WLCG Computer Security Risks Analysis

Dave Kelsey <d.p.kelsey@rl.ac.uk>
Maarten Litmaath <Maarten.Litmaath@cern.ch>
Steffen Schreiner <Steffen.Schreiner@cern.ch>
Von Welch <vwelch@indiana.edu>
Romain Wartel <Romain.Wartel@cern.ch>
John White <John.White@cern.ch>
Christoph Witzig <christoph.witzig@switch.ch>
And the members of the WLCG Security Technology Evolution Group

Version	Date	Author	Comment
0.1	22 November 2011	Romain Wartel	Initial version
0.2	1 December 2011	Romain Wartel	Added new sections
0.3	5 December 2011	Romain Wartel	Added new sections
0.4	7 December 2011	Romain Wartel	Updated during the Security TEG face-to-face meeting
0.5	12 December 2011	Romain Wartel	Added text in the compromised identities section
0.6	13 December 2011	Romain Wartel	Integrated corrections from Maarten Litmaath
0.7	16 January 2012	Romain Wartel	Integrated input from Claudio Grandi, Ursula Epting, Leif Nixon, Igor Sfiligoi, Von Welch, Christoph Witzig.
0.8	31 January 2012	Romain Wartel	Updated following the Security TEG face-to-face meeting
1.0	05 March 2012	Romain Wartel	Added text on the data integrity risk (#10)
1.1	19 March 2012	Romain Wartel	Integrated input from Denise Heagerty

Table of Content

Introduction

Risk management is a key aspect of computer security, as it enables any project or infrastructure to evaluate the different threats they may suffer damage from, and to prioritise and focus the efforts necessary to manage the resulting risks. It is essential indeed to understand what it is important to protect a project or an infrastructure from, before defining what security mechanisms are needed, or if a given security mechanism is worth its cost.

This public document aims at managing the security risks affecting the WLCG collaboration. While WLCG may be affected by a number of security risks of a very different nature, the scope of this document is limited to the computer security risks stemming from malicious intents.

The authors also acknowledge the possibility of attacks conducted by insiders. This however does not result in significantly different risks or different recommendations. As a result, in the context of this risk assessment, insider attacks are not treated as a separate threat, but rather as an aggravating factor to most of the identified risks.

An important aspect of this approach is to propose balanced and cost-effective recommendations. Security has a cost and therefore the goal must be to implement those measures that increase the security while abstaining from introducing unnecessary ones.

There are many different methods and industry standards, for example the ISO/IEC 27000-series, available to conduct risk assessments. The WLCG collaboration has a rather unique configuration, and although this document uses many concepts described in well known standards, it follows a more tailored and focused approach on WLCG risks. The exact boundaries of a service or a resource are for example sometimes not defined in WLCG and, being a collaboration spanning many resources across multiple administrative domains and countries, the notion of control (e.g. over the resources) is often very different than in most traditional infrastructures and corporations.

Taking these aspects into account, the risks are being evaluated and managed through this document based on the following approach:

1. Expose details about the computing environment: incident response and media interest
2. Define the assets in WLCG
3. Identify threats to these assets
4. Assign a likelihood and an impact for each threat. The resulting number is the risk.
5. Manage the most important risks and attempt to mitigate them
6. Understand the residual risks after mitigation

Ultimately, one of the main objectives is to provide a number of recommendations linked to or within this document to reduce the risks and propose improvements to the security framework for the WLCG participants, including security operations and software lifecycle.

Incident response and publicity

1. Understanding and containing security incidents

The impact of security incidents on WLCG depends on the degree of compromise, but also heavily on the degree of traceability implemented on the affected services and resources. Traceability is often defined as the ability to chronologically interrelate the uniquely identifiable entities in a way that matters, and enables the security team to identify the cause, the timeline, and the extent of a security incident. If, for example, an incident occurs because of a compromised user credential, it is essential to be able to tell exactly *which* credential is compromised, so the security teams can revoke it and hopefully determine the reason of the compromise.

