zTALKS

April 2016 RACF Password Environment Survey Responses

Presented by

Richard K. Faulhaber

rkf@newera.com twitter: @faulhaber_rk

April 2016 RACF Password Environment Survey Responses

z/Auditing Essentials

VOLUME 2

Taming RACF – SETROPTS

http://www.newera-info.com/eBooks.html

z/Auditing Essentials

VOLUME 2

Mastering CA ACF2 – GSO

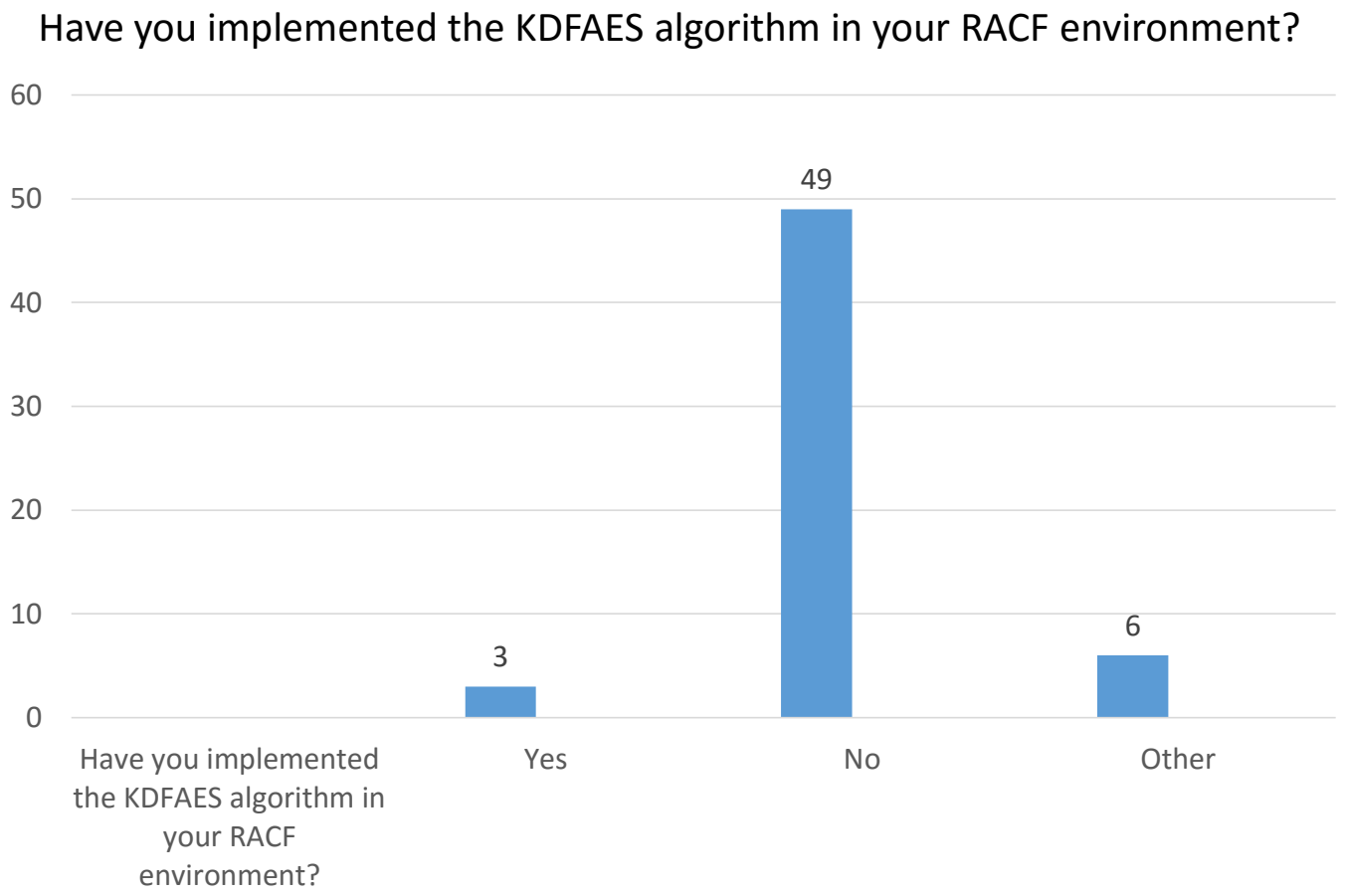
z/Auditing Essentials

VOLUME 2

Controlling CA Top Secret

April 2016 RACF Password Environment Survey Responses

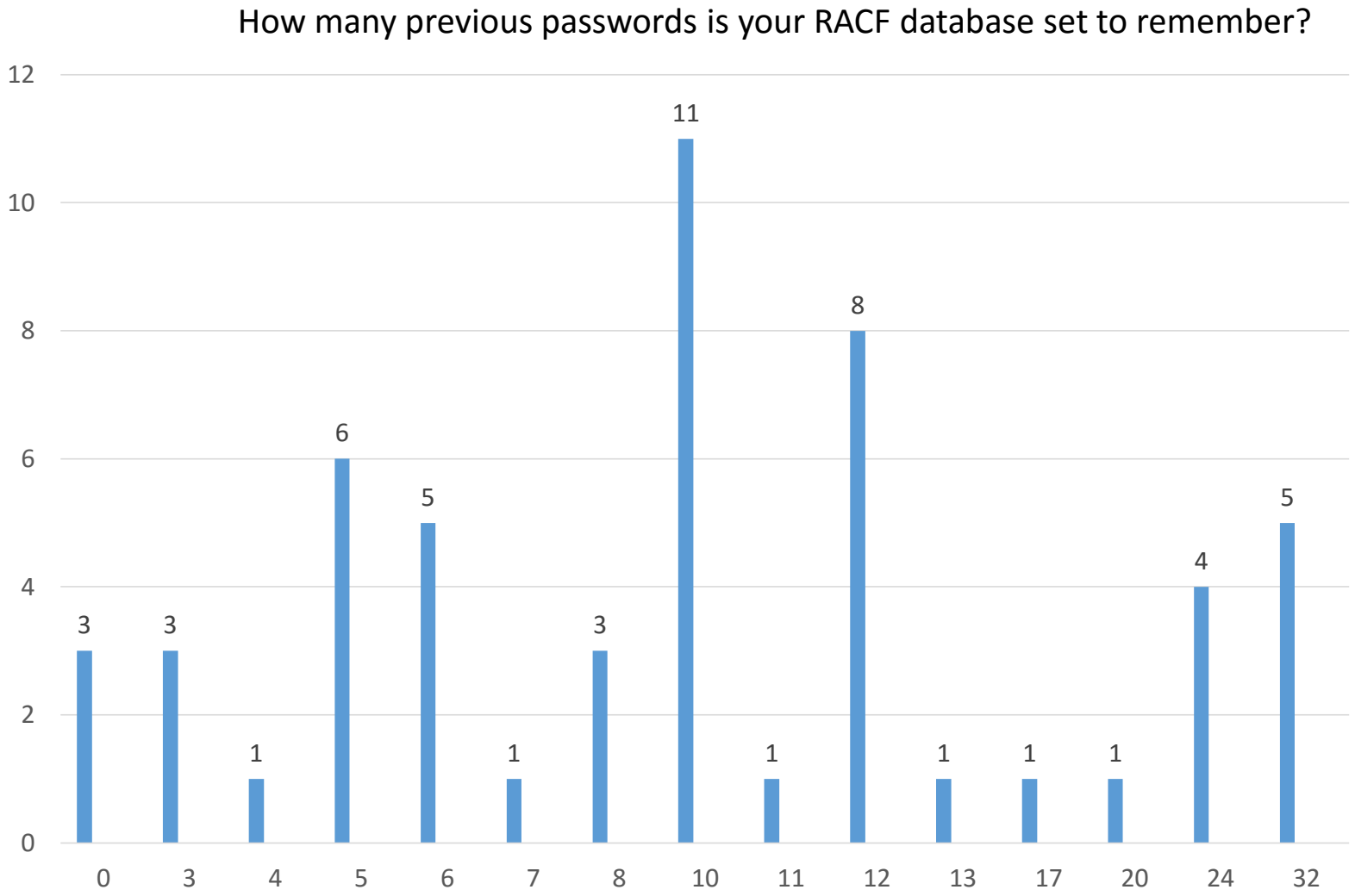
- Deploy two APARs OA43998 (SAF) and OA43999 onto to your systems.
- It is considered Best Practice to implement AES.
- The Point: Use the strongest encryption available that can be used for your environment.



See a current list of restrictions on implementing the KDFAES algorithm in the following APAR: APAR II14765 (http://www-01.ibm.com/support/docview.wss?uid=isg1II14765)

April 2016 RACF Password Environment Survey Responses

- Can be set from 1 to 32 or may be turned off.
- Best Practice: Set history to 10 or higher.
- The Point: Meant to encourage users not to recycle passwords.

