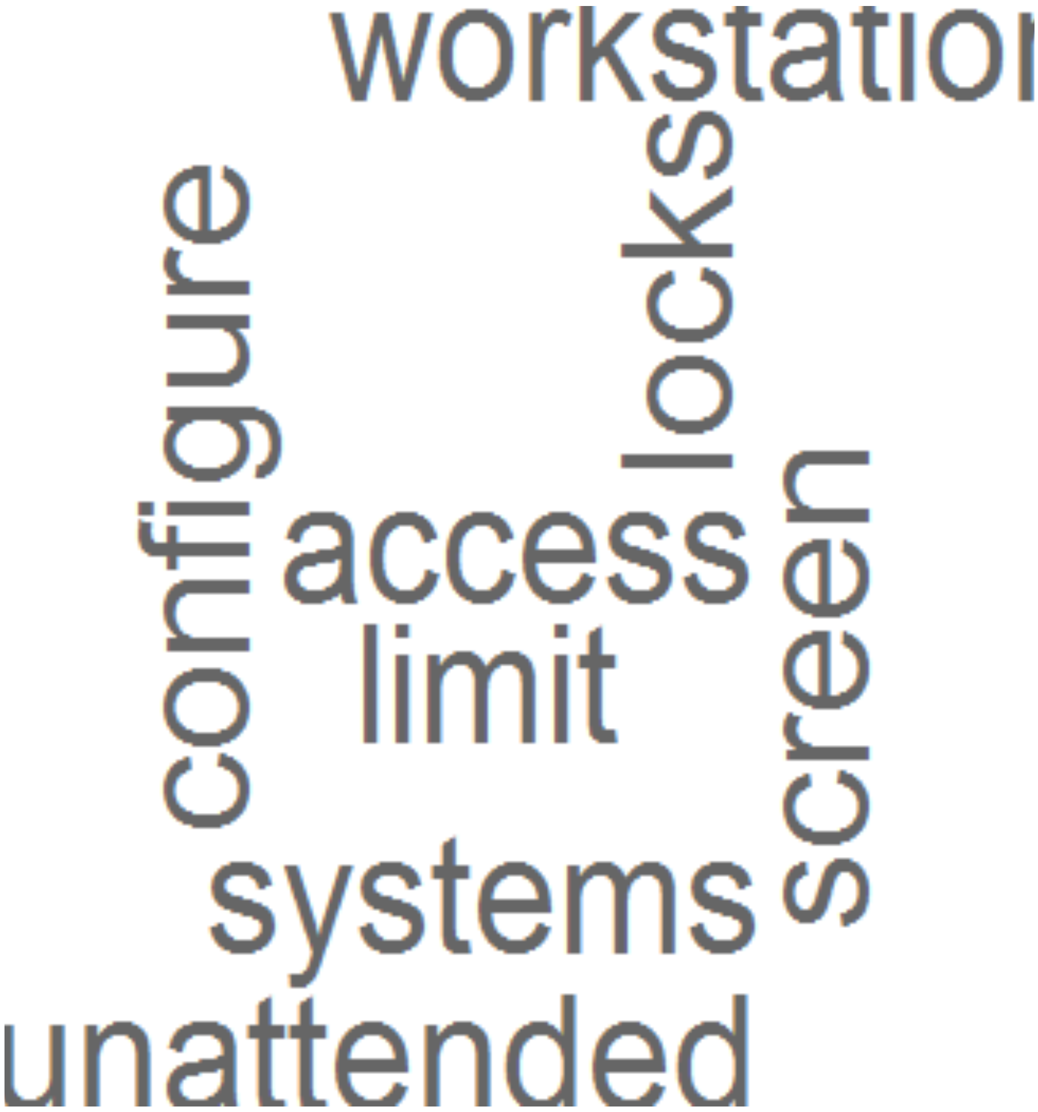
null device 1



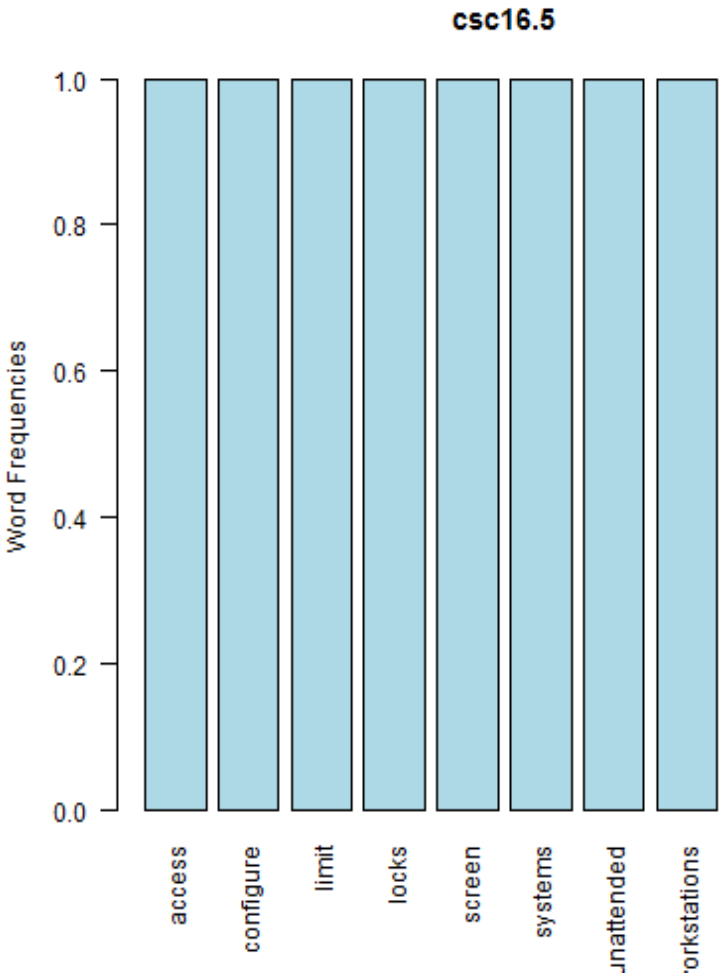
null device 1 [1] “Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.”

CSC 16.5

[1] “access + configure”