Traceability is an extremely important aspect of computer security, and most incidents whose cause could not be determined will most likely re-occur within the next months.

Traceability is a key element to incident response and a sufficient level of traceability is essential to protect WLCG against misused identities and keeping services operational.

In particular, the WLCG Grid Security Traceability and Logging Policy states that:

> *"Identifying the cause of incidents is essential to prevent them from re-occurring. In addition, it is a goal to contain the impact of an incident while keeping services operational. For response to incidents to be acceptable this needs to be commensurate with the scale of the problem.*
>
> *The minimum level of traceability for Grid usage is to be able to identify the source of all actions (executables, file transfers, pilot jobs, portal jobs, etc) and the individual who initiated them. In addition, sufficiently fine-grained controls, such as blocking the originating user and monitoring to detect abnormal behaviour, are necessary for keeping services operational. It is essential to be able to understand the cause and to fix any problems before re-enabling access for the user.*
>
> *The aim is to be able to answer the basic questions who, what, where, and when concerning any incident. This requires retaining all relevant information, including timestamps and the digital identity of the user, sufficient to identify, for each service instance, and for every security event including at least the following: connect, authenticate, authorize (including identity changes) and disconnect."*
> *(https://edms.cern.ch/document/428037)*

In addition to enable the investigation of security incidents and to trace their initial source, traceability is also required to fulfil legal requirements in some jurisdictions.

Containment is also an important aspect, and aims at preventing incidents from spreading to multiple systems and/or user identities. Containment and traceability are related, in that actions that improve containment tend to also improve traceability, and vice versa.

As explained in the next sections, it is also necessary to assume, as part of normal operations, that a small portion of WLCG identities are always compromised.

2. Publicity and press impact arising from security incidents

The computer security aspects related to any large organisation or project are usually a great topic of interest for the media, in particular when security fails (incidents, compromises). In addition, as any large international science project, WLCG and its participants are periodically drawing attention from the media.

Most organisations typically do not communicate on their security policies or procedures. Discussing security incidents publicly is a strong taboo in the industry, although most computing infrastructures are confronted to security incidents on a regular basis.

In WLCG, security incidents are treated as part of normal operations, and all WLCG security policies and procedures are public. Detailed security incidents statistics, as well as the main causes of security incidents are reported on a regular basis during workshops and conferences. However, during a security incident, the security teams of WLCG all collaborate to resolve the incident and protect the privacy and reputation of the affected parties (users, organisation).

This deliberately incomplete information flow, added to the technical complexity of the computer infrastructure used by WLCG, may lead the media to report either incomplete or incorrect information about a given security incident, in particular on its actual impact on the infrastructure.
It is also very common that the actual impact of a given security incident affecting an organisation is significantly exaggerated in the media, or that regular or low severity incidents are presented as exceptional and serious occurrences. Once an article containing erroneous or inaccurate information has been published in the press, experience shows these it is extremely difficult to manage or to correct.

In general, managing negative events in the press is extremely difficult and there is very often a negative impact on the reputation of the parties affected.

As a result, the negative impact of publicity and press that exists irrespectively of the accuracy of the information being published, is an additional aggravating factor for each of the risks presented above.

Assets

An asset is a useful or valuable quality or resource to the collaboration. Assets play a key role, as they define what the collaboration is aiming at protecting with the security policies, procedures and controls it has implemented. Evaluating the benefits of any security measure should be done by evaluating how good it is at protecting one or more assets.

The WLCG collaboration includes a number of assets, both intangible (for example its reputation) and tangible (for example its data resources). The table below lists the main assets of the collaboration. It is the goal of the security teams to protect these assets.

