

**IG CHECKLIST
(DOIM Info Mgt – Info Mgt Op)**

Proponent/Phone No:	Information Management/2-1944	
Functional Area:	Information Management	
Program/Activity Topic:	Information Management Operations	
Date of Revision:	1 August 1999	
Management Control Checklist Applied:	<input type="checkbox"/> YES <input type="checkbox"/> NO <input checked="" type="checkbox"/> NA	
Unit Inspected:	Date Inspected:	
Inspector's Name:	Phone No:	
1. References.		
a. AR 25-1, 25 Mar 97, The Army Information Resources Management Program.		
b. AR 380-19, 27 Feb 98, Information Systems Security.		
c. USAFACFS Memo 25-72, 22 Jun 98, ADPE Procurement Security.		
2. Discussion: The purpose of this checklist is to identify to commanders/directors specific critical management areas of the information mission area function. It is further used as a uniform tool to assess the efficiency of the management of the information mission area at unit level.		
3. Questions.	YES	NO
a. Has commander/director appointed in writing one central point of contact to interact with DOIM on all IMA matters?		
b. Has commander/director appointed in writing an Information Systems Security Official (ISSO) (may be same as POC both must have separate duty appointment as ISSO)?		
c. Has commander/director appointed in writing an Activity Records Manager (may be same as POC but must have separate duty appointment as RMA)?		
Has commander/director required units/offices to turn in required records to the Records Holding Area?		
Has commander/director required units/offices to prepare and submit a files list to DOIM for approval?		
d. Has commander/director appointed in writing a Printing Control POC (may be same as POC but must have a separate duty appointment as Print Control POC)?		
e. Has commander/director appointed in writing an Official Mail Control Officer (OMCO) (may be same as POC but must have a separate duty appointment as OMCO)?		
f. Has commander/director appointed in writing a Publications POC (may be same as POC but must have separate duty appointment as publications POC)?		
g. Has commander/director appointed in writing a telephone control officer (may be same as POC but must have separate duty appointment as TCO)?		
h. Has commander/director assigned responsibility for--		
Completion of risk assessments for ADPE.		
Equipment accountability and physical security.		
Site license and copyright integrity for software.		
i. Has commander/director required that subordinates thoroughly justify the need to use privately-owned hardware or software?		

	YES	NO
j. Has commander/director restricted the use of personally-owned equipment for processing of unclassified material only?		
k. Has commander/director restricted the processing of classified material to equipment having an approved formal risk assessment from the appropriate accreditation authority?		
l. Has commander/director required that classified data be stored either on approved government-owned hard disks in areas approved by DPTM for open storage at the same level as the data being processed or on removable media?		
m. Has commander/director restricted the use of software utility packages to designated POCs or supervisors who are responsible for protection against copyright infringements?		
n. Has the commander/director ensured no games are present on government computers?		
o. Has commander/director developed, implemented, and maintained procedures to strictly control usage of site licensed software for which they are licensed and adhered to control procedures for site licensed software obtained from another licensee?		
p. Has commander/director required subordinates to use only freeware/shareware obtained from appropriated sources (i.e., U.S. Log Center, Navy Research and Development Automation Center (NARDAC), and the Information Systems Command Information Systems Engineering Center (ICS-ISEC))?		
q. Have commander/director established procedures to ensure the physical safeguarding of all automation equipment (i.e., notebooks, computers, printers, etc.)?		
4. REMARKS:		