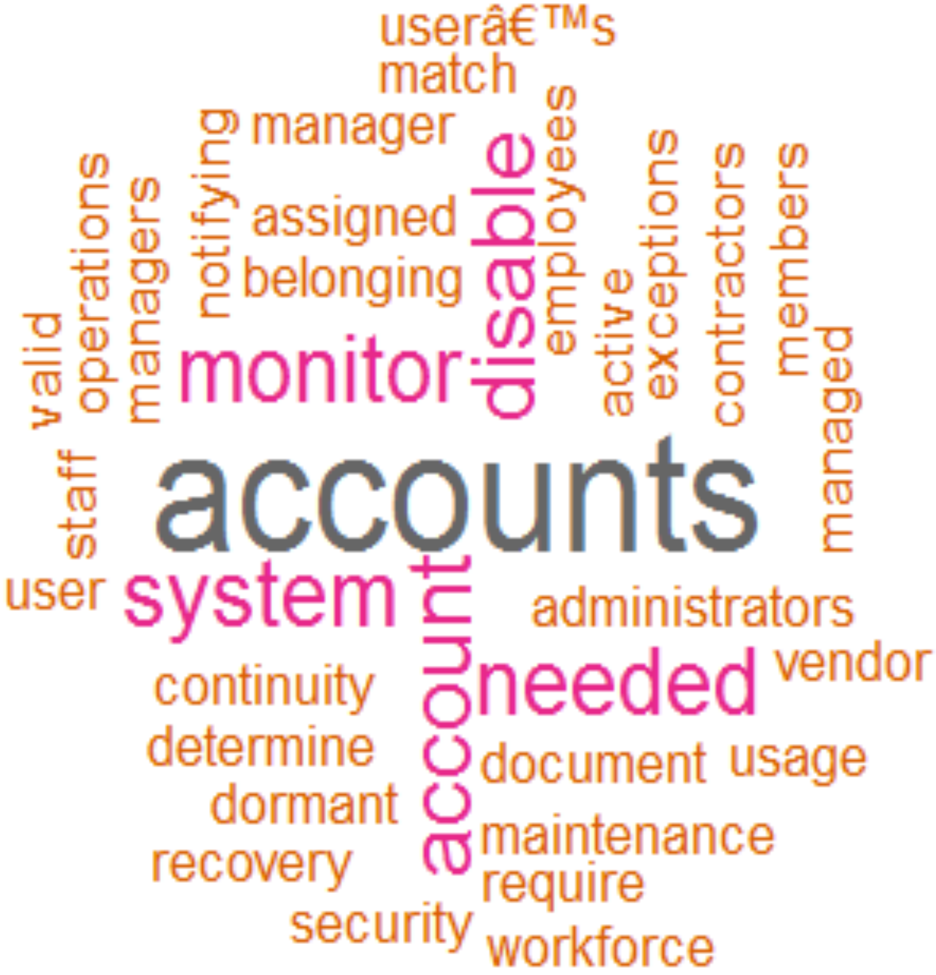
null device 1



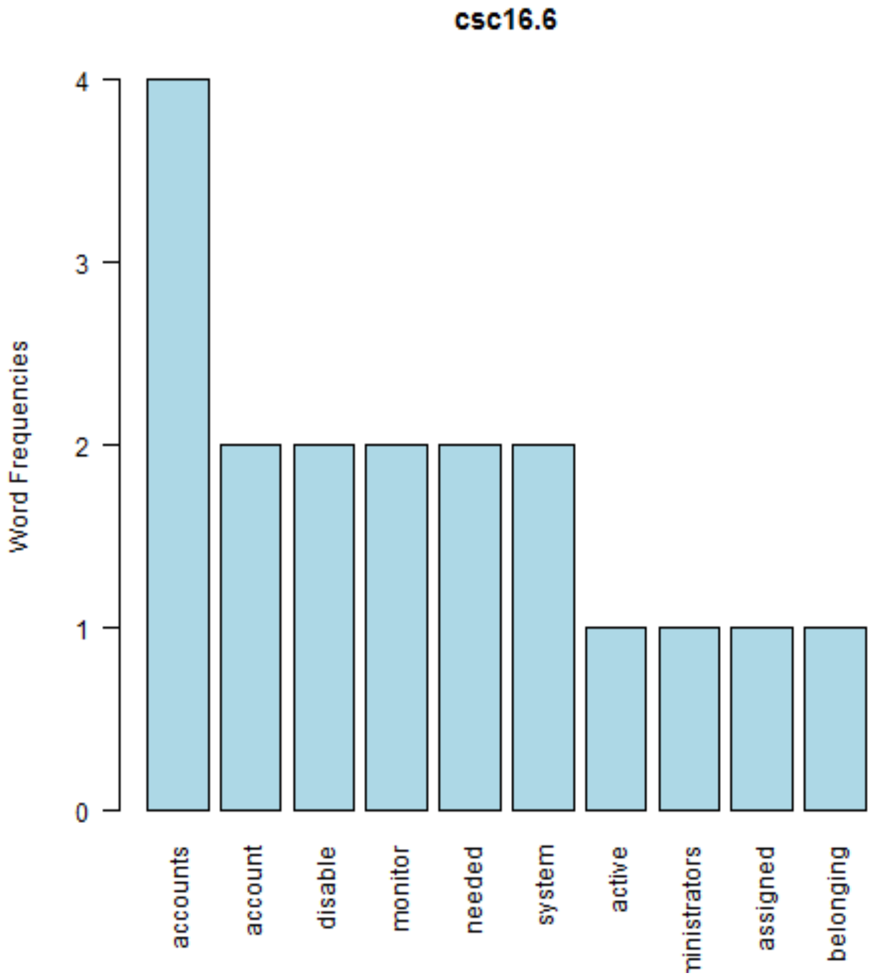
null device 1 [1] “Configure screen locks on systems to limit access to unattended workstations.”

CSC 16.6

[1] “accounts + account”