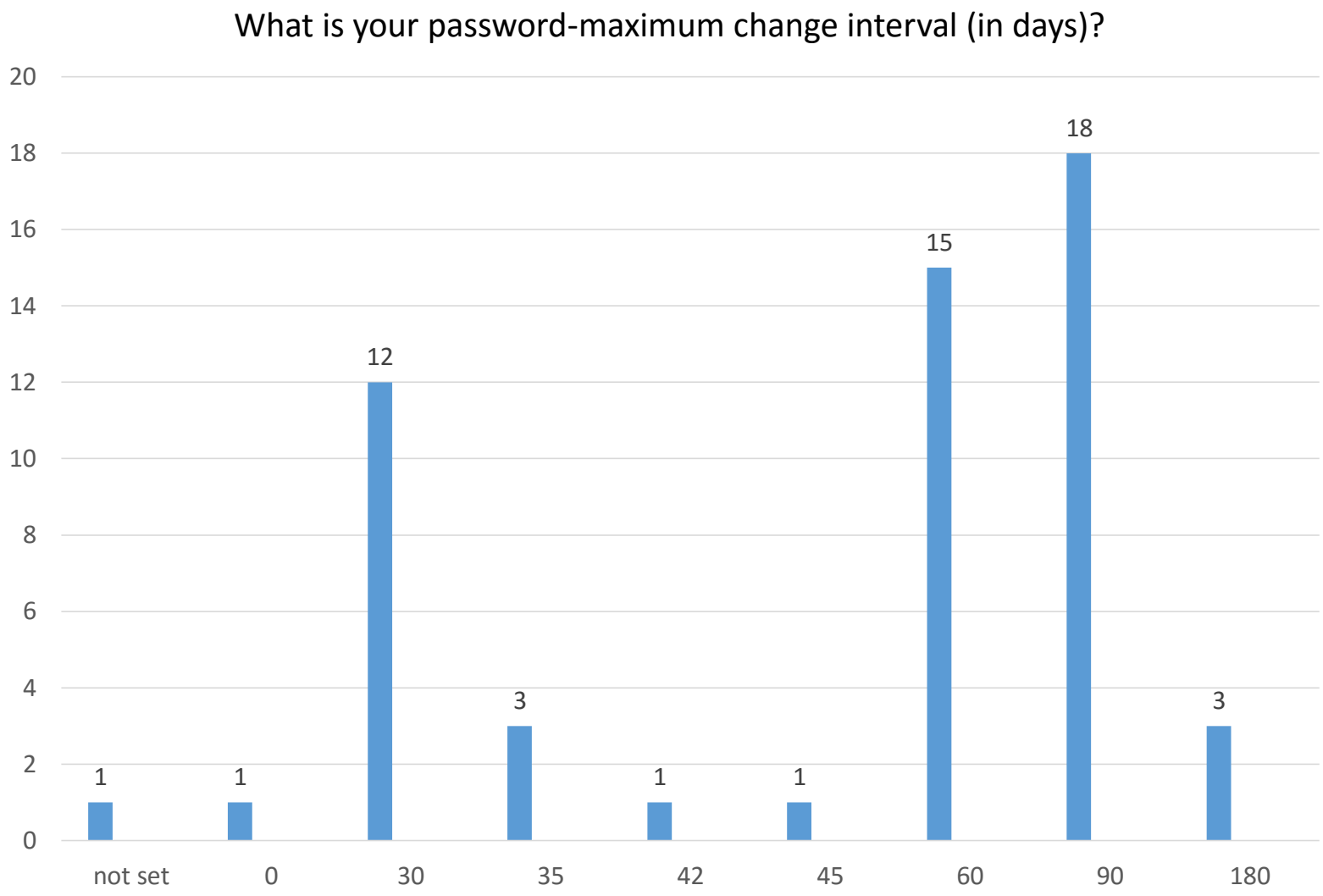


The Password History setting may prevent users from re-using specific passwords; however, it does not prevent a user from re-using a password **pattern**, like this:

January:	**MY01PASS**
February:	**MY02PASS**
March:	**MY03PASS**
April:	**MY04PASS**
May:	**MY05PASS**
June:	**MY06PASS**
July:	**MY07PASS**
August:	**MY08PASS**
September:	**MY09PASS**
October:	**MY10PASS**
November:	**MY11PASS**
December:	**MY12PASS**

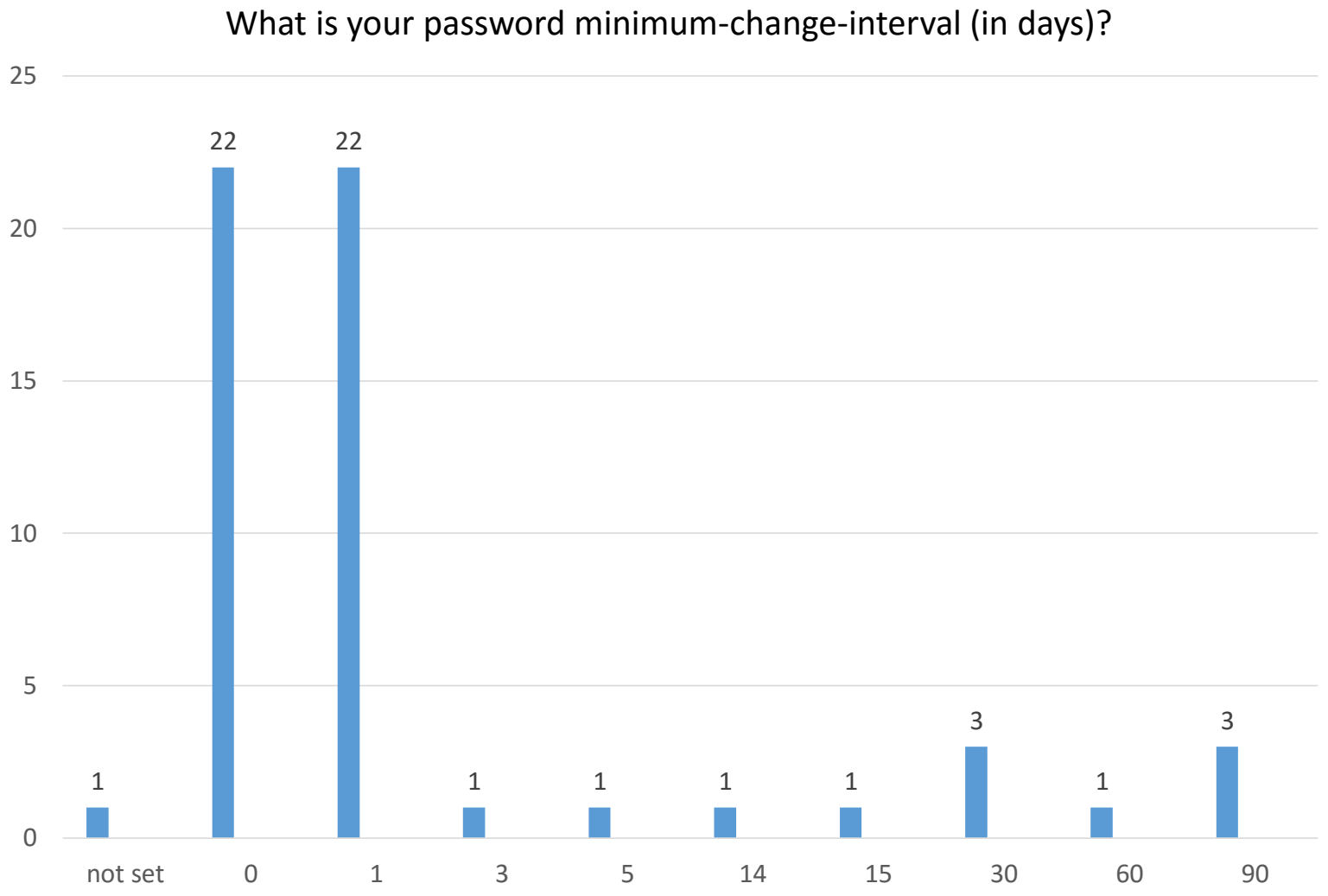
April 2016 RACF Password Environment Survey Responses

- Can be set from 1 to 254 days. Default is 30.
- Best Practice: Set between 1 and 60.
- The Point: Passwords should be changed regularly to keep ahead of a hacker trying to crack a password database or to shorten the time a hacker has access to a compromised account.



