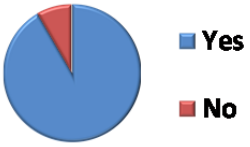
Is General Resource class FSSEC active at your installation?

Responses	Count	Percent %
Yes, on all RACF databases	10	41.7%
Yes, but only on some databases	2	8.3%
No	12	50%
Total	**24**	**100%**

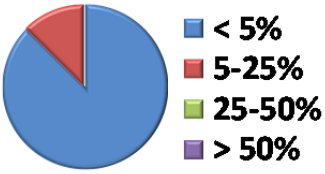
Do you have Extended Access Control Lists (ACLs) defined for any Unix files or directories?

Responses	Count	Percent %
Yes	11	91.7%
No	1	8.3%
Total	**12**	**100%**



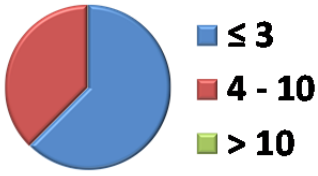
Approximately what percentage of your Unix files and directories have Extended ACLs?

Responses	Count	Percent %
Less than 5%	7	87.5%
5% to 25%	1	12.5%
25% to 50%	0	0%
Over 50%	0	0%
Total	**8**	**100%**



On average, approximately how many user and group permissions are in each Extended ACL?

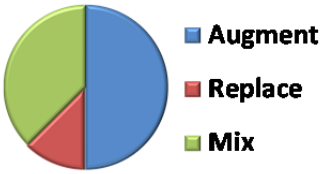
Responses	Count	Percent %
3 or less	5	62.5%
4 to 10	3	37.5%
More than 10	0	0%
Total	**8**	**100%**



Special thanks to Bruce Wells of IBM for his assistance in reviewing and testing this survey.

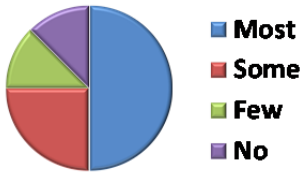
Do you tend to add group ACL permissions to augment or replace the File Security Packet (FSP) group permission? By replace, we mean not grant the FSP group access and use ACLs instead.

Responses	Count	Percent %
Augment	4	50.0%
Replace	1	12.5%
Mix of both	3	37.5%
Total	**8**	**100%**



Do you set up file and directory default ACLs along with your Extended ACLs?

Responses	Count	Percent %
Yes, for most directories with ACLs	4	50.0%
Yes, for some directories with ACLs	2	25.0%
Yes, for a few directories with ACLs	1	12.5%
No	1	12.5%
Total	**8**	**100%**



For what requirements, situations, and/or circumstances have you found it useful to use Extended ACLs?

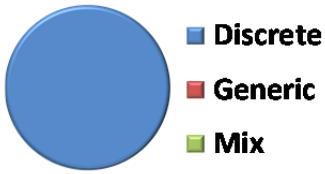
Responses
Ability to grant automation and/or support teams specific access to certain locked down log files, or to service/task ID home directories. The extra flexibility is also useful in many one-off cases where more granular access is required.
When a manager says that a person should have update access to a couple files but others in their workgroup shouldn't.
When group and other don’t cover use case for access
minimal FSP, extend with ACL
Giving access to wsdls to CICS regions, code promotion tool, and CICS/Unix admins at the right level for each. Same reasons as for RACF profiles really.
Owner, Group and other permissions do meet the security requirements.
Granting additional access beyond the standard owner and group
Multiple roles (techies, batch users, CICS, Conf. Mngt tool, …) need to have different types of access on files & directories

Is there a UNIXPRIV profile that protects resource SUPERUSER.FILESYS.ACLOVERRIDE?

Responses	Count	Percent %
Yes, on all RACF databases	0	0%
Yes, but only on some databases	1	11.1%
No	8	88.9%
Total	**9**	**100%**

Is the UNIXPRIV profile guarding SUPERUSER.FILESYS.ACLOVERRIDE a generic profile or a discrete profile.

Responses	Count	Percent %
Discrete on all systems	1	100%
Generic on all systems	0	0%
Mix	0	0%
Total	**1**	**100%**



Who is permitted what level of access to the UNIXPRIV class profile protecting SUPERUSER.FILESYS.ACLOVERRIDE?

Responses	READ	UPDATE	CONTROL	ALTER	Total
All users via UACC					0
All users via ID(*)					0
Technical Support staff					0
System software products that also require this access to SUPERUSER.FILESYS					0
RACF Administrators with System-SPECIAL			1		1
Other					0
Total	**0**	**0**	**1**	**0**	

For the majority of your production z/OS systems, what is the SETROPTS LOGOPTIONS level for class FSSEC?

Responses	Count	Percent %
ALWAYS	6	28.6%
NEVER	0	0%
SUCCESSES	0	0%
FAILURES	1	4.7%
DEFAULT	14	66.7
Total	**21**	**100%**

Are you using REXX EXECs ORLIST, OPERMIT, and ORALTER provided by Bruce Wells of IBM for managing Unix file security?

Responses	Count	Percent %
Have not downloaded them	16	76.2%
Downloaded but not tried them	3	14.3%
Downloaded and tried them	2	9.5%
Downloaded and are using them	0	0%
Total	**21**	**100%**