THE UNIVERSITY OF ALABAMA AT BIRMINGHAM

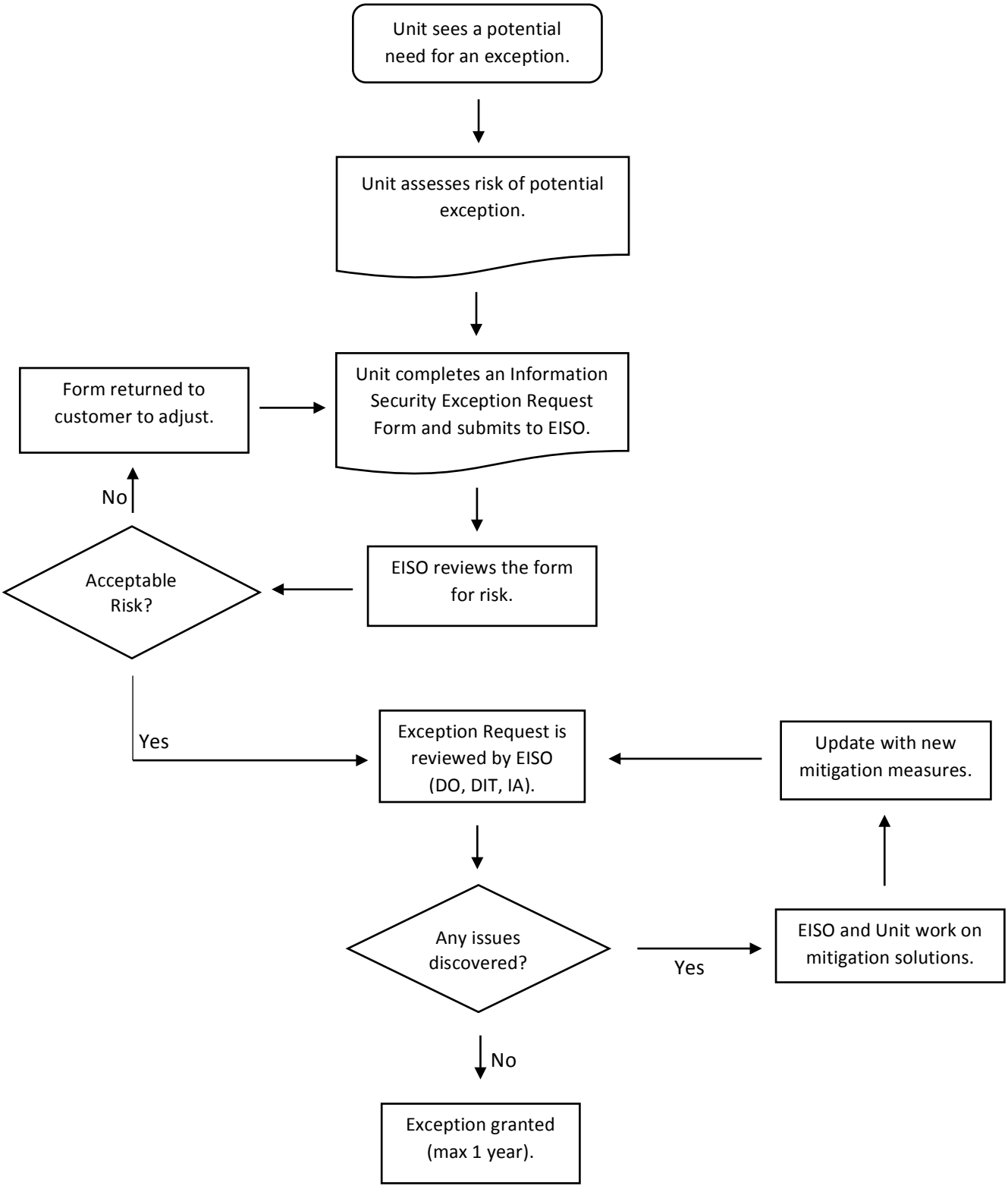
Information Security Policy and Standard Exceptions Process

University of Alabama at Birmingham (UAB) information security policies, standards, guidelines, and procedures establish controls that are used to protect institutional data and IT Resources. While any exception to a policy or standard can weaken protection for University IT Resources and data, occasionally exceptions will need to be made for legitimate University reasons. Centralized and departmental IT units and IT Resource owners who are responsible for ensuring appropriate enforcement of University information security policies and related standards on University IT Resources must use this procedure when requesting an exception to UAB information security policies and standards.

Exception Procedure

The following procedure defines the process for the review and approval of exceptions to UAB information security policies and standards:

- A requestor and their Department Head/Director seeking an exception must assess the risks that non-compliance poses to the University also legitimately ruled out compliant alternatives to the request should any exist. If the Department Head/Director believes the risk is reasonable, then the requestor prepares an Information Security Exception Request Form describing the systems and data involved, the risk analysis, and mitigation steps.
- Submit the completed request form for exception to AskIT@uab.edu. A Service Now ticket will be created and assigned to the Enterprise Information Security group.
- The Enterprise Information Security group will gather any necessary background information with the assistance of the requestor and make a recommendation to approve or deny the request. This group may recommend that other areas such as Data Owners, Departmental IT Management, and/or Internal Audit review certain decisions.
    - Exceptions to current security controls may require implementation of compensating controls to maintain security and reduce risk. Options for compensating controls may be recommended by the requesting party or by the Enterprise Information Security group, Data Owners, Departmental IT Management, and/or Internal Audit.
    - Compensating controls will be the responsibility of the requesting unit to implement and maintain.
- The Chief Information Security Officer, or his or her designee, will approve or deny the request for an exception.
- The requestor and Department Head/Director will be notified of the decision to approve or deny.
- All requests for exception will be retained by the Enterprise Information Security group.
- Exceptions are valid for a maximum of a one-year period. Annually or as appropriate, the Enterprise Information Security group shall review approved exceptions. The requestor and Department Head/Director may be required to attest whether the conditions that merited the original exceptions are still in effect. If necessary a new request for exception must be submitted, reviewed and approved.


Unit sees a potential need for an exception.
Unit assesses risk of potential exception.
Unit completes an Information Security Exception Request Form and submits to EISO.
Form returned to customer to adjust.
No
EISO reviews the form for risk.
Acceptable Risk?
Yes
Exception Request is reviewed by EISO (DO, DIT, IA).
Update with new mitigation measures.
Any issues discovered?
Yes
EISO and Unit work on mitigation solutions.
No
Exception granted (max 1 year).