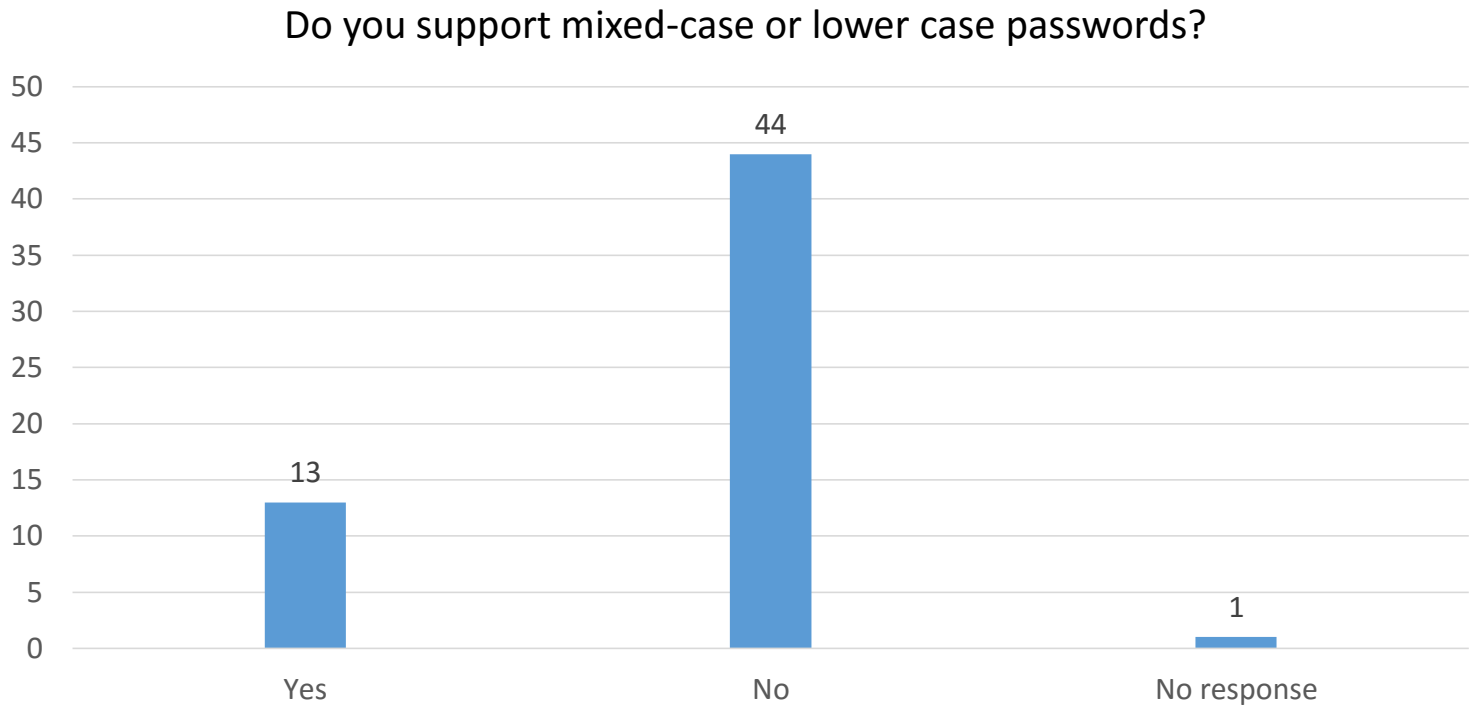
April 2016 RACF Password Environment Survey Responses

- Can be set from 0 to 254 days. Initial default is 0.
- Best Practice: Set greater than 0 but less than 60.
- The Point: Users should be discouraged from recycling old passwords.



April 2016 RACF Password Environment Survey Responses

- NOMIXEDCASE is the default setting.
- Best Practice: Mixed case should be implemented.
- The Point: The password environment should allow for the greatest number of available symbols for crafting passwords.



Allowing mixed-case passwords / Migration considerations for mixed case passwords:

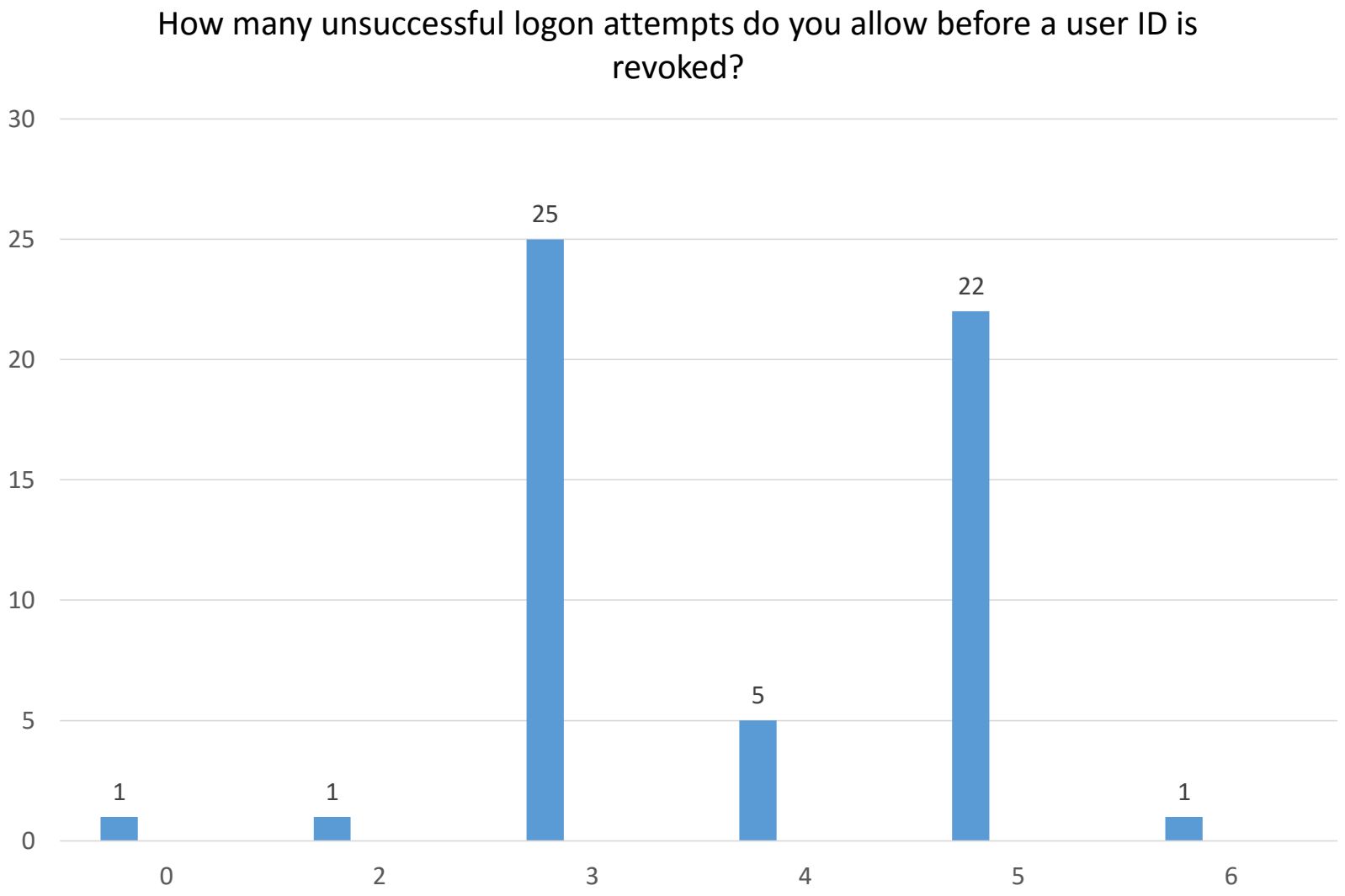
V2R2 - https://www.ibm.com/support/knowledgecenter/?lang=en#!/SSLTBW_2.2.0/com.ibm.zos.v2r2.icha700/amcp.htm

V2R1 - https://www.ibm.com/support/knowledgecenter/?lang=en#!/SSLTBW_2.1.0/com.ibm.zos.v2r1.icha700/amcp.htm

V1R13 - https://www.ibm.com/support/knowledgecenter/?lang=en#!/SSLTBW_1.13.0/com.ibm.zos.r13.icha700/amcp.htm%23amcp

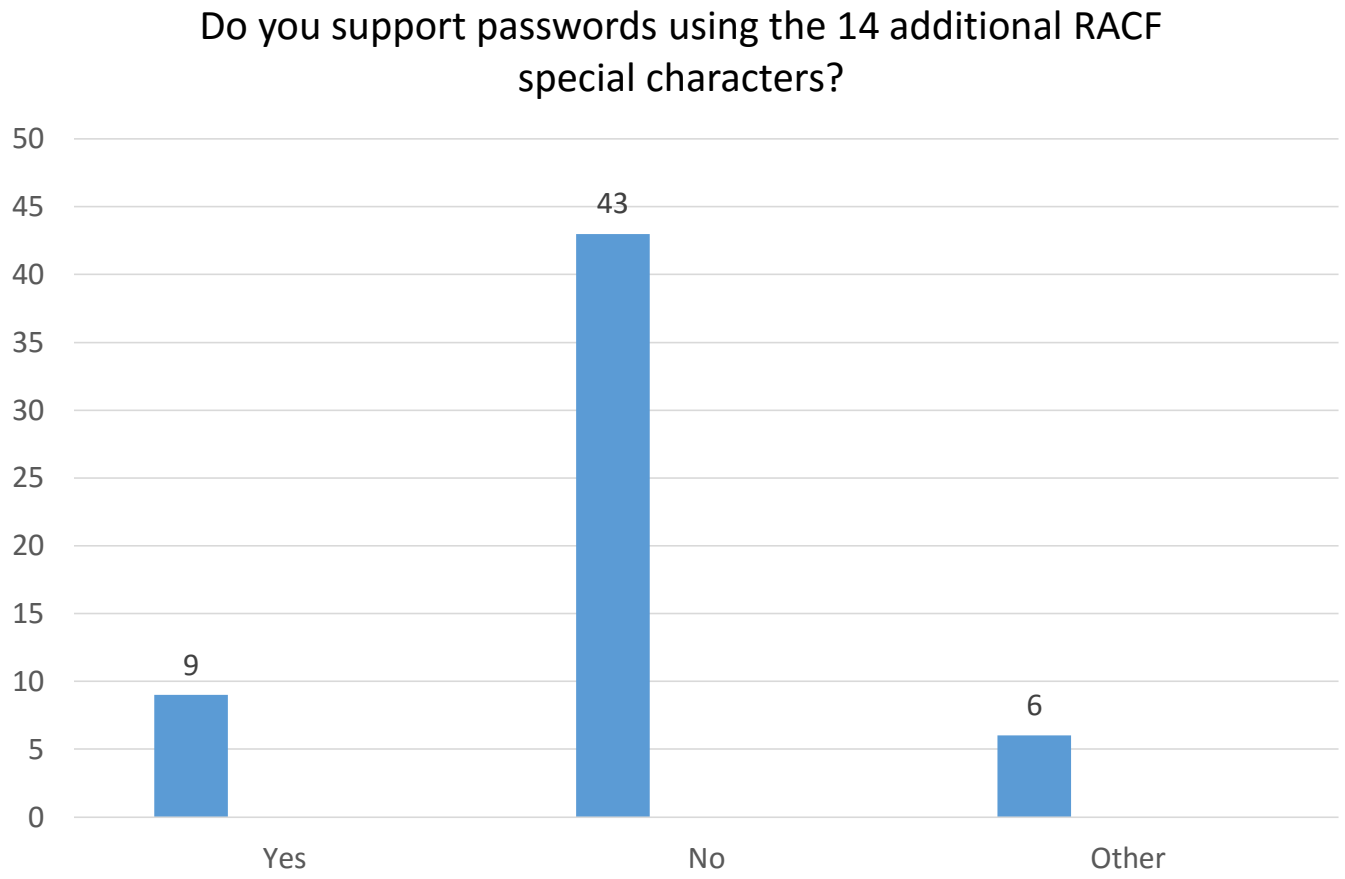
April 2016 RACF Password Environment Survey Responses

