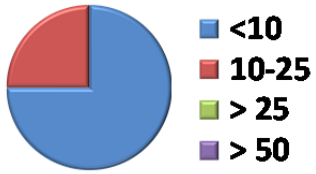
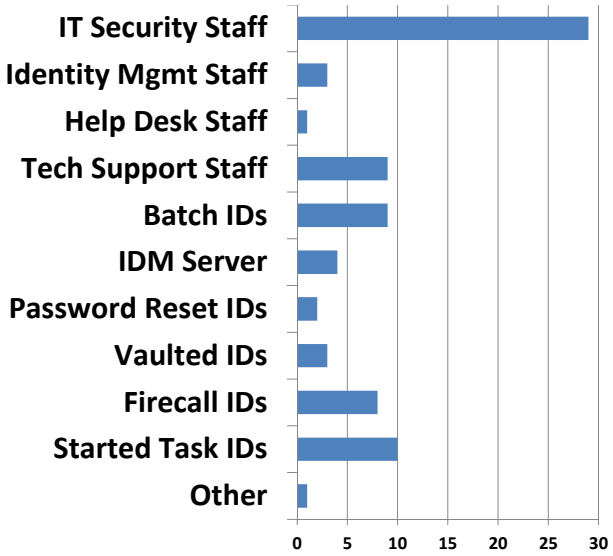
Approximately how many users have been assigned IDs with System-SPECIAL authority?

Responses	Count	Percent %
Less than 10	24	75.0%
10-25	8	25.0%
Over 25	0	0%
Over 50	0	0%
Total	**32**	**100%**



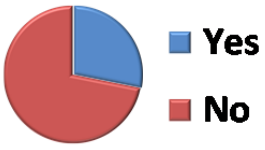
What types of users have been assigned System-SPECIAL authority?

Responses	Count	Percent %
IT Security Staff	29	90.1%
Identity Management Staff	3	9.4%
Help Desk Staff	1	3.1%
Technical Support Staff	9	28.1%
Batch IDs	9	28.1%
Identity Management Server	4	12.5%
Password Reset Server IDs	2	6.3%
Vaulted IDs (e.g., CyberArk)	3	9.4%
Firecall IDs	8	25.0%
Started Task IDs	10	31.3%
Other: • System consoles that are defined only at the DR site and are used for DR startup.	1	3.1%
Responses	**32**	



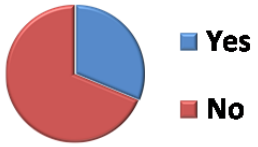
Are any of the System-SPECIAL users consultants, contractors, or outsource vendor staff?

Responses	Count	Percent %
Yes	9	28.1%
No	23	71.9%
Total	**32**	**100%**



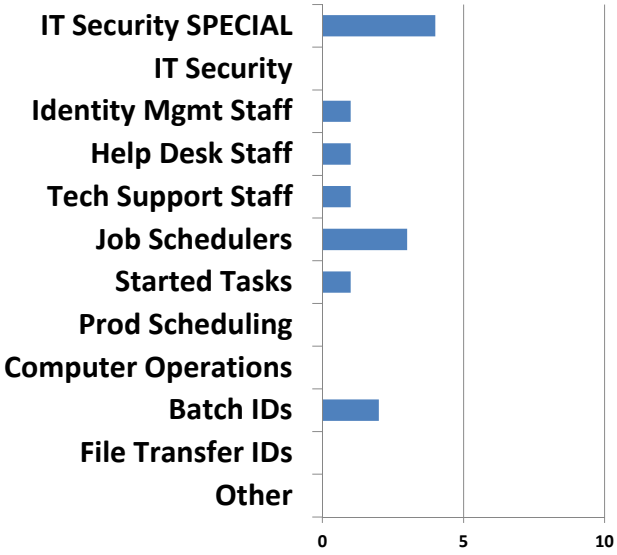
Do you have SURROGAT profiles that permit the submission of IDs with System-SPECIAL authority?

Responses	Count	Percent %
Yes	10	31.2%
No	22	68.8%
Total	32	100%



What types of users have SURROGAT authority to submit System-SPECIAL IDs?

Responses	Count	Percent %
IT Security Staff with System SPECIAL	4	40.0%
IT Security Staff without System SPECIAL	0	0%
Identity Management Staff	1	10.0%
Help Desk Staff	1	10.0%
Technical Support Staff	1	10.0%
Production Batch Job Schedulers	3	30.0%
Started Tasks Other Than Job Schedulers	1	10.0%
Production Scheduling Staff	0	0%
Computer Operations Staff	0	0%
Batch IDs	2	20.0%
File Transfer IDs	0	0%
Other	0	0%
Responses	10	

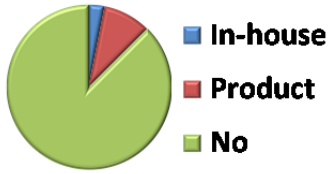


Are any of the users with SURROGAT authority to System-SPECIAL IDs consultants, contractors, or outsource vendor staff?