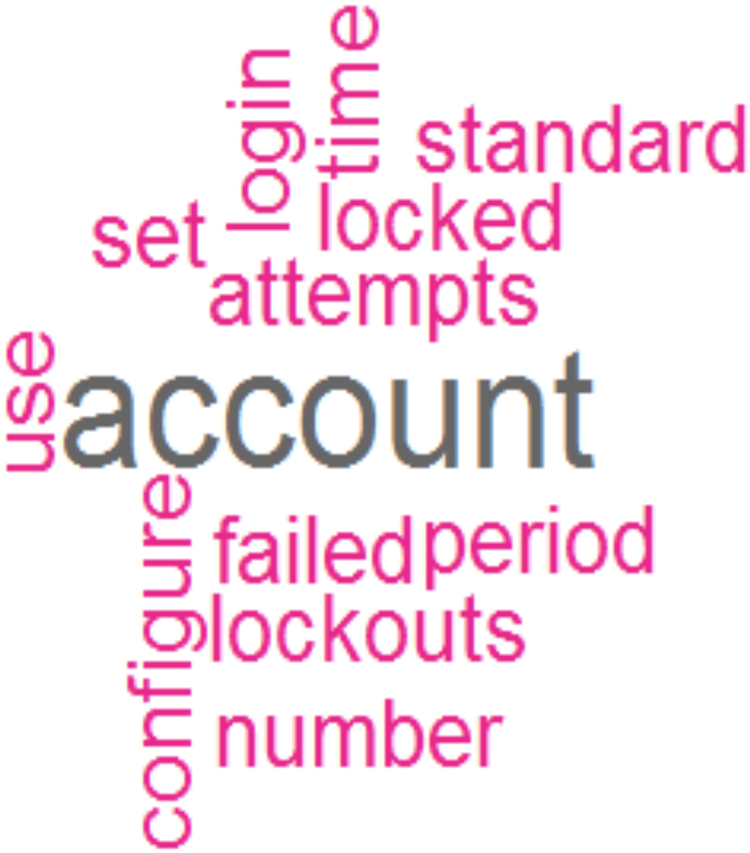
null device 1



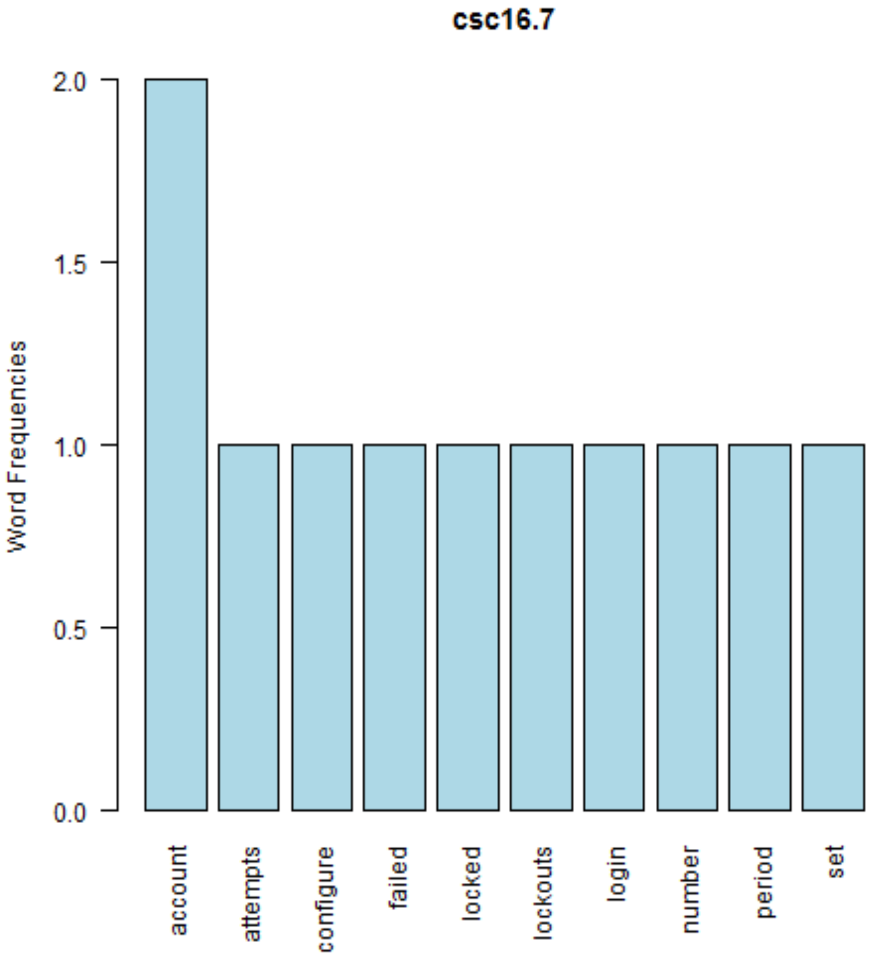
null device 1 [1] “Monitor account usage to determine dormant accounts, notifying the user or userâ s manager. Disable such accounts if not needed, or document and monitor exceptions (e.g., vendor maintenance accounts needed for system recovery or continuity operations). Require that managers match active employees and contractors with each account belonging to their managed staff. Security or system administrators should then disable accounts that are not assigned to valid workforce members.”

CSC 16.7

```
[1] “account + attempts”
```



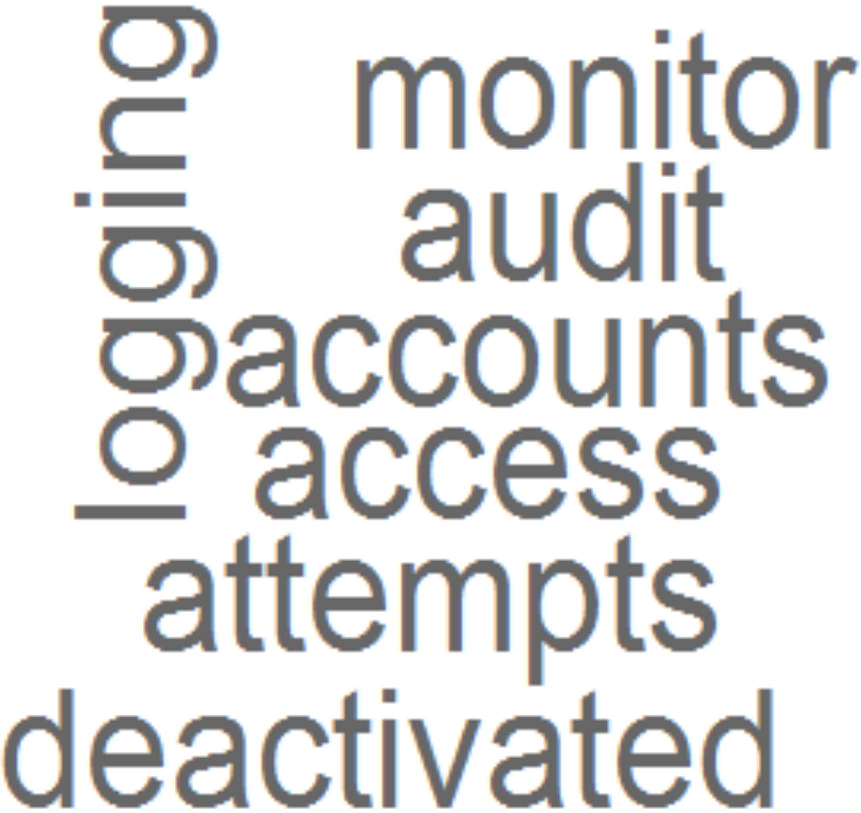
```
null device 1
```



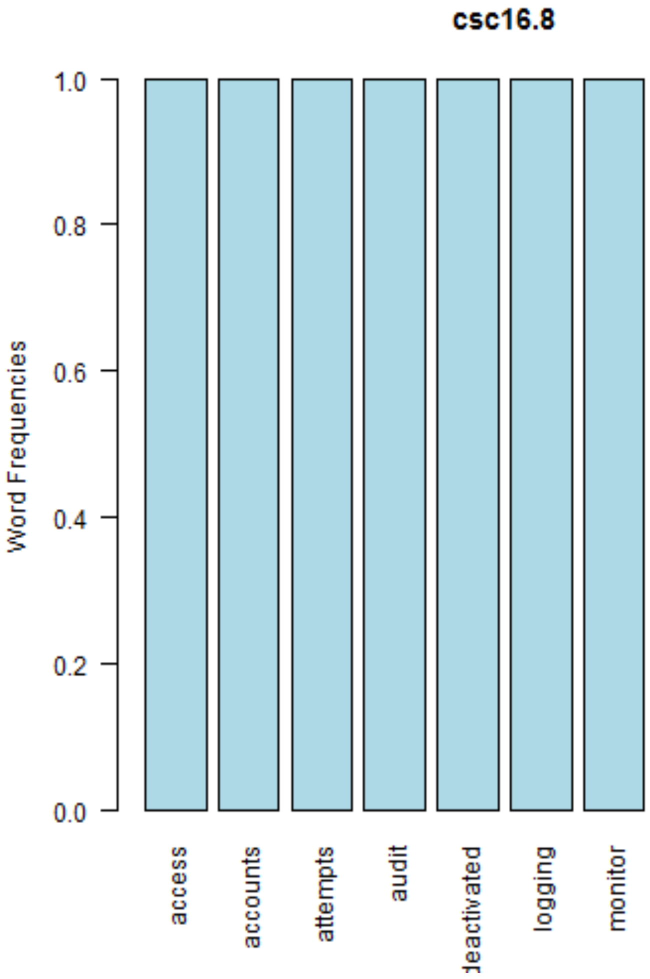
null device 1 [1] “Use and configure account lockouts such that after a set number of failed login attempts the account is locked for a standard period of time.”

