University of Illinois System Identify Assurance Guide

Selecting an Authorization Method

To select an appropriate authorization method, assess the level of risk associated with the business process and the method by which the identity of the person is determined using the **Identity Assurance Guide** on the following page.

To begin, identify the Risk Level based on the Risk Score of the particular process or step. 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 four possible risk levels regarding the authorization of a business process. Level 1 is considered the lowest level of risk and Level 4 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. Methods that provide the appropriate levels of assurance should be:

- commercially reasonable,
- applied in a trustworthy manner,
- relied upon in good faith,
- unique to the individual within the context in which it is used,
- used to objectively identify the person taking the action,
- reliably created by the individual given the circumstances,
- not readily duplicated or compromised given the circumstances,
- linked to the electronic record to which it relates, and
- invalidated if the signature or record is altered.

To assist units in selecting an appropriate authorization method, the following table provides examples based upon the assurance levels expected for a given level of risk. **The examples are intended to illustrate possibilities or options, some of which are currently supported by the system and some of which may not be supported**.

In all cases, units are expected to follow any legal requirements for documenting authorizations that may be associated with the unit's activities. Units are also expected to follow any system, university, or department policies.

Identity Assurance Guide[1]

Risk Score[2]	Authentication and Documentation[3] Attributes of Acceptable Method Based on Risk Score	Examples of Acceptable Authentication Methods	Corresponding Example of System Business Process to Identified Example of Acceptable Authentication Method	Suggested System Authorizer[4]
Level 1: Very Low to Low Risk (1-10)	No identity proofing 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. Unauthenticated electronic or paper form/survey 2. Email from non-system email address 3. Scanned image of signature 4. Paper form with signature 5. Verbal request or approval	1. "Contact Us" web form 2. Admissions question from prospect 3. Thank you note 4. Outside doctor's note documenting a 1 or 2 day absence 5. Help Desk provision of general system assistance	Unit head or designee
Level 2: Moderate Risk (11-15)	Some identity proofing needed, so that confidence exists that the asserted identity is accurate or that system employee is acting with proper authorization. Some reliable record should likely be retained for a time consistent with the unit's record retention policy.	1. Approved system authentication mechanism 2. Signature or request with: a) government issued photo ID or b) established signature on file or c) trusted third party authentication. 3. Scanned image of signature submitted by signer via system authentication mechanism or system email	1. Recording work time internal to a unit 2. System person to sign for receipt of certified mail and then route the mail received, or check out of library material equipment 3. Email received from outside party with a known email address	Unit head or designee
Level 3: High Risk (16-20)	Stringent identity proofing is needed since the system should have high confidence as to the identities of all parties involved in the process.	1. Signature with established signature on file or with trusted third-party authentication. 2. Notarized signature.	1. Submission of purchases (Banner Forms) or iCS Contract system 2. Some contracts or affidavits involving foreign countries.	Comptroller-designee or Assistant Vice President-equivalent or above
Level 4: Very High Risk (21-25)	Requires in-person identity proofing. Very high confidence in the asserted identity's accuracy; used to access high risk data and/or data with compliance requirements.	1. Government approved hardware token 2. In-person signature with government issued photo ID	*Level 4 is rare and expected to only be considered for very high and risky levels of commitment*	President's Cabinet

[1] **The entries in this Identity Assurance Guide table are meant to provide broad guidance. Specific situations or unit protocols may require other processes**.

2 Risk Score is based off UI Risk Impact Scale of $1 million Scale.

[3] Documentation may be electronic.

4 The authorizer should also notify their supervisor. The supervisor may optionally seek additional authorization or consult with IT security, counsel, or others as warranted.

Calculation Tables for the System Risk Score

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

Impact x Likelihood = Risk Score

LIKELIHOOD	
Score	**Definition**
5	Almost certain; expected 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

For help determining the Risk Score, contact the Enterprise Risk Management group.