Asset	Comments
Trust / collaboration	The trust established between WLCG participants, collaborating infrastructures, external partners and funding agencies, needs to be maintained
Reputation	Reflects the opinion of the general public, funding agencies and participants about WLCG
Intellectual property	It includes both copyrighted material and the result of scientific work conducted on WLCG resources
Data protection	The protection of the data (e.g. personal) collected by, stored at and handled by WLCG resources.
Digital identities	Includes both the credentials and the attributes enabling the authentication and authorization of users and services.
CPU resources	Physical or virtual entities that are consumed through services to enable calculations to be conducted, for example worker nodes
Data resources	Physical or virtual entities that are consumed through services to enable LHC data to be stored
Network resources	Network facilities enabling the different WLCG participants to cooperate and users to access WLCG resources
Services	A service is any computing or software system, which provides access to, information about, or controls tangible assets. This includes the services necessary to the usage, support, operation, monitoring of WLCG as well as the communication and dissemination within and outside the collaboration, such as websites, wikis, etc.
Data integrity	The accuracy, lack of alteration and consistency of stored data (for example scientific data) on WLCG resources

Throughout the rest of the document, resources will refer to CPU, Data and Network resources.

Threats

A threat is defined in the following table as a potential event stemming from a malicious intent and inflicting harm or loss to a previously defined asset.

The experience from operations shows that threats are often combined, and that the realisation of one given threat may significantly increase the likelihood or impact of another threat. During the current analysis, the threats are treated as separate and independent.

Threat	Comments	Most affected assets
Misused identities	Identities that have been compromised (silently or detected)	Trust / collaboration, Reputation, Digital identities
Attack propagation between WLCG sites	Single Sign-On infrastructures are prone to internal attack propagation	Trust / collaboration, Digital identities, CPU resources, Data resources
Negative publicity on a non-event	Press or news articles on a non-event	Trust / collaboration, Reputation
Incidents on resources not bound by WLCG policies	In particular external and private cloud infrastructures	Digital identities, Reputation
DoS from an external organisation	A Botnet or external resources may attempt to disrupt WLCG services	Network resources, CPU resources, Data resources
Data removal/corruption/alteration	Focuses in particular on the integrity of user data	Intellectual property, Data integrity
Exploitation of a serious VO/ middleware software vulnerability	Software provider needs to manage vulnerabilities in its software	Trust / collaboration, Reputation, Services
Exploitation of a serious OS vulnerability	WLCG security depends on the security of the OS it relies on	Digital identities, Services
Insecure configuration leading to undesirable access	For example, a local administrator exposes a service accidentally	Digital identities, CPU resources, Data resources, services, Data protection
Insufficient protection of information leading to sensitive data leakage	This includes scientific data, personal or sensitive information	Trust / collaboration, Reputation, Intellectual property, Data integrity, Data protection
Threats originating from trust services	Compromised services may include a CA, MyProxy, OpenID, IdPs, etc.	Trust / collaboration, Digital identities, services

Evaluation of the risks

Based on the threats and assets defined previously, it is possible to assign a likelihood and impact for each occurrence.

The **likelihood** is based on an estimate of the number of expected events per year, mapped to a scale from 1 to 5.
The **impact** is an estimation of the damage that the event would typically cause to the collaboration, from a scale ranging from 1 to 5, where 1 refers to non-significant damage and 5 refers to very serious damage:

1. Minimal impact on WLCG's ability to deliver its services to users
2. Minor impact, operational or financial costs, or local service disruption for less than a week
3. Serious localised disruption of some WLCG services for some users, for a week or more, leading to a productivity loss, or significant financial or operational costs
4. Serious global disruption of some WLCG services to all users, for a week or more, leading to a productivity loss, or significant financial or operational costs
5. Very serious disruption, where WLCG is unable to deliver services to its users, for a week or more, or suffers risk to its funding or other business continuity issue

The estimation of the impact has been conducted based on the experience from past security incidents in or outside the collaboration and does not necessarily reflect a worse case scenario.