CSC 16.8

[1] “access + accounts”



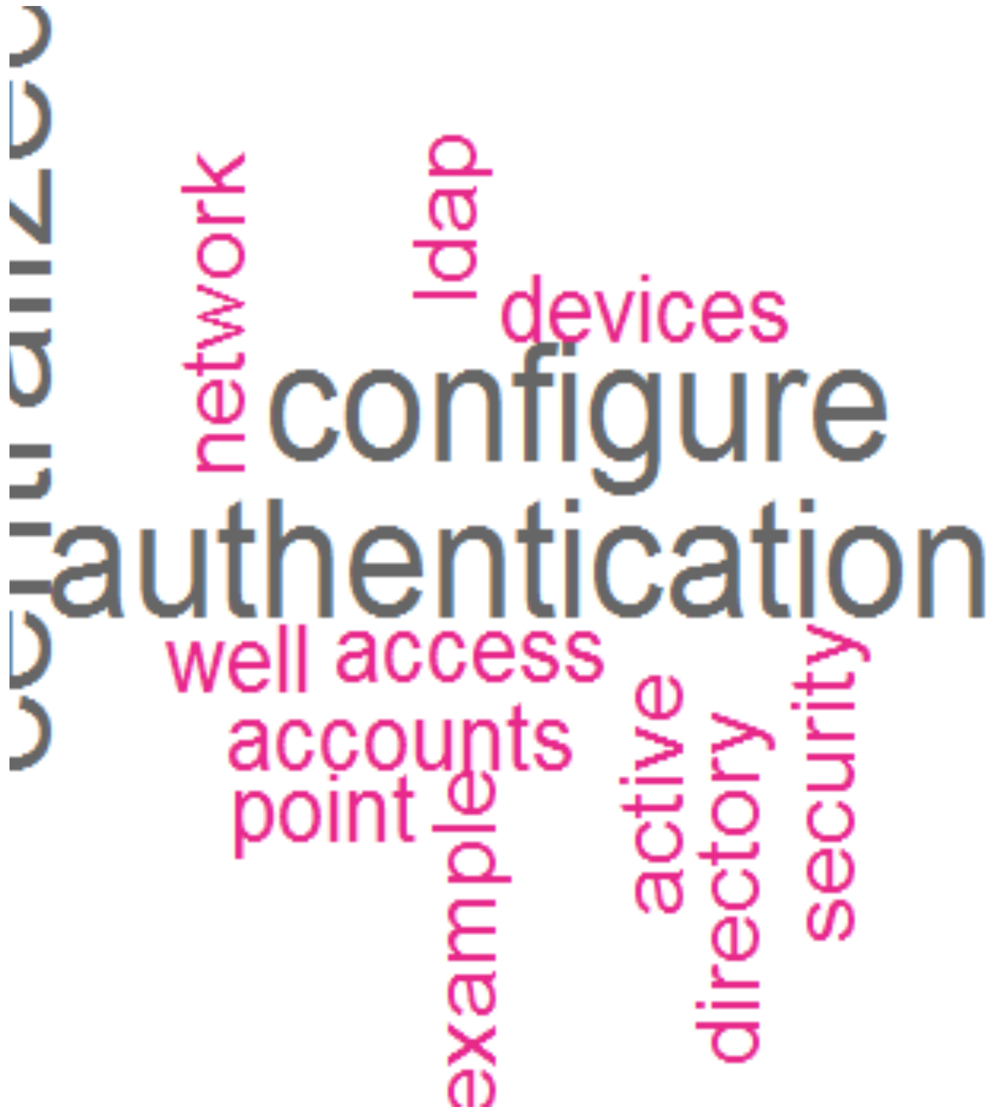
null device 1



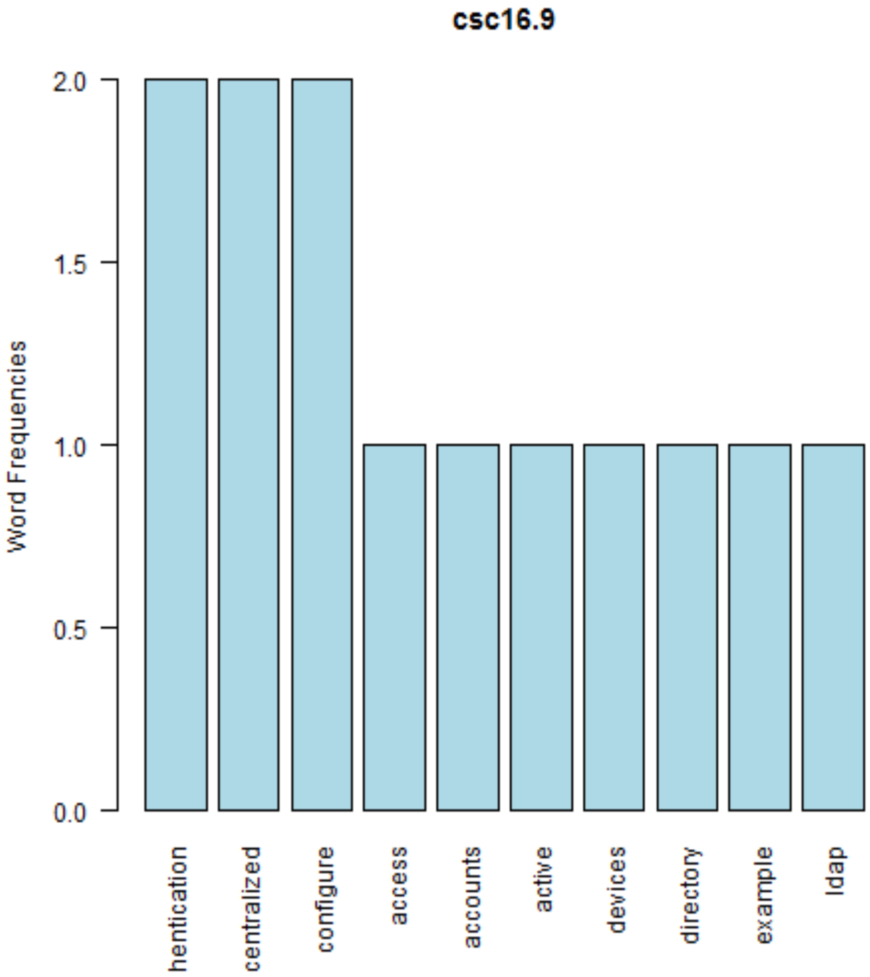
null device 1 [1] "Monitor attempts to access deactivated accounts through audit logging."

CSC 16.9

[1] “authentication + centralized”



