

Document ID: SEC-00

Approval Date: 2022-08-24

Approved By: NSC

Alliance Federation Information Security Glossary

In the event of a discrepancy between the definitions in this Glossary and those in any other document, the definitions in this Glossary of Terms take precedence.

Accountable:

The role is ultimately answerable for the activity or decision.

Alliance Federation Systems and Services:

The technology elements required to implement, operate and manage national services. Not including any elements that have no dependencies with national services.

Data Custodian:

The person who operationally manages one or more sets of data under the direction of the Data Owner or Data Steward.

Data Owner:

The senior-most role accountable for the data throughout its lifecycle.

Data Steward:

The delegate of the **Data Owner**, a role that oversees the lifecycle of one or more sets of data associated with a **National Service**. And can make those decisions as delegated by the **Data Owner**.

National Service:

Advanced Research Computing (ARC) and related capabilities offered by the Alliance Federation (see service map)

Responsible:

The role(s) that has an obligation and is authorized to perform the task. This can be shared between multiple roles.

Risk:

Risk is an uncertain event or condition which, if it occurs, affects the ability of an organization to achieve its operational or strategic objectives.

Risk Management:

The planned and systematic approach for the identification, assessment, response and monitoring of risk to maximize opportunities and minimize losses.

Risk Owner:

The role accountable for the effective management of a specific risk or risk category. This is typically an executive or management role that has the authority and accountability to assume risk on behalf of the organization and ensure risks are effectively managed.

Residual Risk:

The risk score after risk treatment has been completed.

Risk Tolerance:

Risk tolerance is how much risk an organization can withstand to achieve its strategic objectives.

Service Owner:

The role accountable for the effective management (including the action required to respond, document, and monitor risks as directed by the Risk Owner) of a specific service, infrastructure, or service portfolio.

Vulnerability:

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.