Responses	Count	Percent %
Yes	0	0%
No	10	100%
Total	10	100%

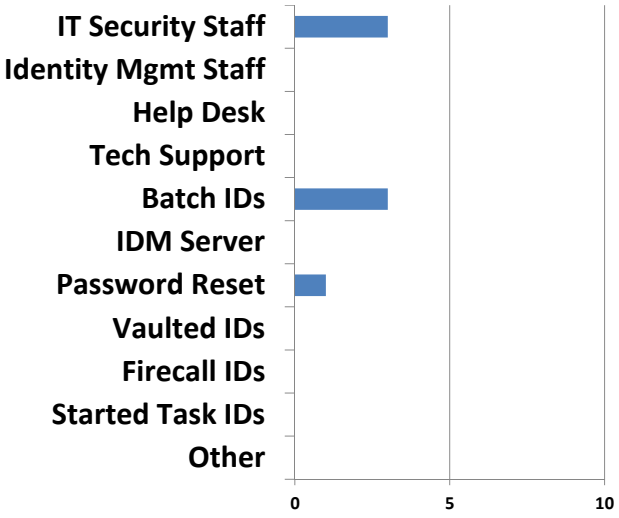
Have you implemented restrictions on what commands and operands certain System-SPECIAL users can use?

Responses	Count	Percent %
Yes, using in-house written RACF commands exits	1	3.1%
Yes, using a RACF Administration add-on product	3	9.4%
No	28	87.5%
Total	**32**	**100%**



What types of System-SPECIAL users have been restricted as to what RACF commands and operands they can use?

Responses	Count	Percent %
IT Security Staff	3	75.0%
Identity Management Staff	0	0%
Help Desk Staff	0	0%
Technical Support Staff	0	0%
Batch IDs	3	75.0%
Identity Management Server	0	0%
Password Reset Server IDs	1	25.0%
Vaulted IDs (e.g., CyberArk)	0	0%
Firecall IDs	0	0%
Started Task IDs	0	0%
Other	0	0%
Responses	**4**	

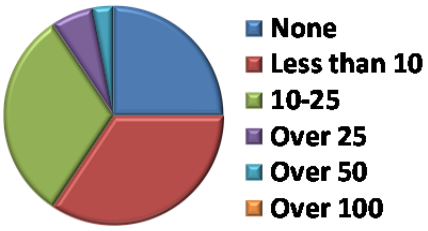


Nature of restrictions:

- Commands that can be done through a change-control process are excluded from other System SPECIAL users.
- Only permit actions on USERS. All other commands restricted.

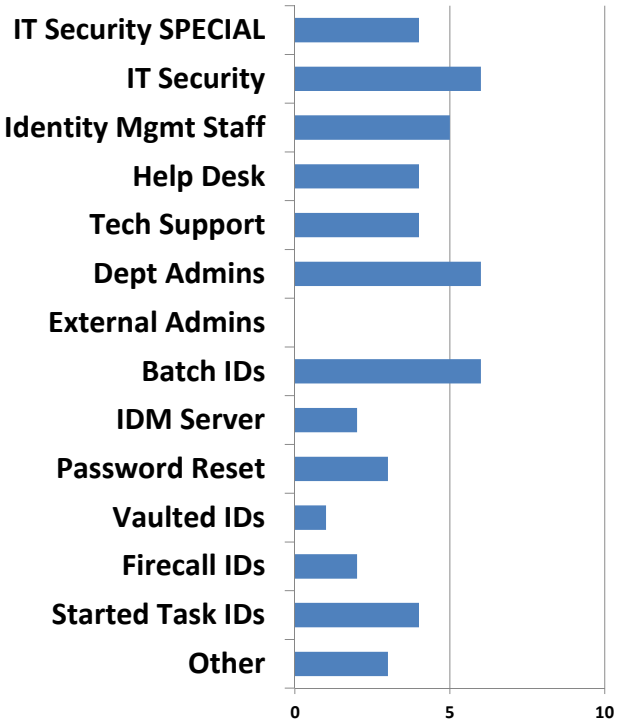
Approximately how many users have been assigned IDs with Group-SPECIAL authority?

Responses	Count	Percent %
None	8	25.0%
Less than 10	11	34.4%
10-25	10	31.2%
Over 25	2	6.3%
Over 50	1	3.1%
Over 100	0	0%
Total	**32**	**100%**



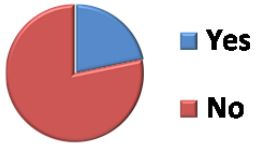
What types of users have been assigned Group-SPECIAL authority?