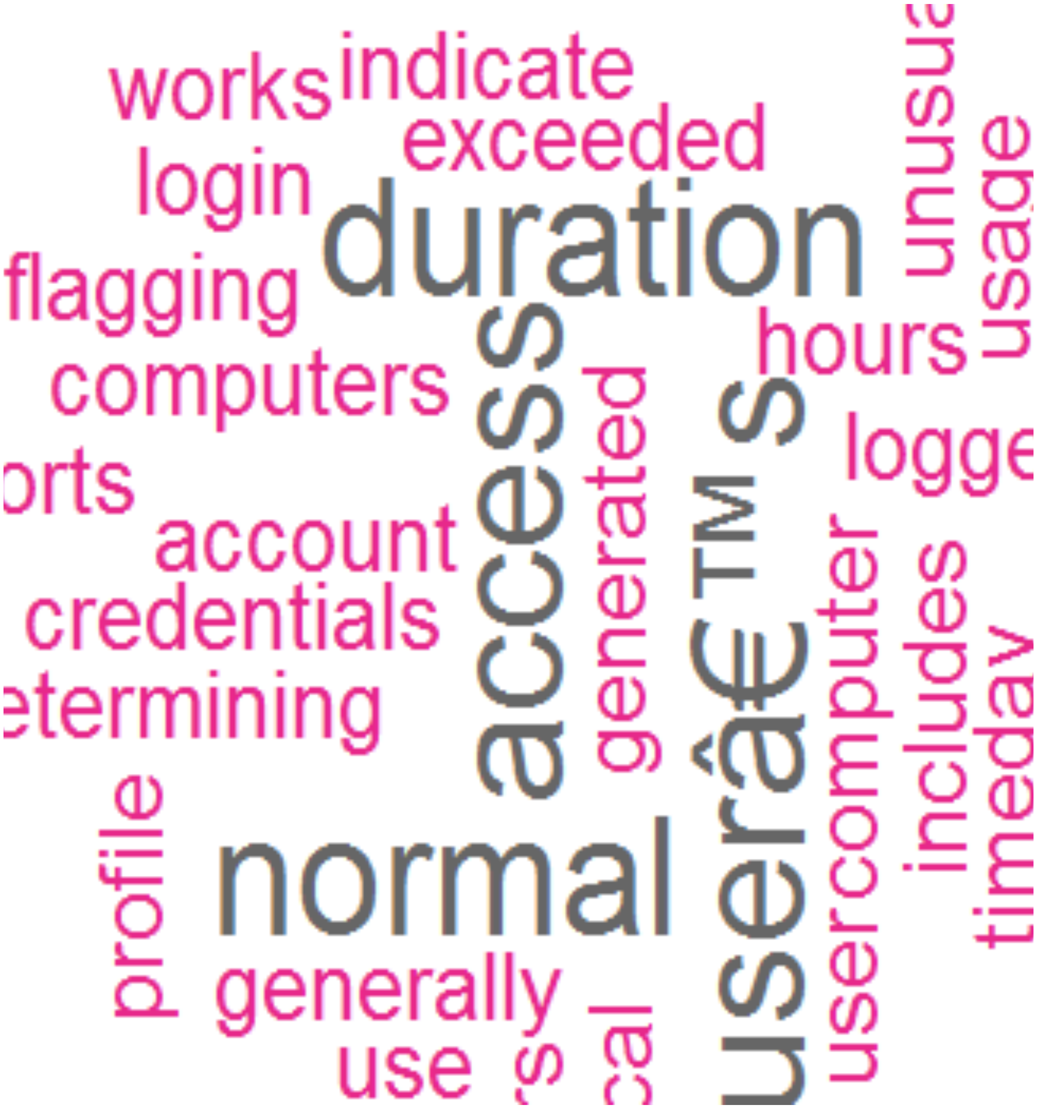
null device 1



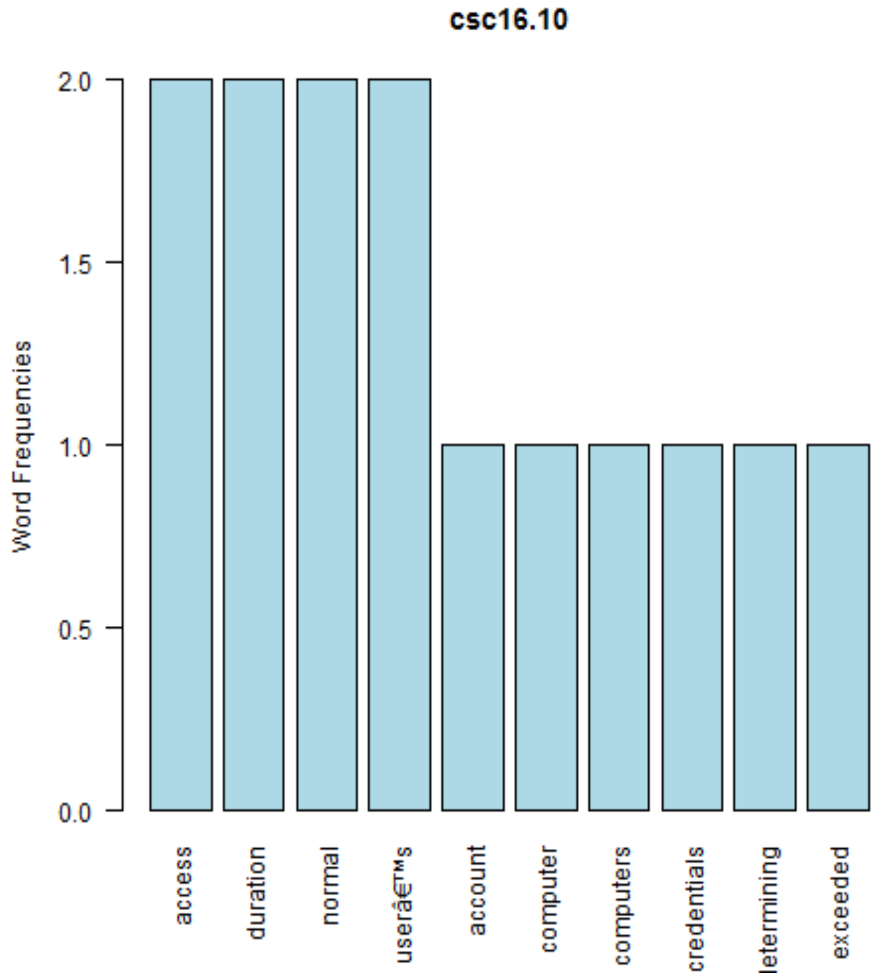
null device 1 [1] “Configure access for all accounts through a centralized point of authentication, for example Active Directory or LDAP. Configure network and security devices for centralized authentication as well.”

CSC 16.10

[1] “access + duration”