- May be set from 1 to 255 or turned off with NOREVOKE.
- Best Practice: Set to the lowest number that is acceptable to your organization.
- The Point: Must allow for typos or forgotten passwords. Should not be set so high it becomes an opportunity for a hacker.



April 2016 RACF Password Environment Survey Responses

- The 14 special characters are: .<+|&!*-%_>?:=
- Best Practice: Requiring at least one non-alphanumeric character.
- The Point: Users should have the largest possible symbol set from which to draw in creating passwords.



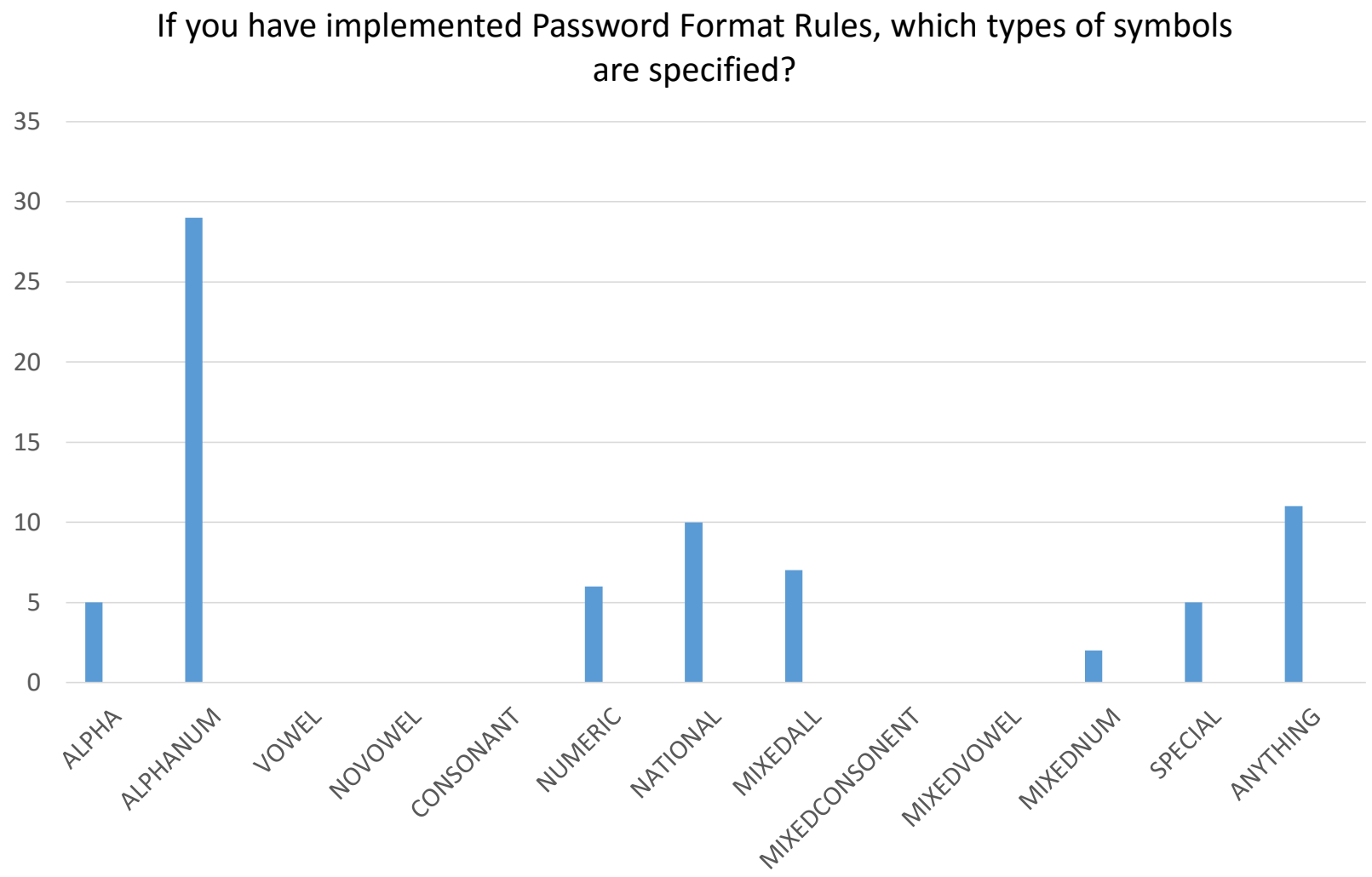
There are some restrictions on using the new special characters, for example, TSO/E will not accept a password beginning with '?'. See the following APAR for a current list of such restrictions and other relevant information: APAR II14765 (http://www-01.ibm.com/support/docview.wss?uid=isg1II14765)