The risk is then calculated for each threat based on the following equation:

Risk = Impact x Likelihood

Impact \ Likelihood	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25

This enables the following risk scale to be defined:

Threat	Likelihood	Impact	Risk
Misused identities			**15**
Category 1 credentials (as defined in "Management of the risks")			
Privileged user	2	4	**8**
Larger number of unprivileged users	2	5	**10**
Small number of unprivileged users	5	**3**	**15**
Category 2 credentials (as defined in "Management of the risks")			
Privileged user	1	4	**4**
Larger number of unprivileged users	2	5	**10**
Small number of unprivileged users	2	**3**	**6**
Attack propagation between WLCG sites	**3**	4	**12**
Exploitation of a serious OS vulnerability	4	**3**	**12**
Threats originating from trust services	2	4	**8**
Negative publicity on a non-event	2	4	**8**

Threat	Likelihood	Impact	Risk
Insecure configuration leading to undesirable access	**3**	2	**6**
Insufficient protection of information leading to sensitive data leakage	**3**	2	**6**
Incidents on resources not bound by WLCG policies	1	**4**	**4**
Exploitation of a serious VO/middleware software vulnerability	2	2	**4**
Data removal/corruption/alteration	1	**3**	**3**
DoS from an external organisation	1	1	**1**

Management of the risks

1. Misused identities

Risk score: 15 / 25

Compromised identities

Compromised identities may be very difficult to detect and remain undiscovered in the infrastructure for an extended period of time, enabling the attacker to silently propagate its attack further. The ability for the attacker to demonstrate determination and patience has become common, in particular in the context of so-called advanced persistent threats (APT).

The severity of the attacks resulting from compromised identities varies depending on multiple factors, including the roles and number of compromised identities. However, this issue constitutes an important risk for WLCG and many security measures and procedures have been and are being implemented to mitigate this risk. Experience from the recent years has shown that compromised identities are the most common intrusion vector for the security incidents that have affected WLCG. Attackers often initially capture credential on a weak service before propagating their attack further within our infrastructure by reusing the stolen credentials.

Any credential that can be copied (typically password and keys) by an attacker is prone to be compromised and harvested. Many public tools enable password collection or SSH private key harvesting and this particular issue is one the main intrusion vectors in most computing infrastructures.

The WLCG collaboration relies mainly on two main authentications realms: a public key infrastructure (X509 PKI) and traditional client/server authentication (e.g. username/password for SSH).

An important aspect of credentials protection and management depends on the typical deployment scenario they are used in, rather than on the authentication realm. For example, enabling x509 to authenticate against SSH would most likely not lead to a reduction of the number of SSH incidents. As a result, two different categories of deployment have been identified:

- **Category 1**: Where services accepting the credentials are directly accessible to an attacker, for example username/password used to connect to an Internet service like SSH.
- **Category 2**: Where services accepting the credentials are not directly available to an attacker. Multiple ingredients are needed to obtain credentials to authenticate. For example, the grid certificate of a user, accessible only on a host whose access requires SSH authentications with different credentials.

In WLCG, Category 1 is typically used for SSH authentication to User Interfaces (UI), or to authenticate to grid portals. Category 2 is typically used by end users to generate a proxy certificate from their X509 certificate, or by privileged services (e.g. Apache) to authenticate end users via X509.

The experience shows that credentials of the Category 1 (e.g. SSH passwords, etc.) are currently the main target of attackers, and that efforts to reduce the number of compromised identities should focus in priority on this category.

A number of malware currently implement Session or TTY hijacking mechanisms designed to steal open sessions of the victim. The attack happens after the victim has authenticated and does not depend on the quality of the authentication (multi-factor, biometric, etc.). The limiting factor is that the attacker must have privileged access on the system, hence hardening and keep the host up to date with security patches is essential.

Given the large scale of WLCG operations, security & operation teams as well as software developers needs to assume a small portion of the users are compromised at any point in time. Incidents and compromised identities are part of normal operations and the WLCG services and procedures should be designed to prevent significant service outage when they occur.

Misused resources

Attacks against the infrastructure used by WLCG are often relying on compromised identities (see next section). It can also happen that a legitimate user has become malicious. Either way, compromised identities (for example, SSH credentials or X509 private keys) are a frequent occurrence and part of normal operations and have to be constantly been dealt with on a thorough and professional manner. Most of the identities that have been compromised usually become misused in a short period of time.

