Infrastructure Name:	EGI					Version 3
Prepared By:	David Kelsey			**On Date:**	06-May-13	17-Jan-13
Reviewed By:	<insert name>			**On Date:**	<insert date>	
Operational Security [OS]	**Maturity**	**Evidence (Document Name and/or URL)**	**Version Number**	**Document Date**	**Document Page or Section Number**	**Comments**
OS1 - Security Model	1					Not really documented. EMI architecture?
OS1.1 - Authentication	1					X.509 PKI
OS1.2 - Authorisation	1					VOMS, Grid mapfile, Argus, SCAS, LCAS
OS1.3 - Access Control	1					Based on AuthN and AuthZ. CRLs for revocation
OS1.4 - Confidentiality	0					An EDG requirement
OS1.5 - Integrity	0					An EDG requirement
OS1.6 - Availability	0					An EDG requirement
OS1.7 - Compliance Mechanisms	2	Top-level Security Policy			Section 6	
OS2 - Security Patching						
OS2.1 - Patching Process	2	Service Operations Security Policy				
OS2.2 - Patching Records & Communication	1? 2?					Pakiti monitoring, Security dashboard
OS3 - Vulnerability Mgmt						
OS3.1 - Vulnerability Process	2	EGI SVG procedures				
OS3.2 - Dynamic Response	2	SVG and CSIRT procedures				SVG RAT can assess anything - otherwise CSIRT
OS4 - Intrusion Detection	0					But some sites do this
OS5 - Regulate Access	2	Top-level Security Policy			section 2.5.4	
OS6 - Contact Information						
OS6.1 - Contact Users	2	VO Membership Management Policy				
OS6.2 - Contact Service Providers	2	Service Operations Security Policy				
OS^.3 - Contact Resource Providers	2	Service Operations Security Policy				
OS7 - Policy Enforcement						
OS7.1 - Enforcement	2	Top-level Security Policy				
OS7.2 - Escalation Procedure	1?					Is this documented?
OS7.3 - Emergency Powers	1?					Is this documented?
Incident Response [IR]						
IR1 - Contact Information						
IR1.1 - Contact Service Providers	2	Service Operations Security Policy				
IR1.2 - Contact Resource Providers	2	Service Operations Security Policy				
IR1.3 - Contact Communities	2	VO Membership Management Policy				
IR1.4 - Expected Response Times	1?					Does OLA specify this?
IR2 - Incident Response Procedure						
IR2.1 - IR Roles & Responsibilities	2	ee Incident Response Policy and Procedures				
IR2.2 - IR Identification & Assessment	2	ditto				
IR2.3 - IR Minimizing Damage	2	ditto				
IR2.4 - IR Response & Recovery	2	ditto				
IR2.5 - IR Communication Tools	2	ditto				
IR2.6 - IR Procedures	2	ditto				
IR3 - IR Collaboration						
IR3.1 - Internal Collaboration	2	ee Incident Response Policy and Procedures				
IR3.2 - External Collaboration	2	egistered under TERENA Trusted Introducers				
IR4 - information Sharing Restrictions	2	rusted Introducer and Traffic lights scheme				
Traceability [TR]						
TR1 - Traceability						
TR1.1 - Production of Logs	2	Traceability policy				Do we have procedures?
TR1.2 - Retention of Logs	2	Traceability policy				
TR2 - Data Retention	2	Traceability policy				
TR3 - Traceability Controls	0					What should this include?
Particpant Responsibilities [PR] - Individual Users						

PR1 - AUP	2	See User AUP				
PR1.1 - Defined Acceptable Use						
PR1.2 - Non-Acceptable Use						
PR1.3 - User Registration						
PR1.4 - Protection & Use of Credentials						
PR1.5 - Data Protection & Privacy						
PR1.6 - IPR						
PR1.7 - Disclaimers						
PR1.8 - Liability						
PR1.9 - Sanctions						
PR2 - User Awareness & Agree	2	VO Membership Management Policy				AUP accepted during registration with VO
PR2.1 - User Awareness						
PR2.2 - User Agreement						
PR3 - Communication of extra requirements						
Particpant Responsibilities [PR] - Collections of Users						
PR11 - Policy Awareness	2	VO Membership Management Policy				
PR11.1 - Awareness						
PR11.2 - Abide by						
PR12 - User Registration & Management	2	VO Membership Management Policy				
PR12.1 - User Registration						
PR12.2 - User Renewal						
PR12.3 - User Suspension						
PR12.4 - User Removal						
PR12.5 - User Banning						
PR13 - Responsibility for Actions						
PR14 - User Identification - traceability						
PR15 - Logs of Membership Management Actions	2	VO Membership Management Policy				
PR16 - Define Common Aims & Purposes	2	VO Registration Policy				
Particpant Responsibilities [PR] - Resource Providers and Service Operators						
PR21 - Vulnerability Patching	2	Service Operations Security Policy				
PR22 - Incident Reporting	2	Service Operations Security Policy				
PR23 - Physical and Network Security	2	Top-level Security Policy				
PR24 - Confidentiality and Integrity of Data	0					Is this addressed? Where?
PR25 - Retention of Appopriate Logs	2	Traceability policy				
Legal Issues [LI]						
LI1 - Intellectual Property Rights	2	EGI OLA				
LI2 - Liability, Responsibilities & Disclaimers	2	Top-level Security Policy				And OLA?
LI3 - Software Licensing	2	Service Operations Security Policy				And VO Operations?
LI4 - Dispute Handling and Escalation	2	Top-level Security Policy				
LI5 - Data Protection Responsibilities	1					Not properly addressed
LI6 - Any Additional Restrictions	0					Are there any?
Protection and Processing of Personal Data [DP]						
DP1 - Accounting Data	2	Accounting data policy				
DP2 - User Registration Data	2	VO Membership Management Policy				
DP3 - Monitoring Data	0					Not yet?
DP4 - Logging Data	0					Not yet?
DP5 - User Personal Data	0					Not yet?
Assessment Score						
Raw Score						
Weight						