April 2016 RACF Password Environment Survey Responses

- May be set from 1 to 255 days. NOWARNING is the default.
- Best Practice: Suggested value of 10 days.
- The Point: Give a user time to come up with a password that is easy to remember but difficult to guess. .

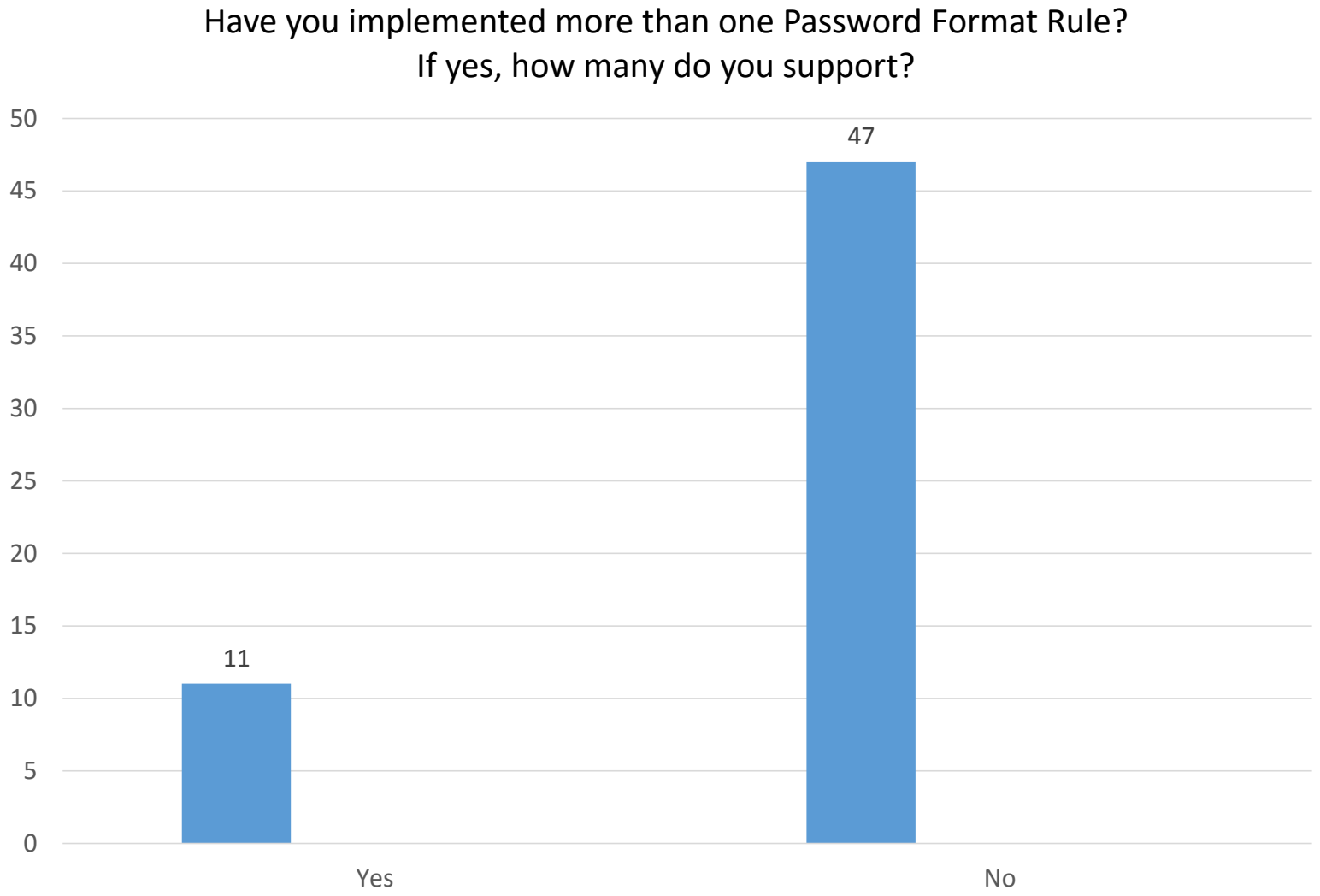
April 2016 RACF Password Environment Survey Responses

- RACF allows for 8 rules. New passwords must satisfy only one rule.
- Best Practice (DoD): 8-chars long, mix of letters, numbers, special chars., no repeats or consecutive characters, no user info or dictionary words.
- The Point: Rules should enforce the use of symbol sets that would break with typical password conventions.



April 2016 RACF Password Environment Survey Responses

- 3, 4, 7, 8 rules.
- 1- using 8 rules to enforce use of at least one numeric.
- 3 – using System REXX, a password processing exit or Windows Active Directory to check password strength.
- 2- don’t know.



April 2016 RACF Password Environment Survey Responses

If you have implemented more than one as indicated in question 10 above, why do you feel the need for more than one Password Format Rule?