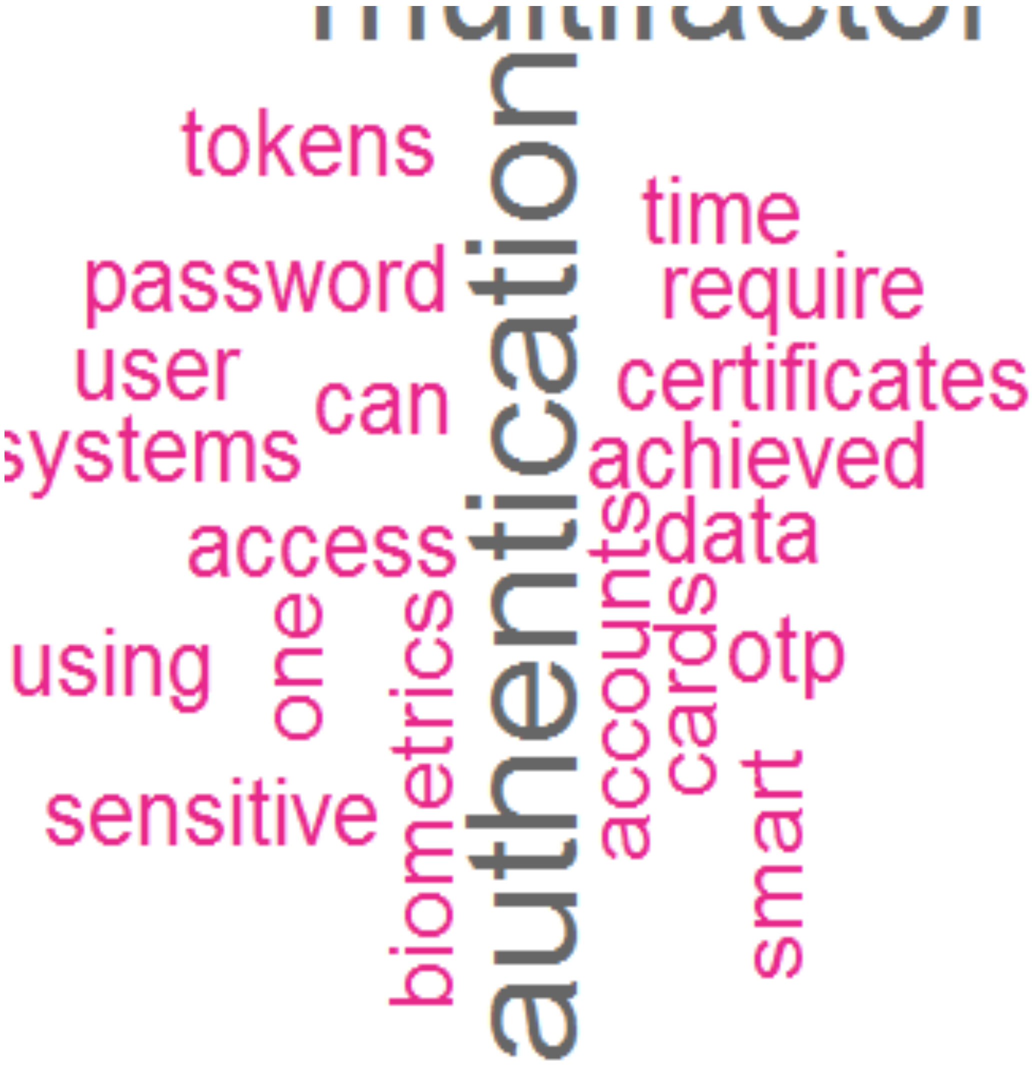
null device 1



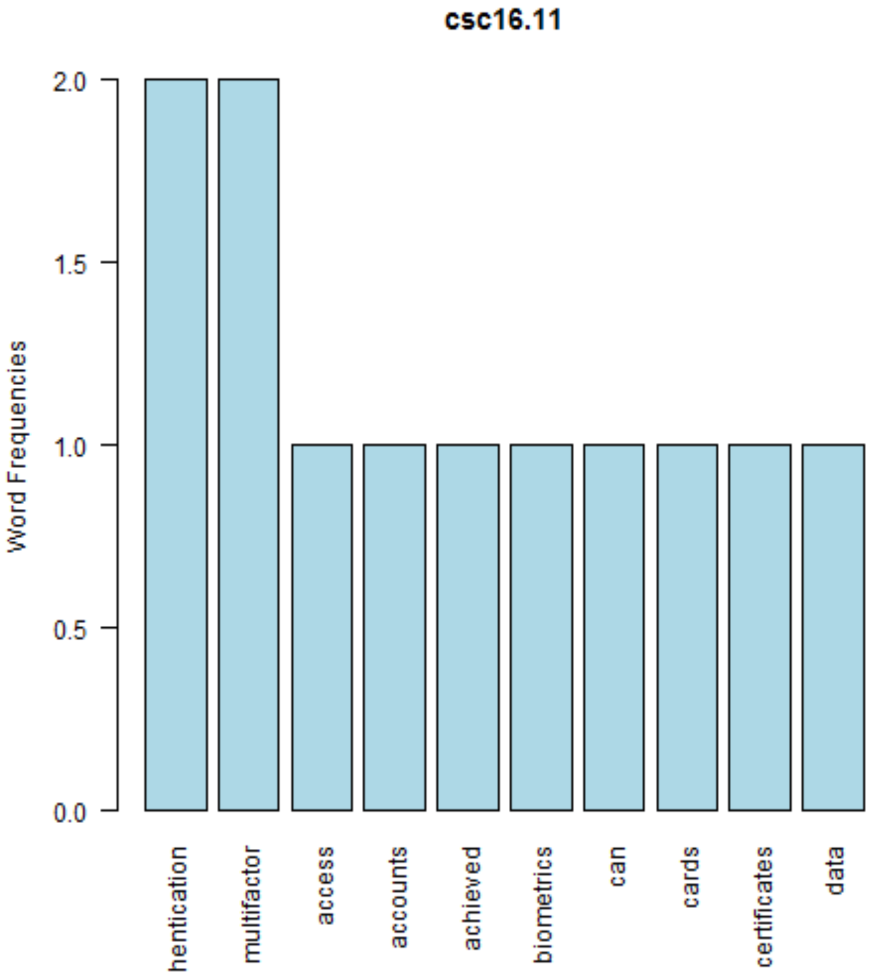
null device 1 [1] “Profile each userâ s typical account usage by determining normal time-of-day access and access duration. Reports should be generated that indicate users who have logged in during unusual hours or have exceeded their normal login duration. This includes flagging the use of the userâ s credentials from a computer other than computers on which the user generally works.”