Responses	Count	Percent %
IT Security Staff with System SPECIAL	4	17.4%
IT Security Staff without System SPECIAL	6	26.1%
Identity Management Staff	5	21.7%
Help Desk Staff	4	17.4%
Technical Support Staff	4	17.4%
Departmental Security Administrators	6	26.1%
External Client Security Administrators	0	0%
Batch IDs	6	26.1%
Identity Management Server	2	8.7%
Password Reset Server IDs	3	13.0%
Vaulted IDs (e.g., CyberArk)	1	4.4%
Firecall IDs	2	8.7%
Started Task IDs	4	17.4%
Other: • Business manager - decide which group (branch office) to assign to given user. • Mainframe moved off-shore, and off-shore admins define many group special users. • Automation bots that connect users to a group.	3	13.0%
Responses	**23**	



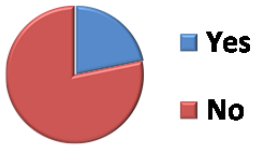
Are any of the Group-SPECIAL users consultants, contractors, or outsource vendor staff?

Responses	Count	Percent %
Yes	5	21.7%
No	18	78.3%
Total	23	100%



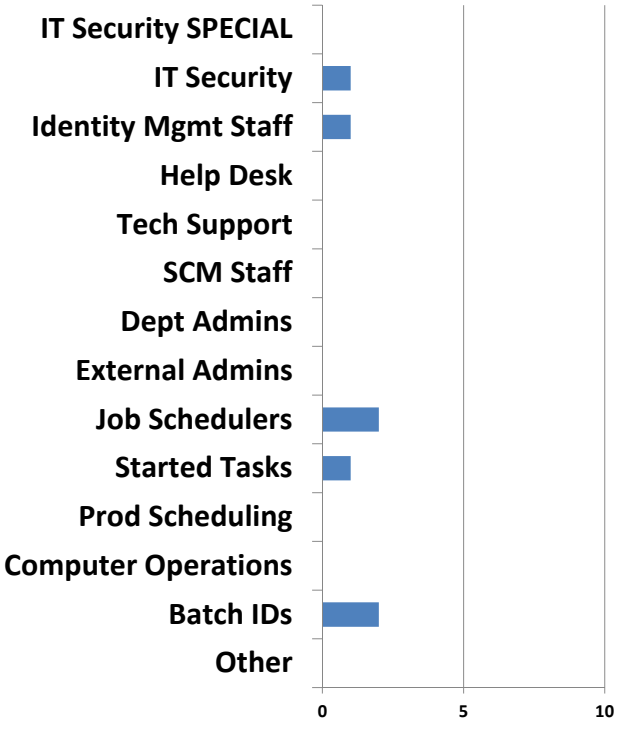
Do you have SURROGAT profiles that permit the submission of IDs with Group-SPECIAL authority?

Responses	Count	Percent %
Yes	5	21.7%
No	18	78.3%
Total	23	100%



What types of users have SURROGAT authority to submit Group-SPECIAL IDs?

Responses	Count	Percent %
IT Security Staff with System SPECIAL	0	0%
IT Security Staff without System SPECIAL	1	20.0%
Identity Management Staff	1	20.0%
Help Desk Staff	0	0%
Technical Support Staff	0	0%
Software Change Management Staff	0	0%
Departmental Security Administrators	0	0%
External Client Security Administrators	0	0%
Production Batch Job Schedulers	2	40.0%
Started Tasks Other Than Job Schedulers	1	20.0%
Production Scheduling Staff	0	0%
Computer Operations Staff	0	0%
Batch IDs	2	40.0%
Other	0	0%
Responses	5	

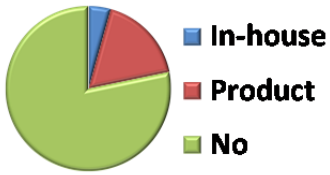


Are any of the users with SURROGAT authority to Group-SPECIAL IDs consultants, contractors, or outsource vendor staff?

Responses	Count	Percent %
Yes	0	0%
No	5	100%
Total	**5**	**100%**

Have you implemented restrictions on what commands and operands certain Group-SPECIAL users can use?

Responses	Count	Percent %
Yes, using in-house written RACF commands exits	1	4.4%
Yes, using a RACF Administration add-on product	4	17.4%
No	18	78.3%
Total	**23**	**100%**



What types of Group-SPECIAL users have been restricted as to what RACF commands and operands they can use?

Responses	Count	Percent %
IT Security Staff	2	40.0%
Identity Management Staff	0	0%
Help Desk Staff	2	40.0%
Technical Support Staff	2	40.0%
Software Change Management Staff	1	20.0%
Departmental Security Administrators	2	40.0%
External Client Security Administrators	1	20.0%
Batch IDs	3	60.0%
Identity Management Server IDs	1	20.0%
Password Reset Server IDs	2	40.0%
Vaulted IDs (e.g., CyberArk)	2	40.0%
Firecall IDs	2	40.0%
Started Task IDs	2	40.0%
Other	0	0%
Responses	**5**