Published on *University of Colorado* (https://www.cu.edu)

Choosing a SaaS Solution [1]

Introduction

Software as a Service (SaaS) is a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted. It is sometimes referred to as "on-demand software."

The SaaS model is becoming increasingly more common in home and business networks alike, and is the poster child for the “Cloud” paradigm in IT. Some popular examples of SaaS products include Microsoft Office 365, Amazon Web Services, Dropbox and WebEx. While SaaS products have unique benefits over “on premises” software (access from anywhere, reduced reliance on hardware, storage of information in the Cloud), they can also introduce unique risks in the form of service and network complication and data security. This document is designed to help the reader understand and anticipate the impacts of SaaS solutions.

SaaS Checklist

A SaaS product used for the University of Colorado community should strive to meet the following requirements. While we recognize that different use cases may require more or less stringent guidelines than those outlined here, the checklist has been designed to be a good starting point for any purchaser of a Software as a Service product.

Business Requirements:

- The product provides functional support for University of Colorado's business.
- The product satisfies a unique need and there is not an existing IT-supported solution which accomplishes the same thing.
- Acquisition of the product adheres to University procurement rules. [2]
- The service provider is viable and provides support for the product.
- The service provider has a process to notify the user about changes in the product (e.g., functionality, UI).

Technical/Integration Requirements:

- The system availability of the product meets business requirements.
- The product supports requirements around the management of users and access rights.
- The product supports development and testing requirements.
- Use of the product is reviewed and approved by the appropriate data oversight groups.

Security Requirements:

- The product supports University of Colorado's data security requirements. [3]
- The product complies with University policy and legal requirements.

- The product is reviewed and approved for accessibility and security review, as appropriate.
- The product includes log and/or event notification.

See the content below for details about the items in this checklist.

I. Business Requirements

The product provides functional support for University of Colorado's business.

- The product must satisfy the functional business requirements of the University of Colorado community.
- The product must fit well with other products in your unit’s portfolio. Can you leverage the combined power of as many of your products and the broader University’s products as possible?
- If being used as part of a research project, confirm that the product satisfies the applicable business and technical requirements (e.g., research reproducibility or data policy considerations). Speak to the appropriate research computing resources for more information.
    - Boulder - Resources are available on the website for Research Computing or submit a Help Request form
    - Colorado Springs - Email questions to Greg Williams (gwillia5@uccs.edu [4])
    - Denver - Email Research and Shared Services at rss@ucdenver.edu [5]

The product satisfies a unique need and there is not an existing IT-supported solution which accomplishes the same thing.

- Check with OIT to see if there is an existing vendor relationship you can use.

Acquisition of the product adheres to University procurement rules.

- Use the CU Marketplace for SaaS procurements whenever possible and avoid using a procurement-card for SaaS products. The Marketplace is designed to help make your purchase as smooth as possible and saves time vs. reconciling procurement card expense reports. Lastly, making your purchase via the Marketplace increases the PSC’s ability to identify opportunities to pool University resources and leverage entreprise spend, yielding better pricing and terms for all CU faculty and staff.
- Avoid click-through agreements – Cloud vendors make it easy to accept their license agreements by presenting them in a “click-through” format. If a user is not authorized to sign legal agreements on the University’s behalf, they are not authorized to accept click-through agreements. All agreements should be reviewed by the PSC to ensure that you and the University are not taking on undue risk.
- Use a purchase order for SaaS procurements whenever possible. If total annual spend will exceed $10,000, a standing purchase order may be appropriate. Speak with a purchasing agent for more information.

The service provider is viable and provides support for the product.

- The service provider must be a stable entity running on a sustainable business model and unlikely to disappear. The service provider must interact with other services or tools supporting activities in their segment of the market.
- The service provider offers a baseline level of support which matches the specific business requirements.
- University of Colorado must understand a full support model before broad deployment of any SaaS product or service. Even inexpensive or “free” SaaS products cost something to offer and extend to the University of Colorado community. The funding model must match the cost (e.g., ongoing licensing or support costs).
- University of Colorado must clearly understand the lifecycle of the product, including the business workflow, contractual obligations, and the service provider's responsibilities for supporting an exit strategy for University of Colorado.

The service provider has a process to notify the user about changes in the product.

- This includes any changes to user interface, APIs, integrations, data structure, or physical location (if appropriate).

II. Technical/Integration Requirements

The system availability of the product meets business requirements.

- Consider support for peak usage, 24x7 access, scheduled maintenance, business continuity, etc.
- Any established SaaS provider must have a track record for availability, both on uninterrupted normal service and during upgrades/changes. You need to assure that the records shows an acceptable level of service availability for your business needs.
- Usually a third party audit assesses disaster recovery readiness, and University of Colorado gets the information indirectly. The acceptable level of RTO/RPO (Recovery Time Objective/Recovery Point Objective) demonstrated by a provider is a business decision.
- The exit strategy must include devolving business process, data, and the references to the service provider which will not convey directly (e.g., name of SaaS provider in web links).

