UCF Vendor Risk Management (VRM) Guide

**Why is VRM important?**

To minimize the risk to university data, the university needs to take a methodical approach when engaging third party service providers and cloud-based services for data storage, processing or outsourcing of university data. The Vendor Risk Management program (abbreviated VRM) is UCF Infosec’s answer to this need.

**Does VRM apply to the service I’m looking to acquire?**

The VRM process applies to any university department or university business unit considering contracting with a third party service provider for the purposes of storing, transmitting, processing, or collecting university data on our behalf.

In this process, the service-seeking unit submits information about the proposed vendor, solution, and data involved. The Information Security Office (ISO) reviews this package and follows up with the service-seeking unit and/or vendor regarding any questions or concerns. The Information Security Office review results in a formal VRM Assessment report which summarizes what was reviewed, any findings/concerns, and recommendations. The report is reviewed and signed by the appropriate UCF business and data owners, and a signed copy with their signatures must be returned to the Information Security Office.
This section provides the information security office with more information on who’s requesting the product and who from the business unit will reach out to the vendor if there’s a technical issue. If you’re unsure of who this may be for your area, please contact the information security office at infosec@ucf.edu.
The solution/vendor information security provides the information security office with basic vendor information that is critical for our review. If you are unsure of how to answer any of the questions, please contact the information security office at infosec@ucf.edu.
• The SHUD-Q (Secure Handling of UCF Data Questionnaire) formerly known as the SHUDA is a document that should be shared with the vendor regardless of the data involved. If there is pushback from the vendor, please contact the information security office.

• Providing the data involved, guides the information security office in their data classification process. If you are unsure or have any questions about what should be listed, please contact the information security office at infosec@ucf.edu.
The data elements section also guides the information security office in the data selection process, please try to be as accurate as possible when filling this section out. If there is a data type not listed, please include it in the other data types section. For any questions, please contact the information security office at infosec@ucf.edu.
• The implementation questions provide the information security and data privacy teams with more information on access management and data protection. If you are unsure how to answer a question, please contact the information security office at infosec@ucf.edu.

• For the form to be completed, the completed SHUD-Q from the vendor must be attached to the ticket. If you don’t have the document just yet, you can save the ticket to your wish list and ServiceNow will send you reminders on a weekly basis. There may be more documents requested based on data classification, more information about that can be found at Vendor Risk Management - UCF Information Security.

An offline version of the ServiceNow form that you can work with the vendor on, can also be found at Vendor Risk Management - UCF Information Security.