CSC 16.11

```
[1] "authentication + multifactor"
```



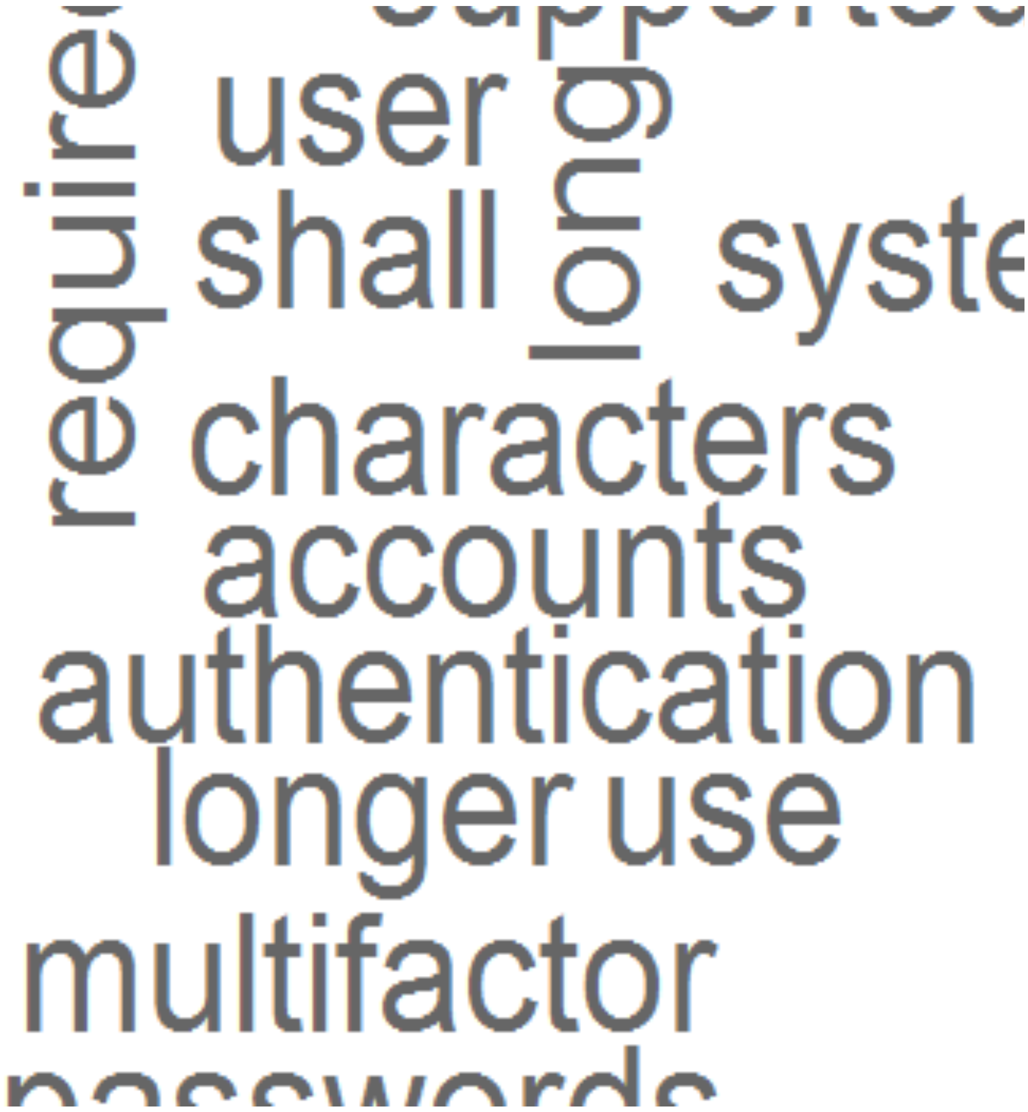
```
null device 1
```



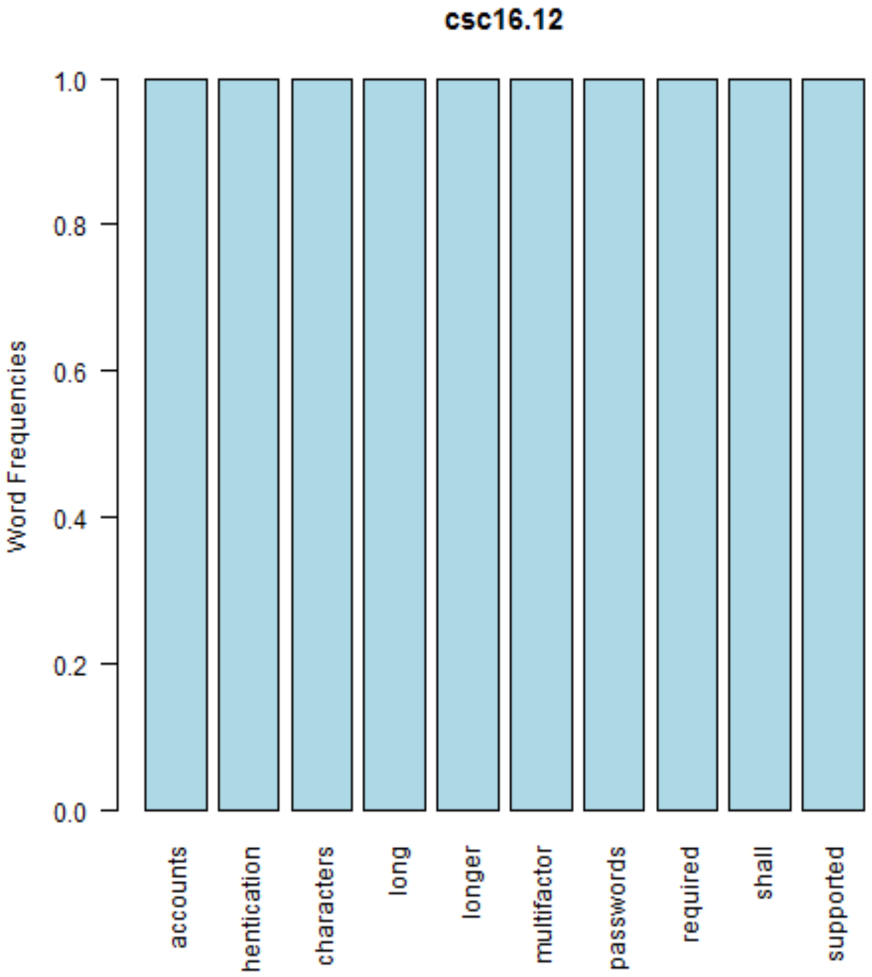
null device 1 [1] “Require multi-factor authentication for all user accounts that have access to sensitive data or systems. Multi-factor authentication can be achieved using smart cards, certificates, One Time Password (OTP) tokens, or biometrics.”

