Workload Manager Risk assessment

List of risks

Risk no	Risk description	Threat
1	Service unavailable / loss of data due to hardware failure	hardware failure
2	Service unavailable / loss of data due to software failure	software errors (stack/dead processes, hard disk full because log files, ...)
3	service unavailable / loss of data due to human error	human error: staff not well aware/trained about service and procedures, lacking of documentation, patching/upgrading procedures not properly followed, ...
4	service unavailable for network failure (Network outage with causes external of the site)	network outage
5	Not enough people for maintaining and operating the service	Unavailability of key technical and support staff (holidays period, sickness, ...)
6	Major disruption in the data centre.	Fire, flood, failure or disruption of the power supply , natural disasters, environmental disaster, major events in the environment,
7	Major security incident. The system is compromised by external attackers and needs to be reinstalled and restored.	Software vulnerabilities, identity theft, unauthorised access
8	(D)DOS attack. The service is unavailable because of a coordinated DDOS.	Denial of service attack

Risks rating criteria

In order evaluate the level of a risk, it is first assessed its likelihood and impact. Both of them are integers between 1 and 4 (inclusive):

Rating	Likelihood	Impact
1	Unlikely to happen	Minimal impact
2	Happens less than once per year	Minor impact, local service disruption less than 1 week
3	Happens every few months / more than once per year	Serious disruption for multiple users, more than a week
4	Happens every 2-3 months or more frequently	Serious disruption to the ability to deliver service

Then the risk level is given by the product of Likelihood and Impact (from 1 to 16), and the risks are prioritised in the following way:

- Low: 1 and 2
- Medium: 3 and 4
- High: 6, 8, and 9
- Extreme: 12 and 16

Likelihood	**Impact**			
	1 - Minimal impact	**2 - Minor impact, local service disruption less than 1 week**	**3 - Serious disruption for multiple users, more than a week**	**4 - Serious disruption to the ability to deliver service**
1 - Unlikely to happen	(1) Low	(2) Low	(3) Medium	(4) Medium
2 - Happens less than once per year	(2) Low	(4) Medium	(6) High	(8) High
3 - Happens every few months / more than once per year	(3) Medium	(6) High	(9) High	(12) Extreme
4 - Happens every 2-3 months or more frequently	(4) Medium	(8) High	(12) Extreme	(16) Extreme

Risk no 1

Risk description	Service unavailable / loss of data due to hardware failure
Affected components of the service	All the service components
Threats	hardware failure
Consequences of risk occurrence	Temporary service inavailability. Failures of some user jobs already submitted to the system. Loss of some logging information.
Established measures	Reactive countermeasure: Data protection with daily backups (6 months retention) of the entire database and on-the-fly backup of the binary logs. Regular snapshots of virtual machines hosting DIRAC4EGI services. MySQL Database restoring from daily backups; point in time recovery, if needed, from binary logs backups. VM servers restored from snapshots.
Identified / remaining vulnerabilities	The main vulnerability is the MySQL database provided as a service by CC-IN2P3
Likelihood	1 - Unlikely to happen
Impact	3 - Serious disruption for multiple users, more than a week
Risk level	(3) Medium
Treatment - Protective/mitigation measures - recovery activities - controls	the measures already in place are considered satisfactory and risk level is acceptable
Expected duration of downtime/ time for recovering	1 working day after the hardware faiure recovery

Risk no 2

Risk description	Service unavailable / loss of data due to software failure
Affected components of the service	All the service components
Threats	software errors (stack/dead processes, hard disk full because log files, ...)
Consequences of risk occurrence	Temporary service inavailability.
Established measures	Reactive countermeasure: Data protection with daily backups (6 months retention) of the entire database and on-the-fly backup of the binary logs. MySQL Database restoring from daily backups; point in time recovery, if needed, from binary logs backups.
Identified / remaining vulnerabilities	Mysql Database for the affected component.
Likelihood	2 - Happens less than once per year
Impact	2 - Minor impact, local service disruption less than 1 week
Risk level	(4) Medium
Treatment - Protective/mitigation measures - recovery activities - controls	the measures already in place are considered satisfactory and risk level is acceptable
Expected duration of downtime/ time for recovering	1 working day

Risk no 3

Risk description	service unavailable / loss of data due to human error
Affected components of the service	All the service components
Threats	human error: staff not well aware/trained about service and procedures, lacking of documentation, patching/upgrading procedures not properly followed, ...
Consequences of risk occurrence	Temporary service inavailability.
Established measures	Reactive countermeasure: Data protection with daily backups (6 months retention) of the entire database and on-the-fly backup of the binary logs. MySQL Database restoring from backups for affected components. Restoring Configuration data from backups.
Identified / remaining vulnerabilities	Mysql Database for the affected component.
Likelihood	2 - Happens less than once per year
Impact	2 - Minor impact, local service disruption less than 1 week
Risk level	(4) Medium
Treatment - Protective/mitigation measures - recovery activities - controls	the measures already in place are considered satisfactory and risk level is acceptable
Expected duration of downtime/ time for recovering	1 working day

