Risk Assessment & Path Selection Guide

In selecting the appropriate electronic signature or workflow solution, the first step is to identify the level of risk for the form or workflow. For this purpose, the University has identified three possible risk levels and created an Identity Assurance Guide. The selection process will be the responsibility of the department and is expected to require some level of professional judgement in certain cases. Examples of the types of risk have been included to assist in identifying the levels but the department may have other significant factors to consider in their decision-making process.

To begin, identify the Risk Level based on the Risk Score of the process in question. Once the Risk Level has been identified, the level of assurance required to confirm a person's identity can be determined. The assurance level is then used to determine appropriate authorization methods. In other words:

1. determine risk score/risk level
2. determine identity assurance level
3. select appropriate method of authorization.

There are three possible risk levels regarding the authorization of a business process. Level 1 is considered the lowest level of risk and Level 3 the highest level of risk. The level of assurance needed so that a person's identity can be trusted must be determined based on the impact of authentication errors or misuse of credentials. As the consequences of an authentication error increase, the level of assurance should increase. Low impact risks will require lower levels of assurance and less stringent methods of authorization. Higher impact risks will require higher levels of assurance and more stringent methods of authorization.

To assist departments in selecting an appropriate authorization method, a table with examples based upon assurance levels expected for a given level of risk has been provided at the end of this guide. The examples are intended to illustrate possibilities or options, some of which are currently supported by the University and some of which may not be supported. In all cases, departments are expected to follow any legal requirements for documenting authorizations that may be associated with the department's activities. Departments are also expected to follow any system or university policies.

If it is desirable or necessary to use an electronic signature tool other than those provided in the examples below, please ensure it adheres to the guidelines set in the Electronic Signature Policy. Departments needing assistance should consult with ITS.

Calculation Tables to Determine Risk Score

Impact x Likelihood = Risk Score

Example: Impact of 4, Likelihood of 2, results in Risk Score of 8 (4 x 2 = 8)

Impact	
Score	Definition (Financial/Non-Financial)
5	Greater than $1 million or Extreme reputational impact
4	$0.5 million to $1 million or High reputational impact
3	$0.1 million to $0.5 million or Medium to low reputational impact
2	$5,000 to $0.1 million or Low to no reputational impact
1	Less than $5,000 or No reputational impact

Likelihood of Unauthorized Execution	
Score	Definition
5	Highly likely; nearly certain to occur
4	Likely; probably will occur
3	Possible; might occur at some time
2	Unlikely; could occur at some time
1	Rare; may occur

Identity Assurance Guide				
Risk Score	**Authentication and Documentation Attributes of Acceptable Method Based on Risk Score**	**Examples of Acceptable Authentication Methods**	**Corresponding Example of Business Process**	**Suggested System Authorizer**
Low Risk (1-10)	No identity proofing or security procedures required due to low/no risk transaction. Little confidence needs to be established for the asserted identity, which is usually self-asserted. Minimal or no records need to be retained to document the transaction.	1. Electronic Signature Options a. Email from any address b. Scanned image of signature or electronically written signature c. Self-signed PDF d. Unauthenticated Qualtrics survey or Microsoft Forms submission	AIS new account request Accounting corrections Bursar collection reports	Fiscal Officer/ designee or responsible individual
Moderate Risk (11-15)	Some identity proofing via a security procedure is needed so that confidence exists that the asserted identity is accurate or the employee is acting with proper authorization. Some reliable record should likely be retained for a time consistent with the University's record retention policy.	1. Digital Signature Options: a. e-ID authenticated Qualtrics survey or Microsoft Forms submission b. e-ID authenticated digital certificate used in conjunction with Adobe Acrobat c. Use of an e-ID authenticated workflow system - SharePoint, HireTouch, Kuali Build, Kuali Research d. Scanned image of a signature or electronically written signature submitted via SIUE email address e. 3rd party authenticated digital certificate from a trusted Certificate Authority (CA) (Adobe Sign, DocuSign, etc.)	Most HR forms SARF Tuition waiver Salary deferral Employment contracts AIS transfer vouchers Purchase requisition Dependent verification Illinois residency	Unit head or designee
High Risk (16-25)	Stringent identity proofing via multiple security procedures is needed since the system should have high confidence as to the identities of all parties involved in the process.	1. Digital Signature Options: a. Digital certificate signed using the Illinois Public Key Infrastructure (PKI) b. 3rd party multifactor authenticated digital certificate from a trusted Certificate Authority c. Notarized remote signature	Expected to be very rare. Possibly some contracts or affidavits involving foreign countries.	Vice Chancellor level, designee, or approved designated University authorized signatory

Adapted with permission from the University of Illinois Identify Assurance Guide.