

## Security Risk Assessment Checklist

The checklist number is string + number, where string represents the area of applicability.

Available areas:

- ALL - generic, applies to all hosts
- CE - for computing element host
- GIIS - for host running GIIS
- WN - worker node host
- VOMS - for host running VOMS server
- NFS - filesystem shared with NFS

Number	Description	Command	Correct setting or value	Comment
ALL1	check the CAs authorized i.e. latest IGTF distribution + correct crt fetching (cron job)			
ALL2	check IGTF distribution permissions			
ALL3	check the host certificate i.e. permission of the private key (only readable by root)			
ALL4	check the allowed users i.e. they should not have superuser privileges + cron.deny + at.deny (grid-users)			
ALL5	check clocks are synched			
ALL6	check logging (backlog and security) (x-check) -> to be implemented.			
ALL7	check open ports and what services are behind it. -> stop services which are not needed.			

CE1	check the permissions of the installation			
CE2	check the permissions of the daemons			
CE3	check the permissions of the jobs dirs (to prevent job output thefts)			
CE4	check the voms credentials i.e. VOMS certificate and its permissions			
CE5	check the VO information			
CE6	check the enabling of the lcas/lcmaps			
CE7	check the lcmaps plugins			
CE8	check limits → prevent downtimes from excessive resource usage (memory, disk, #files, ...)	limit, ulimit		
GIIS1	check the users allowed in (who is allowed on service and what role he/she has.)			
GIIS2	check filter for the SMSCG area			
UI1	check users allowed in			
UI2	check configured GIISes, VOs			

VOMS1	check users allowed in			
VOMS2	check mysql access			
VOMS3	check tomcat CAs (in case restart it)			
NFS1	check the read only settings for all the users but the special sga ones: check that it is limited to local LAN and all machines on local LAN are managed. (If you use another technology, check whether similar issue exists, e.g. lustre, afs, gpfs, ... ).			
WEB	Ensure web-servers and web-applications are up to date. (e.g. nessus and nikto -> low hanging fruits). Check only required ports are open.			
WN	check the users: only pool accounts should exist (varies depending on the site)			
Grid Users	ssh disabled. no password accounts -> config to deny password-less login.			