Cloud Services/Software Review

The UMBC software review process is a comprehensive assessment of software purchase and renewal requests for compliance with security, technical, procurement, and legal policies.

The State of Maryland requires an efficient and effective audit review process whether the software is used on personal computers or as part of a cloud-based Software as a Service (SaaS). The review process is designed to reduce risks associated with data integrity, shared network services, and contract requirements between third party vendors and the University.

- Compliance with federal and local data requirements (FERPA, HIPAA, etc.).
- Compliance with state purchasing and COMAR regulations.
- Data storage, access, confidentiality, integrity, sensitive institutional information and personally identifying information.

Yes. However, software installed on a local machine is usually reviewed more quickly and is of lower risk.

DoIT Business Analyst, DoIT Security, UMBC Legal, and UMBC Procurement

**DoIT Business Systems Group:** The primary point of contact throughout the review process. Manages and supports the review when needed. Conducts initial inventory and information gathering.

**DoIT Security:** Reviews the product for any security vulnerabilities, data management, and other technical risks of product use. Creates recommendations for the requestor, legal, and/or DoIT Business Analyst.

**DoIT Technical:** Oversees the review of products requiring SSO and/or an interface. Provides DoIT Business Analyst with feasibility and timeline estimates.

**Legal & Procurement:** Oversees the legal/procurement review. Modifies terms and Contracts. Ensures UMBC legal risk is mitigated and procurement requirements are met.

**New:** 1-4 weeks

**Renewal:** 1-2 weeks

Software for research may often fall under different guidelines and policies which may expedite or reduce the need for a review. Products should still be submitted so that they may be inventoried by DoIT, but the review process may be shorter in comparison to non-research reviews.

You can expedite this process by providing the Business Analyst with any of the following information when submitting your ticket:

- Additional information regarding the product and its use.
- Complete vendor contact information (if not already provided in the ticket).
- IT security documents available from the vendor (e.g. SOC reports, security white papers, industry compliance, etc.).
- Legal purchasing documents associated with the product (e.g. Terms & Conditions, Privacy Policy, Quote, etc.).
- If using a purchase requisition, submit that to procurement in parallel with this process and include the RT number of this ticket.

The software could be denied for a number of reasons which commonly include:

- The vendor is unwilling to meet Maryland law and procurement policies.
- The product and/or its data are not secure.
- The vendor does not meet UMBC procurement guidelines.
- The product does not support single sign-on compatible with UMBC’s existing technology.
- The vendor is unwilling to communicate with or provide information to the software review committee.
If the product has been purchased or renewed but has not been vetted by DoIT security, a review will be conducted within the next year to avoid interruptions and maintain business continuity. Be aware that you may receive outreach from a member of the DoIT security office during this time period.