Misused identities are typically used by attackers as a vector to deploy a malicious payload on WLCG services or resources. The payload may either be a mean for the attacker to propagate its attack or provide direct benefit.
Benefits for the attackers focus usually around money, including re-selling CPU time, data or network access, or simply calculation results (e.g. Bitcoin data mining). Ego and fame are also very common motivation for the attacker.

Whenever misused identities are reported or detected, the WLCG security teams follow the pre-established incident response procedures aimed at:

- Informing all WLCG services or resources owner
- Containing the incident
- Reconstructing the event and its timeline
- Proposing means to prevent similar incidents to re-occur

Attack against or from external resources

Attacks affecting WLCG resources often come from computing resources outside of the WLCG collaboration. This constitutes additional challenges to the security teams, as it is often more difficult to understand the root cause of the compromises when the attack started outside the collaboration. Experience shows that closely collaborating with the appropriate security teams or organisations outside the collaboration can greatly increase the ability to reconstruct the incidents that started outside WLCG and therefore help protect the collaboration.

The security practices of computing resources outside WLCG may also be much lower than within WLCG and put the credentials of WLCG users at risk, subsequently leading to compromised identities.

Incidents occurring within WLCG may also impact external resources when the attacker attempts to propagate its attack from WLCG services or resources to external organisations. This can lead to an increase of existing risks or to additional risks or costs, as the external organisations affected may seek financial or legal action against WLCG. In all cases, incidents involving external resources are significantly increasing the likelihood of media interest and of damage to the reputation of WLCG.

Malicious privilege escalation

During an ongoing attack, it is very frequent that attackers attempt to gain administrative privileges, in order to capture further credentials of other users of the compromised system. The captured credentials may either give access to the compromised system via a different user, or enable the attacker to propagate its attack to other resources (by capturing the credentials used by a local user on the compromised system to connect to remote hosts).

When an attack involves privilege escalation on a shared system, it is almost guaranteed that multiple identities will be compromised. As an additional side effect, the initial infection vector is likely to be more difficult to identify for the investigator (for example, privileged users may temper with the system, logs, etc.).

Privilege escalation is a significant aggravating factor reducing the ability to contain and resolve the security incidents. As a result, it is essential that all WLCG services or resources are securely configured, hardened and follow appropriate procedures to reduce the risk of privilege escalation to a minimum.

Security controls

The prompt management of compromised identities is an essential element of security in WLCG. Whenever a compromised identity is detected, it must be blocked and its access to the resources must be blocked as well.

WLCG has a large number of resources, involving a number of different services with different control mechanisms. Time being a critical parameter when controls are applied, it is important for all WLCG services to implement central blocking mechanisms, both central to the resource, and central to WLCG. The goal is to enable the resource security teams and WLCG security teams to block a given identity in an automatic and timely manner across all the resources they are responsible for.

2. Attack propagation between WLCG sites

Risk score: 12 / 25

WLCG services or resources enable authenticated and authorized users to perform actions transparently across the entire infrastructure. In most cases, the user can choose and execute almost any binary, either via a grid job (X509 realm), or by obtaining a full shell (SSH realm). From the security point of view, this translates into enabling arbitrary remote code executions for the WLCG users. Although this functionality enables the necessary flexibility required by scientists to conduct their work, it creates specific risks that needs to be managed.

From the experience gained through the attacks observed in the recent years in the academic community, most of the attackers attempt to propagate their attack further to other organisations or external systems. In the majority of the cases, this is done by exploiting the existing privileges, credentials and accounts of the compromised identity.

And typically, due to the nature of their collaborative work and shared interests, WLCG users have accounts or use the same federated account to access resources in multiple organisations. Once their identity has been compromised, it is often quite easy for the attacker to gain unauthorized access to further resources.

As a result, security teams in WLCG observe that many of the attacks they suffer from originate from a partner site, and as soon as a compromised identity has been detected at a given service or resource, the likelihood that another service or resource provider in WLCG is compromised is quite high.