- Decided to add a few unique formats for some specific application IDs
- Trying to prevent use of easily guessed passwords such as those with repeating, too similar passwords, or those on a restricted list like month.
- To require at least one NUMERIC or one NATIONAL.
- Had a request to allow a 6 character password.

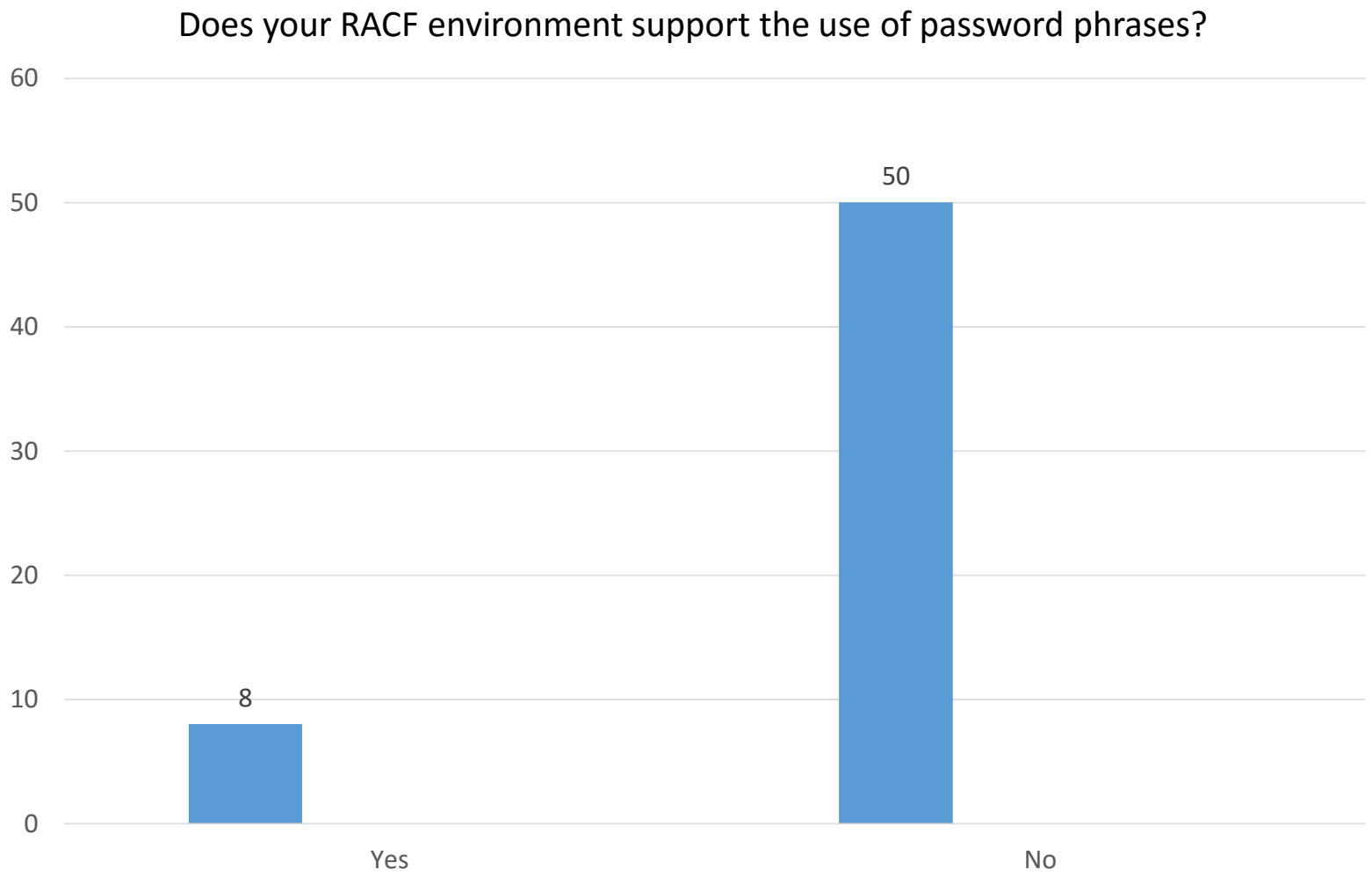
Within RACF, rules are not tied to specific users or IDs.

Though there are 8 possible rules, a new password need satisfy only one of them.

The Point: Password format rules get users to include specific types of characters an avoid certain patterns.

April 2016 RACF Password Environment Survey Responses

- Password phrases – the future of passwords.
- Best Practice: Adding length to passwords (ie, using password phrases) makes them stronger.
- The Point: Strength in numbers.



Why Complex Passwords Should Be Fact and Not Fiction: http://www.newera-info.com/RF1.html

Some new ideas for comment and discussion...

- Tie specific password rule to specific user or group of users.

- Logon Screen – Audit message: Send an email or text to the user with each successful logon. Vacation mode – A message sent to the user and a message sent to the user's supervisor. Each would be independently switchable.

April 2016 RACF Password Environment Survey Responses

RACF Survey for May 2016… RACF Data Processing Options:

- AUTOMATIC_DATASET_PROTECTION
- ENHANCED_GENERIC_NAMING
- REAL_DATA_SET_NAMES
- JES-BATCHALLRACF
- JES-XBMALLRACF
- JES-EARLYVERIFY
- PROTECT-ALL
- TAPE_DATA_SET_PROTECTION
- SECURITY_RETENTION_PERIOD
- ERASE-ON-SCRATCH
- SINGLE_LEVEL_NAME
- LIST_OF_GROUPS_ACCESS_CHECKING
- INACTIVE_USERIDS_AUTOMATICALLY_REVOKED
- DATA_SET_MODELLING

Richard K. Faulhaber
rkf@newera.com twitter: @faulhaber_rk