Risk Assessment

An actual template for a risk assessment is not provided, since it heavily relies on the type of processing that is taking place. However, the following questions and table can be used as an input into conducting a risk assessment, or even a full DPIA. The table below provides possible risk sources, and how can they be considered and mitigated. More information is provided in WP29 opinions [WP29-WP248rev.01] and AARC guideline [AARC-G042].

Questions to ask yourself when filling this table:

- What type of processing involving personal data do you conduct?
- What are the risks associated with these processing activities?
- What are the mitigation procedures? Review of processing activities?
- Is the documentation about all processing activities relevant and up-to-date?

**delete this box after completing the Risk Assessment.*

Risks	Impacts on data subjects	Main risk sources	Main threats	Existing or planned measures	Severity	Likelihood
Illegitimate access, disclosure or misuse of personal data						
Unwanted change of data						
Disappearance of data						
Insufficient security						

© Owned by the authors and made available under license:
https://creativecommons.org/licenses/by-nc-sa/4.0/
Other Sources / Attribution / Acknowledgements: SCIv2 from the WISE Community, used under CC BY-NC-SA 4.0. EGI e-Infrastructure Security Policy EGI-SPG-SecurityPolicy-V2, used under CC BY-NC-SA 4.0. The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).

Policy Development Kit was reviewed by the AAF Trust and Identity Pathfinder Policy Working Group, by and for Australian national research infrastructure, enabled by NCRIS.

controls						
Non-compliance with Privacy Act or other regulations						

© Owned by the authors and made available under license:
https://creativecommons.org/licenses/by-nc-sa/4.0/
Other Sources / Attribution / Acknowledgements: SCIv2 from the WISE Community, used under CC BY-NC-SA 4.0. EGI e-Infrastructure Security Policy EGI-SPG-SecurityPolicy-V2, used under CC BY-NC-SA 4.0. The research leading to these results has received funding from the European Community’s Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).

Policy Development Kit was reviewed by the AAF Trust and Identity Pathfinder Policy Working Group, by and for Australian national research infrastructure, enabled by NCRIS.