Incident response in a scenario where the affected service or resource providers are all part of WLCG is easier to manage, as all WLCG participants are bound by the same WLCG policies and procedures, enabling them to share technical information and collaborate freely in order to resolve the incident.

3. Exploitation of serious OS vulnerabilities

Risk score: 12 / 25

The Operating System used by the service or resource providers play a critical role in the security of WLCG. They implement important parts of the security policies, for example authentication or traceability. By definition, operating systems include many components with low level and high privileges and it is very common for these components to be affected by serious software vulnerabilities.

It is very common that these vulnerabilities are used to either gain unauthorized access to an affected resource, or to enable

malicious local users (typically in the context of compromised identities) to gain privileges on the affected system, thus compromising the security of the vulnerable systems and of parts of the computing infrastructure used by WLCG.

Typically, attackers start harvesting credentials shortly after privileged access has been gained in order to propagate the attacker further, and experience shows that unpatched known software vulnerabilities is the main cause of privilege escalation in WLCG.

There are a number of aggravating factors:

- The severity assessment scale typically used by the operating systems vendors is rarely in-line with the scale used by WLCG security teams. As a result, some potentially serious vulnerabilities for WLCG might be treated with a lower level of priority by the vendors, which may bring additional delay the release of the security update or patch, and expose WLCG services or resources for a longer period of time
- It is a challenge for sites to keep up-to-date with security patches and the security teams dedicate significant efforts to monitor the patching status of each sites

4. Threats originating from trust services

Risk score: 8 / 25

WLCG relies on a number of trust services, handling for example sensitive information or credentials, in order to operate. Such services include for instance certificate authorities, MyProxy, VOMS, Kerberos or OpenID services.

Trust services are often high value targets for attacker and may constitute a single point of failure for any infrastructure, in particular with regards to the authentication and authorization systems. The delegation process used by several WLCG components enables the infrastructure to cope with a short unavailability of the corresponding service. However, it is necessary to consider the possibility that the trust services WLCG relies on become compromised.

5. Negative publicity on a non-event

Risk score: 8 / 25

The Large Hadron Collider and the WLCG collaboration are large, complex and unique infrastructures, whose specification numbers far exceed what is generally encountered by the general public. Such an environment often attracts attention from the media, on both positive and negative events. In the computer security field, experience shows there is a risk that reporters seeking a sensational or spectacular story publish an article about a non-event. The non-event may either be a minimal impact security incident blown out of proportion, or an event that has simply not happened at all.

Such a situation can affect any large organisation and is always difficult to manage, as it is often extremely difficult to prove the non existence of an event. The media and public generally assume the organisation is hiding facts and recovering from the situation by publishing additional information is rarely effective.

This negative publicity on a non-event risk is part of the environment the WLCG collaboration operates and largely outside the control of its participants. Nevertheless, the reputation impact on the collaboration may be significant.

6. Insecure configuration leading to undesirable access

Risk score: 6 / 25

Although WLCG aims at providing an homogenous configuration for its services or resources, a number of configuration options are delegated to the local staff, in order to accommodate local services and policies. Similarly, lower level configuration, like operating systems and basic services, is typically performed by local staff.

These more manual steps, coupled with heterogenous staff experience and skills, may introduce insecure configurations at some of the services or resources used by WLCG. These vulnerabilities may lead to undesirable or unauthorised access to the resource, either directly or via compromised identities. Lack of security expertise or training is an aggravating factor.

7. Insufficient protection of information leading to sensitive data leakage

Risk score: 6 / 25

The access control list (ACL) mechanism used by a number of WLCG data resources, including both grid-specific and traditional storage solutions (e.g. AFS), is often complex, with heterogenous policies based on the local site policy and the technology being used. The security architecture has primarily concentrated on the job submissions aspects and the security aspects of the data resources is often seen as less mature.

Data resources are not only used to store scientific data and programs and research draft papers, and WLCG users also store personal or sensitive information (e.g. credentials) on them. It is therefore essential to ensure tights ACLs to access these resources.

