LogicGate Risk Acceptance Guide

Last Modified on 10/30/2026 12:52 pm EDT

For more details about the Information Security Office, **please visit our website**!

The Risk Acceptance process is used to document instances where a known risk cannot be fully remediated or where a requirement of a Wharton policy or standard cannot currently be met.

Requestors can access the Risk Acceptance process through the Wharton ISO website.

If you are unsure whether a Risk Acceptance is appropriate, contact the Wharton Information Security Office at security@wharton.upenn.edu.

What is a Risk Acceptance?

A Risk Acceptance documents a known risk that Wharton has chosen to accept for a defined period of time or under specified conditions.

Risk Acceptance replaces the previous Exception terminology and process. The change in name more clearly reflects the purpose of the process: documenting the risk, the reason it cannot currently be fully addressed, any compensating controls, and the formal decision by an appropriate Risk Owner to accept that risk.

A Risk Acceptance does not remove the underlying requirement or risk. It documents the decision to accept that risk under the conditions and timeframe described in the request.

When to Submit a Risk Acceptance

Submit a Risk Acceptance when:

- A Wharton policy or standard requirement cannot currently be met
- A required security control cannot be implemented as designed
- A known risk will remain in place for a period of time
- Wharton ISO directs you to document a risk through the Risk Acceptance process

A Risk Acceptance should not be used as a substitute for implementing required controls when remediation is reasonably available.

Before You Begin

Before starting a Risk Acceptance request, be prepared to provide:

- The system, application, service, or process involved
- The specific requirement that cannot currently be met
- Existing or proposed compensating controls
- A requested expiration or review date
- Supporting documentation, if available

Providing complete and accurate information will help Wharton ISO review the request more efficiently.

Starting a Risk Acceptance Request

1. Go to the Wharton ISO website and click the **Risk Acceptance** button.
2. Log in to LogicGate using your PennKey SSO credentials.
3. Select the blue **Create Record** button in the upper-right corner of the home screen.
4. Complete the required Risk Acceptance Details, Impact, and Dates sections.
5. Describe the associated risk and any compensating controls already in place.
6. Link any related Initiative Reviews or Products, if applicable.
7. Review the request for accuracy and completeness.
8. Select **Submit**.

After You Submit

Wharton ISO will review the request and determine whether additional information, clarification, or documentation is needed. LogicGate will send email notifications when action is required.

Wharton ISO's role is to review the request and provide a recommendation. The identified Risk Owner then reviews the request and determines whether to formally accept the risk on behalf of the School.

Risk Ownership and Acceptance

A Risk Owner is a senior leader with the authority to formally accept risk on behalf of Wharton.

Wharton ISO does not formally accept risk on behalf of the School. ISO reviews the request, evaluates the proposed controls and mitigations, and makes a recommendation to the identified Risk Owner.

The Risk Owner then reviews the request and either:

- **Accepts the risk**, including any associated conditions or mitigation requirements; or
- **Does not accept the risk**, in which case the request is closed and the requestor is notified.

In most cases, ISO expects potential concerns to be addressed during its review through required mitigations before the request is reviewed by the Risk Owner.

Duration, Expiration, and Review

All Risk Acceptances have an expiration date. Even long-term risks are expected to be reviewed at least annually to confirm that the risk still exists, the business need remains valid, and required mitigations are still appropriate and effective.

Before a Risk Acceptance expires, the responsible parties should determine whether the underlying risk has been remediated or whether continued acceptance is needed.

If additional time is required, an extension request can be submitted through LogicGate for ISO evaluation, and Risk Owner review and sign-off.

FAQs

Why is the Exception process being renamed Risk Acceptance?

The new name more clearly reflects the purpose of the process. Rather than simply documenting an exception to a requirement, the process records the underlying risk, compensating controls, mitigation plans, and the decision by an appropriate Risk Owner to formally accept that risk.

Is a Risk Acceptance the same thing as an Exception?

Risk Acceptance replaces Wharton's former Exception process.

Existing references to an "exception" may still appear in older documentation or communications, but new requests should use the Risk Acceptance process beginning October 30, 2026.

Does an accepted risk mean the policy or standard no longer applies?

No. A Risk Acceptance does not remove or change the underlying policy or standard requirement. It documents that the associated risk has been reviewed and formally accepted under specified conditions and for a defined period of time.

How early should I submit a Risk Acceptance?

Submit the request as soon as you know that a required control or policy requirement cannot be met. Submitting early provides time for ISO to evaluate the risk, request additional information if necessary, identify required mitigations, and route the request to the appropriate Risk Owner.

How long does a Risk Acceptance review take?

Wharton ISO's target is to complete its review within two weeks, provided we have complete and accurate information and all documentation needed for review.

More complex requests, incomplete submissions, or requests requiring additional mitigation may take longer. Final timing may also depend on Risk Owner review.

Who should be listed as the Risk Owner?

The Risk Owner should be a senior leader with the authority to formally accept risk on behalf of Wharton, such as the Wharton CIO. Wharton ISO can help determine the appropriate Risk Owner if you are unsure.

What are compensating controls?

Compensating controls are safeguards that help reduce risk when the preferred or required control cannot currently be implemented.

For example, if an application cannot support PennKey SSO, compensating controls might include requiring MFA through another authentication method, restricting access to approved users, or limiting access through a VPN.

What are mitigation requirements?

Mitigation requirements are actions that must be taken to reduce or manage the accepted risk.

A risk may still be accepted while one or more mitigations remain outstanding. Those mitigations will be assigned to responsible parties with specific due dates and tracked as part of the Risk Acceptance.

Does a Risk Acceptance expire?

Yes. All Risk Acceptances include an expiration date. Long-term accepted risks are still expected to be reviewed at least annually to confirm that continued acceptance is appropriate.

Can a Risk Acceptance be extended?

Yes. If the underlying risk cannot be remediated before the existing acceptance expires, an extension request can be submitted through LogicGate. The extension will be reviewed to confirm that the risk, business need, and compensating controls remain appropriate.

What happens if the Risk Owner does not accept the risk?

The request will be closed and the requestor will be notified. Wharton ISO's review is intended to identify concerns and required mitigations before the request reaches the Risk Owner, so we expect formal non-acceptance to be relatively uncommon.

Can I link a Risk Acceptance to another LogicGate record?

Yes. Risk Acceptance requests can be linked to related Initiative Reviews and Products in LogicGate. Linking related records helps maintain context and provides a clearer record of how the risk was identified and managed.

How does Risk Acceptance relate to an Initiative Review Finding?

An Initiative Review may result in a Finding that identifies a required control or remediation.

If that requirement cannot be completed within the necessary timeframe, a Risk Acceptance may be used to document and formally accept the associated residual risk. The Risk Acceptance can be linked to the related Initiative Review to maintain the connection between the original review, the identified risk, and the acceptance decision.

How can I check the status of my request?

Log in to LogicGate and check the **My Work** section of your home page. LogicGate will also send email notifications when additional information or action is required.

Getting Help

Wharton ISO is available for requestors both during and after the transition to LogicGate. Please join our weekly office hours, or email security@wharton.upenn.edu for more support.