

How to submit a request for a Vendor Risk Assessment

All hardware or software purchases will require a submitted request for a Vendor Risk Assessment in Service Now. This guide will assist with explaining the process for submitting a vendor risk assessment on behalf of the requestor.

Requester

The requester is responsible for providing the following:

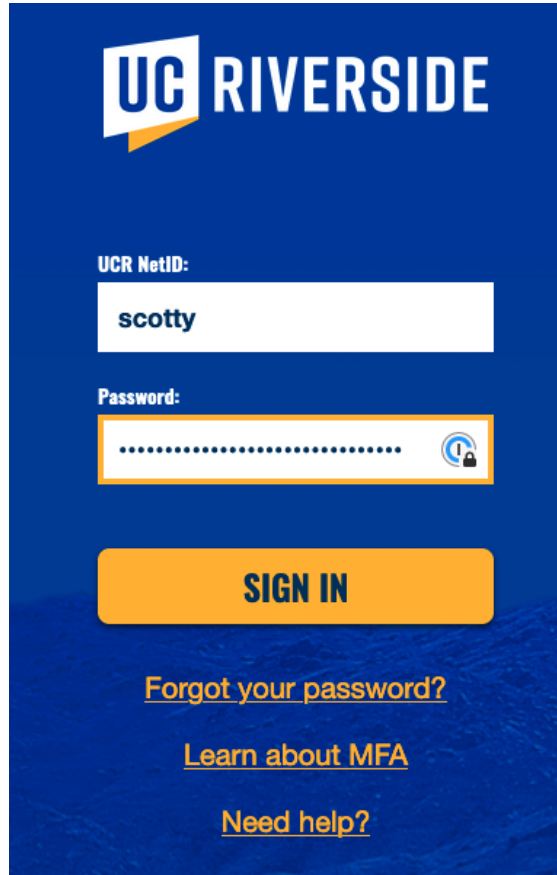
- Providing complete intake forms, A, B, and/or the alternate intake A waiver.
 - [Intake A](#): Intake A is intended to facilitate communication requirements. Intake A must be provided to the vendor, by the requestor, but only completed by the vendor to the best of their ability.
 - [Intake A \(Waiver\)](#): Is to be completed by the requestor if the vendor is unwilling to complete Intake A.
 - [Intake B](#): Required for any service, hardware, or software which may create, store, process, or transmit, Institutional Information and/or access IT resources. This is to be completed on behalf of the requestor.
- Responding to questions from the IT Security Analyst and/or SOM procurement about their procurement request.
- Contacting the vendor if the vendor does not respond to requests from IT Security Analyst and/or SOM procurement.
- Managing permissions to services or products.

Submitting a request for a vendor risk assessment

Before submitting a software or hardware request, it is highly recommended to have all intake forms, invoices, approved by a department approver, and COA number(s), to prevent delays. Providing incomplete requirements will cause delays in the security review, thus elongating the completion time.

Once all required information is obtained, proceed to the following:

1. Navigate to Service Now and submit a request for a [Software Request](#) or a [Hardware Request](#).
2. When redirected, sign in with campus netID and campus password.

The image shows a login form for UC Riverside. At the top left is the UC Riverside logo, consisting of the letters 'UC' in a white box with a yellow triangle pointing down, followed by the word 'RIVERSIDE' in white. Below the logo, there are two input fields. The first is labeled 'UCR NetID:' and contains the text 'scotty'. The second is labeled 'Password:' and contains a series of dots, with a small icon of a person and a lock to its right. Below the password field is a large orange button with the text 'SIGN IN' in black. Underneath the button are three links: 'Forgot your password?', 'Learn about MFA', and 'Need help?', all in orange text.

3. Once signed in, you will be asked to complete a software or hardware request form. You will be required to enter the following: Full name (requestor), email address, type of request, and vendor information such as contact information.

Software Request

User Information

Requestor 

Email

Phone

Department

Role

Preferred Contact Method

Request Type

Supervisor

Request Detail

* Software name

* Vendor Name



* Vendor Email Address


* Does the vendor accept a (PO) Purchase Order? (The PO is the preferred payment)


* COA

Add

Remove All

Actions	COA Code	Percentage
 	123456789	100


More Information 

In order to properly process this request you must attach 


- [Intake form A](#)
- [Intake form b](#)
- [Invoice](#)

without the necessary attached documents this request may be delayed.

Additional Information (if needed)

Brief description of intended use, intended users, and background of service. 

[Submit](#)

 Add attachments

4. Additionally, it is important to include as much detail when providing the following.
 - A. Completed intake forms A and B
 - a. or Intake A (Waiver) and Intake B.
 - B. Vendor-provided invoice or quote.
 - C. Department approval
 - D. COA number(s)
5. Once submitted, SOM IT will receive the request and be routed to the required groups. It is recommended to review [Steps 1 -5 in skills and responsibilities](#) to review SLAs and additional requirements from SOM IT or other campus groups.

Estimated Time of Completion

Below are the following departments and groups in the Office of Information Technology (OIT) and Campus, affiliated with a software or hardware purchase. These steps are performed following the submitted hardware or software request.

- Step 2 - (OIT) IT Procurement: IT Procurement receives the request and enters the order in Oracle. This is estimated to be completed in **3 -5 business days** if all information is provided. If the provided information is not complete or descriptive, the action can take **5 days or more**.
- Step 3- (OIT) IT Security, SOM Compliance (if needed): IT Security to review security architecture, security risk assessment, and obtain Business Associate Agreement (if needed). Estimated completion date within **10 - 85 business days** if all required information is obtained.
- Step 4 - (OIT) IT Security and IT Procurement: Security will finalize the security review and forward it to IT Procurement to approve the purchase request. Estimated completion date within **3 - 5 business days** if the information has been completed and approved.

- Step 5 - (SOM) Procurement and (Campus) Central Procurement. - SOM Procurement will create the Purchase Order, and process the invoice for payment. SOM Procurement has estimated a completion date of **5 - 7 business days**. Afterward, the invoice will be routed to Central Procurement to pay the vendor in an estimated **3 - 90 business days**.

Delays

- Nonresponsive vendor (regarding obtaining security documentation, security architecture review, or risk assessment review)
 - After 14 days of not receiving additional information from the vendor, the department is asked if they wish to continue with the purchase. Doing so would require an exception, which may require additional approvals. Otherwise, the department also has the option to find a new vendor.
- Lack of information from the department or internal department on how the product will be used.
- Vendors requesting redlines to Appendix DS or not willing to agree to Appendix DS
 - Determine who will accept risk and move with an exception process.