The user, the local administrator and the virtual organisation all play a key role to implement appropriate ACLs. If either of them fail to implement sufficient controls, there is a risk that sensitive information may leak, for example exposing sensitive data.

8. Incidents on resources not bound by WLCG policies

Risk score: 4 / 25

WLCG participants providing services to users may need, either temporarily or permanently, to run their services on external CPU or data resources (e.g. Amazon Cloud). Outsourcing to external cloud services is for example a common implementation.

This is a rather recent trend, used only by a small number of WLCG participants and the likelihood of severe problems remains low. However, a security compromise on an external resource not endorsing WLCG policies could have a very serious impact (scoring 5 in the impact scale) for the collaboration.

External resource providers are rather unlikely to have agreed and sign the existing security policy requirements enforced in WLCG. This may some time implicitly or explicitly bring additional risks to the collaboration, including:

- Operational and reputation risks: an incident affecting the external provider may affect WLCG services or the reputation of the collaboration. The external provider may in addition not have any obligation to inform or collaborate with WLCG on the incident, potentially making the incident resolution in WLCG significantly more difficult.
- Financial risks: an attacker may consume large amount of resources paid for by WLCG. Also, an incident affecting WLCG resources hosted on an external infrastructure may involve attacking further external organisations. In this case, the external infrastructure supporting WLCG may be involved in the case and seek damage to WLCG. For example, all Amazon EC2 users agree to the following terms and conditions:

  "*If we or our affiliates are obligated to respond to a third party subpoena or other compulsory legal order or process described above, you will also reimburse us for reasonable attorneys' fees, as well as our employees' and contractors' time and materials spent responding to the third party subpoena or other compulsory legal order or process at our then-current hourly rates.*" (https://aws.amazon.com/agreement/)

Any WLCG participant making use of resources not endorsing the WLCG security policies should inform the WLCG Management Board, who will decide to accept or reject the resulting risk.
WLCG denies any liability and all liability and legal issues and consequences are the responsibility of the employing institution recommending the use of these non-WLCG resources to its users.

9. Exploitation of a serious VO/middleware software vulnerability

Risk score: 4 / 25

WLCG uses specific software, in particular in two areas: the middleware, enabling underlying computing resources to communicate, and the VO software, enabling the users from each VO to use the infrastructure. Just like there are risks inherent to operating systems vulnerabilities, there are risks linked with possible vulnerabilities in the middleware or VO software. The vulnerability management process, including its risk assessment team, are providing a classification of the vulnerabilities affecting middleware issues.

A small part of the software specific to WLCG operates with system privileges and may therefore lead to a system compromise, should they suffer from a severe vulnerability. Unlike operating system software that may vary from one resource to the other, many resources are running similar middleware components, possibly leading to risk affecting many of them impact in case a vulnerability is discovered.

10. Data removal/corruption/alteration

Risk score: 3 / 25

Data integrity and data protection are crucial assets to the LHC experiments. Data may be the result of intensive and expensive human or machine work and the ability to preserve the integrity of large amount of data is essential. For these reasons datasets are present in the infrastructure in multiple copies, in some cases on tape devices. The most likely risk is a loss of resource while data is being restored from copies. For this reason, it is critical to implement and maintain adequate authentication and authorization controls on storage systems. It is also essential to enforce the rule of least privileges as often as possible at the resource centres, in order to avoid creating additional exposure for the data. The large volume of data, the number of different storage technologies, as well as the number of different storage location all constitute additional challenges.

11. DoS from an external organisation

Risk score: 1 / 25

Any organisation or infrastructure directly connected to the Internet may be affected by Distributed Denial of service (DDoS) attacks, which consists in rendering the targeted service(s) unavailable by sending them a very high number of requests. WLCG services or resources may be subject to such an attack as well. However, its resources are distributed across a large number of resources and the more centralised services, like authentication/authorization use caching systems, like the short-lived x509 proxies, enabling the work to continue for up to 24 hours after their issuing service has been taken offline.