Risk no 4

Risk description	service unavailable for network failure (Network outage with causes external of the site)
Affected components of the service	All the service components
Threats	network outage
Consequences of risk occurrence	Temporary service inavailability. low risk of a loss of results of already running user jobs
Established measures	Preventive countermeasure: Geographically distributed redundant Configuration Service. Redundant failover Request Management Service. Failover mechanism for recovering job outputs.
Identified / remaining vulnerabilities	Running payloads under the DIRAC Workload Management control
Likelihood	2 - Happens less than once per year
Impact	1 - Minimal impact
Risk level	(2) Low
Treatment - Protective/mitigation measures - recovery activities - controls	the measures already in place are considered satisfactory and risk level is acceptable
Expected duration of downtime/ time for recovering	1 hour after the network recovery

Risk no 5

Risk description	Not enough people for maintaining and operating the service

Affected components of the service	Resources management. User support. Security infrastructure components
Threats	Unavailability of key technical and support staff (holidays period, sickness, ...)
Consequences of risk occurrence	Some computing and storage elements can be unavailable due to the lack of timely intervention. Changes in the security infrastructure components not timely reflected, e.g. changing VOMS server certificates. User problem reports answered slowly.
Established measures	Preventive countermeasure: Automation of synchronization with BDII, VOMS, GocDB information indices. Automated resource monitoring service. Training multiple system administrators. Involving new participants to the service administration group.
Identified / remaining vulnerabilities	No timely reaction to the user reported problems
Likelihood	2 - Happens less than once per year
Impact	1 - Minimal impact
Risk level	(2) Low
Treatment - Protective /mitigation measures - recovery activities - controls	the measures already in place are considered satisfactory and risk level is acceptable
Expected duration of downtime/ time for recovering	1 or more working days

Risk no 6

Risk description	Major disruption in the data centre.
Affected components of the service	All the service components
Threats	Fire, flood, failure or disruption of the power supply , natural disasters, environmental disaster, major events in the environment, ...
Consequences of risk occurrence	Temporary service inavailability. Definite loss of important databases, most notably File Catalogs.
Established measures	Reactive countermeasure: Daily backups (6 months retention) of the entire database and on-the-fly backup of the binary logs. Regular snapshots of virtual machines hosting DIRAC4EGI services. Reestablinshing services in a different hosting environment. Restoring databases from backups if still available. Partial restoring of the File Catalogs contents from the storage elements information.
Identified / remaining vulnerabilities	Everything will be affected
Likelihood	1 - Unlikely to happen
Impact	4 - Serious disruption to the ability to deliver service
Risk level	(4) Medium
Treatment - Protective/mitigation measures - recovery activities - controls	the measures already in place are considered satisfactory and risk level is acceptable
Expected duration of downtime/ time for recovering	several weeks

Risk no 7

Risk description	Major security incident. The system is compromised by external attackers and needs to be reinstalled and restored.
Affected components of the service	All the service components
Threats	Software vulnerabilities, identity theft, unauthorised access
Consequences of risk occurrence	Temporary service inavailability.
Established measures	Reactive countermeasure: Daily backups (6 months retention) of the entire database and on-the-fly backup of the binary logs. Regular snapshots of virtual machines hosting DIRAC4EGI services. Reinstalling service components with the configuration restored from backups. Changing security tokens (logins, passwords) for accessing the service servers and databases. Assume that the database service is not affected, otherwise restoring the databases from backups.
Identified / remaining vulnerabilities	Services hosted on a compromised server
Likelihood	1 - Unlikely to happen
Impact	2 - Minor impact, local service disruption less than 1 week
Risk level	(2) Low
Treatment - Protective /mitigation measures - recovery activities - controls	the measures already in place are considered satisfactory and risk level is acceptable
Expected duration of downtime/ time for recovering	1 or more working days

Risk no 8

Risk description	(D)DOS attack. The service is unavailable because of a coordinated DDOS.
Affected components of the service	All the service components
Threats	Denial of service attack
Consequences of risk occurrence	Temporary slow or no access to the service components. mailnly the Service Web Portal
Established measures	Preventive countermeasure: Limited service queries queues avoiding dangerous overloading of the service components. Automatic service restart after going down due to an overload. Automatic recovery after the end of the DOS attack.
Identified / remaining vulnerabilities	Service Web Portal
Likelihood	1 - Unlikely to happen
Impact	1 - Minimal impact
Risk level	(1) Low
Treatment - Protective/mitigation measures - recovery activities - controls	the measures already in place are considered satisfactory and risk level is acceptable
Expected duration of downtime/ time for recovering	1 hour

Risk No 9

Risk description	Resource Centres unavailability
Affected components of the service	None
Threats	The WMS can not connect to sites providing computing resources
Consequences of risk occurrence	Users actions blocked or delayed or running at reduced capacity
Established measures	Reactive countermeasure: Regular update of site administrators contact information. Once the risk occurs, WMS admins will contact the site administrators to solve the unavailability.
Identified / remaining vulnerabilities	Site certificates outdated. CE or SE temporary unavailability or decommission.
Likelihood	2 - Happens less than once per year
Impact	2 - Minor impact, local service disruption less than 1 week
Risk level	(4) Medium
Treatment - Protective/mitigation measures - recovery activities - controls	the measures already in place are considered satisfactory and risk level is acceptable
Expected duration of downtime/ time for recovering	1 or more working days depending on the site administrators response time