CSC 16.12

```
[1] “accounts + authentication”
```



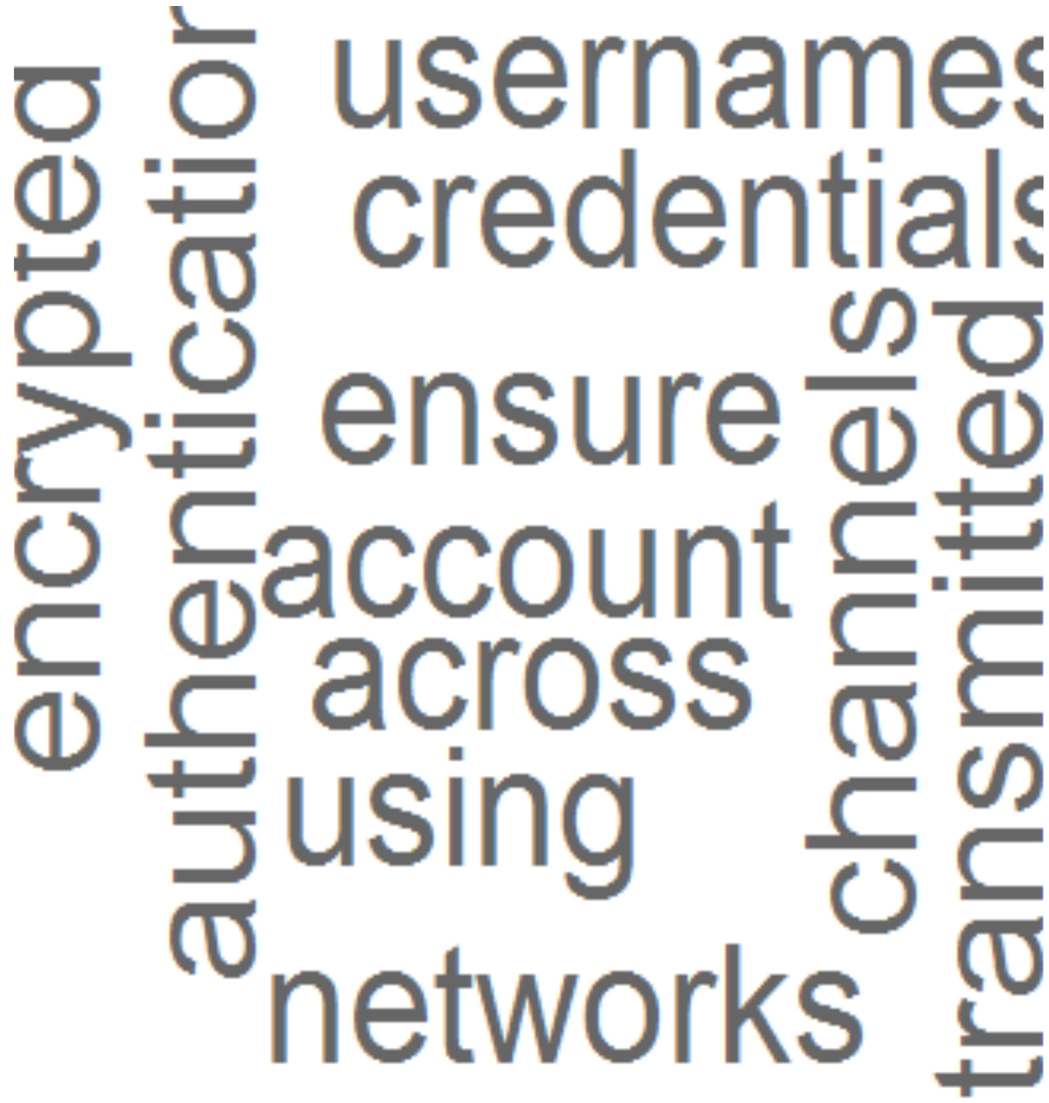
```
null device 1
```



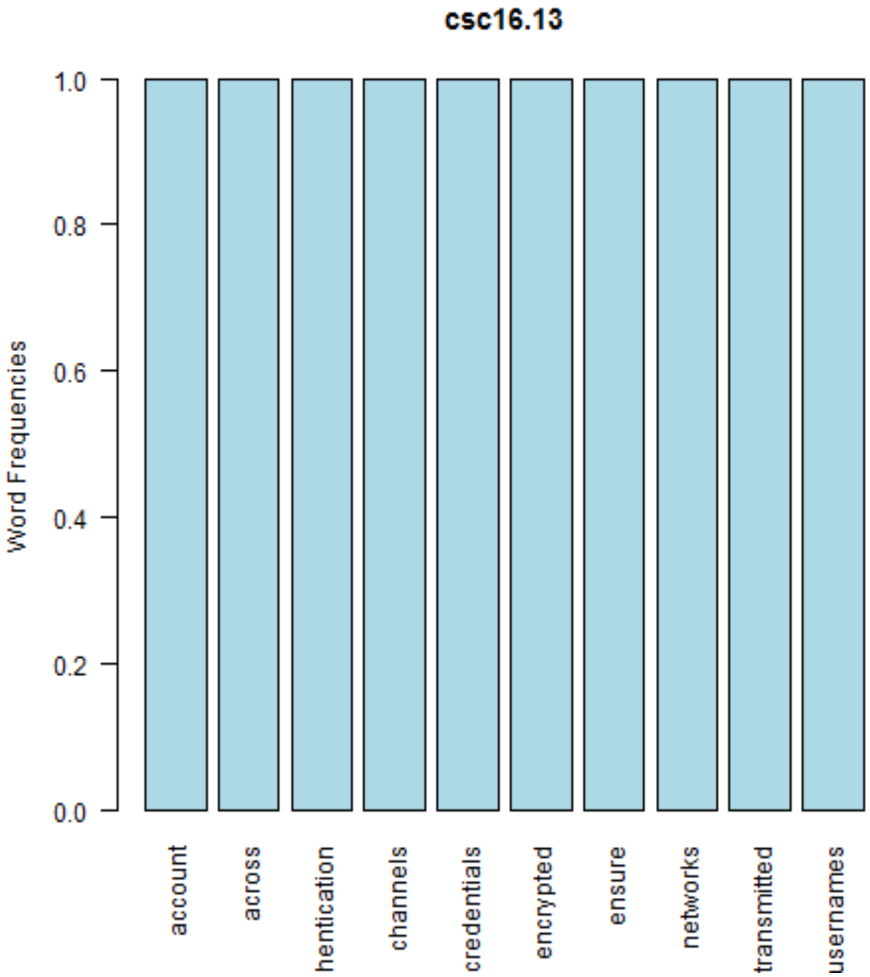
null device 1 [1] "Where multi-factor authentication is not supported, user accounts shall be required to use long passwords on the system (longer than 14 characters)."

CSC 16.13

[1] “account + across”



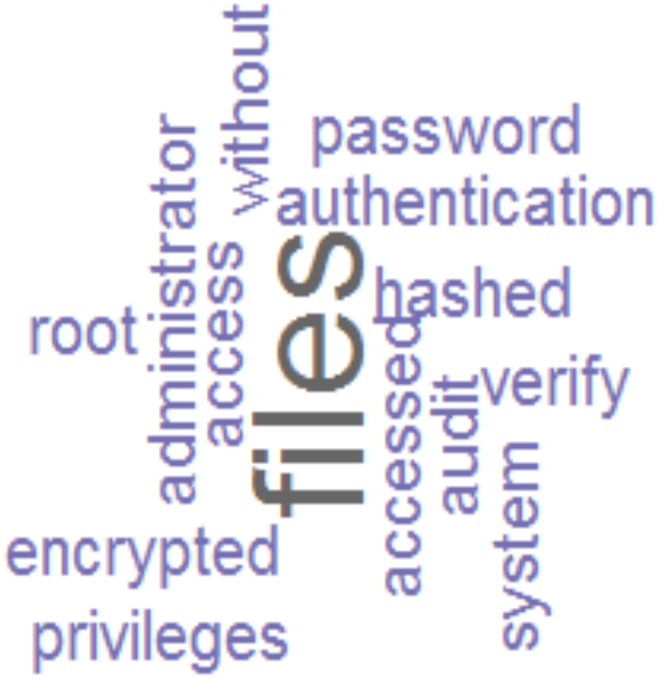
null device 1



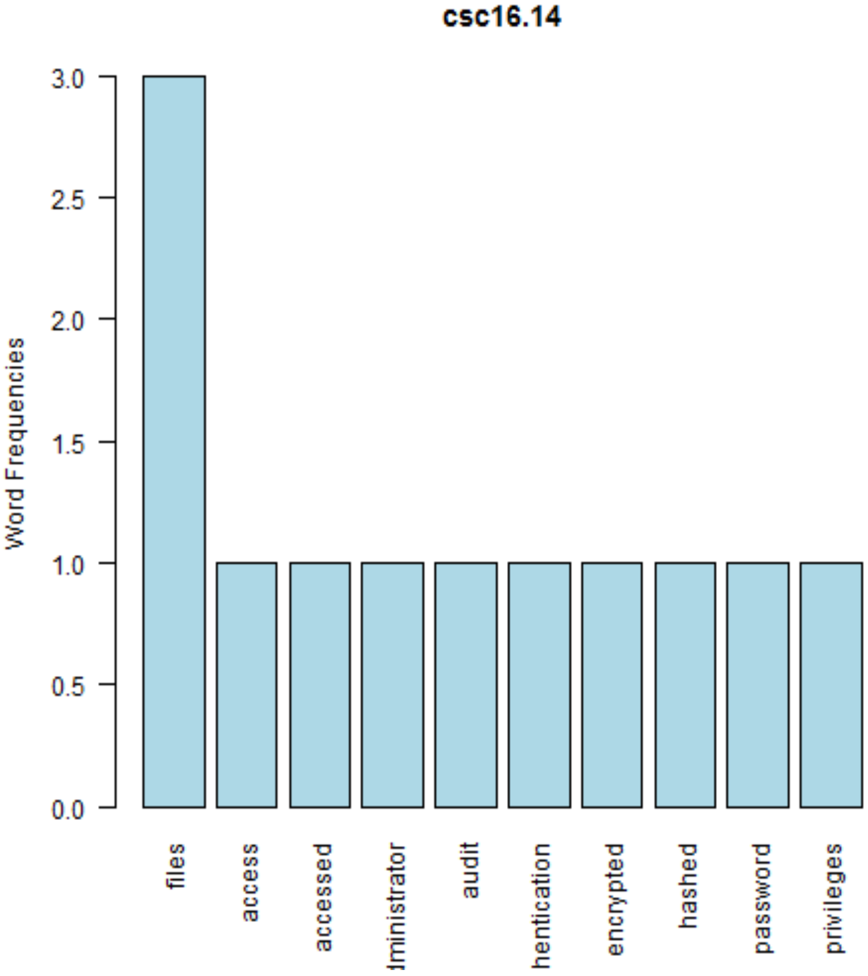
null device 1 [1] "Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels."

CSC 16.14

[1] “files + access”



null device 1



null device 1 [1] “Verify that all authentication files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system.”