The product supports requirements around the management of users and access rights.

- If the solution requires login, is it possible to integrate with the campus single sign-on system? Has the campus Identity Management team been consulted?
- Have plans been made for how users will be created, access will be changed and how users will be removed from the solution?

The product supports development and testing requirements.

- Is there an environment provided by the vendor separate from the main live production

system for testing changes?
- If custom development is occurring with this solution, is there a separate environment provided by the vendor for development?
- Does the schedule of new features moving through testing and into the live production environment proposed by the vendor align with business requirements?

Use of the product is reviewed and approved by the appropriate data oversight groups.

- Does the solution need to exchange data with other University systems?
  - If so, has the access to that data been approved through the data governance process [6]? Contact data.governance@cu.edu [7] for more information.
  - If the data will be exchanged on a regular basis, have the managers of the systems holding that data been consulted to determine if the solution's data integration technologies are sufficient and acceptable?
- Does the solution require reporting or analytics outside the scope of what is provided by the solution?
  - If so, have the relevant data analytics staff been consulted to determine how the solution could fit with campus or system data analytics efforts?
- Do you have a plan for extracting the data from the solution should you discontinue its use?

III. Security Requirements

The product supports University of Colorado's data security requirements.

- The product must comply with the appropriate standards for the University's risk classifications. For the handling of confidential or highly confidential data or sensitive business processes (e.g., financial or health care transactions), you must contact your campus information security office before selecting or using a SaaS provider.
- All reputable SaaS providers document their alignment with relevant compliance standards/processes. For example, ISO 27001 is a compliance standard and framework that ensures a range of security practice and controls are performed by the service provider. This and similar objective audits can help you gain and maintain assurance for a range of business uses.

The product complies with University policy and legal requirements.

- Beyond the operational reporting necessary for incidents, the service provider must define their responsibilities for reporting timeliness, completeness, root cause, and mitigation strategy.
- Depending upon the type of data/business process involved with a SaaS provider, statutory regulations (e.g., the PCI Data Security Standard or HIPAA) may constrain the location of the data and require very specific notification requirements. If you have questions about these requirements, contact your campus information security office.
- In the case of breaches or outages, in addition to the necessary operational reporting, there must be defined service provider responsibilities for reporting timeliness, completeness, root cause, and mitigation strategy.
- (Boulder only) The product must conform with University accessibility standards.

The product is reviewed and approved for accessibility and security review, as appropriate.

- Contact your campus IT Security and Compliance team for accessibility and security review. *This step is especially important when using a P-card, since PSC won't be able to route the purchase to the appropriate team for additional review.
    - Boulder - https://www.colorado.edu/ictintegrity/ict-review-process [8]
    - Colorado Springs – email security@uccs.edu [9] and comply@uccs.edu [10] with a description of the service
    - Denver - https://www1.ucdenver.edu/offices/office-of-information-technology/softw [11]...
    - System – email security@cu.edu [12] with a description of the service

The product includes log and/or event notification.

- The SaaS provider must have incident notification mechanisms in place (e.g., email or SMS) for any service outage or security incident.
    - For example, it tracks administrative access or configuration changes to deployment.

Comments or questions?

For more information, contact your campus IT department or the relevant department indicated above.

CU Boulder

OIT IT Service Center
303-735-4357
help@colorado.edu [13]

UCCS

OIT Help Desk
719-255-4357
helpdesk@uccs.edu [14]

CU Denver | Anschutz Medical Campus

OIT Help Desk
303-724-4357
UCD-OIT-HELPDESK@ucdenver.edu [15]

CU System

UIS Service Desk
303-860-4357
help@cu.edu [16]

Groups audience:

Office of Information Security

Source URL:https://www.cu.edu/security/choosing-saas-solution

Links
[1] https://www.cu.edu/security/choosing-saas-solution [2] https://www.cu.edu/psc/procurement-rules
[3] https://www.cu.edu/security/policy [4] mailto:gwillia5@uccs.edu [5] mailto:rss@ucdenver.edu
[6] https://www.cu.edu/security/data-management-group-process [7] mailto:data.governance@cu.edu
[8] https://www.colorado.edu/ictintegrity/ict-review-process [9] mailto:security@uccs.edu
[10] mailto:comply@uccs.edu [11] https://www1.ucdenver.edu/offices/office-of-information-technology/softw [12] mailto:security@cu.edu [13] mailto:help@colorado.edu [14] mailto:helpdesk@uccs.edu [15] mailto:UCD-OIT-HELPDESK@ucdenver.edu [16] mailto:help@cu.edu