

e-Authentication Risk Assessment

In order to provide an authentication services that can be used across government, the e-Authentication project must first identify the full range of authentication requirements for the electronic Government Initiatives and projects. The e-Authentication Initiative teamed with the Software Engineering Institute (SEI) at Carnegie Mellon University to develop a risk-based approach to authentication requirements, called the **e-Authentication Risk and Requirements Analysis**, or **e-RA**. This approach identifies the risks associated with insufficient authentication of users, and it forms the basis for the definition of authentication requirements.

The e-RA process aims to ensure that a user has the proper credential to perform a particular action (generally termed a transaction) in a system or web portal. The e-RA maps each transaction to a set of pre-defined authentication criteria that represent various levels of proof of a user's identity. This mapping is used to select and implement appropriate technological and operational solutions that ensure the transaction's authentication requirements are met.

The initial risk assessment activities focus on those areas of the e-Government initiative or project that are subject to authentication controls and risk, including the user population, transactions, and corresponding data. The objectives of the e-RA are:

1. Document and characterize the transactions and associated data.
2. Identify the risks (threats and impacts) associated with authentication of the actors (or users) for the range of transactions.
3. Define the authentication criteria for the initiative's transactions, which become the authentication requirements.
4. Analyze the authentication needs and map to standardized levels of authentication.

The e-RA approach focuses on authentication risks; and therefore, the e-RA approach does not provide a comprehensive profile of overall risk for an organization. Access to and ability to communicate with key Initiative or project personnel is necessary to validate and refine results.

The e-RA has several components aimed at delivering a repeatable process and leading a project through the process in an efficient manner. Included are a e-RA Automated Workbook, which helps document and analyze all the relevant information, as well as supporting instructional manuals. Any Agency, Initiative or technology/Web application owner wishing to obtain e-RA materials and conduct an e-RA can contact Mark Liegey of the e-Authentication Initiative at mark.liegey@gsa.gov.