Key points to consider when acquiring and managing a Cloud solution

Guidelines to help prospective SaaS users learn the best way to evaluate, purchase and use SaaS resources at Stanford

Evaluate

Be mindful of University security and compliance requirements

Comply with University Policies and Legal Requirements
SaaS and Cloud resources can only be used at Stanford if their use is compliant with University policies.

Data Security
The Information Security Office (ISO) has defined how data types are classified and are to be protected. A Data Risk Assessment (DRA) or waiver from ISO is required for any SaaS or Cloud use that will store or process University data.

Privacy and Accessibility
Confirm that the use of the Cloud resource or SaaS application will not violate any part of the Admin Guide regarding privacy and accessibility.

Identity & Authentication
Determine if the solution supports the University's Identity and Access Management (IAM) requirements when applicable.

Breach or Security Incident Notification
Determine if the Cloud vendor will provide adequate and timely notification of a security breach to fulfill University obligations.

Business Continuity and Disaster Recovery
Understand the options for BC/DR provided by the vendor. Ensure that their options meet your business requirement for system and data availability and protection.

Select

Avoid these common pitfalls when selecting a vendor

Free Trials
Free trials are available for many SaaS solutions, but users are still responsible for securing University data and being compliant with all University policies.

Avoid Customizing SaaS Products
If possible, avoid customizing a SaaS solution. It is frequently difficult and costly to do so. Sometimes it is unavoidable, but often with more research competitive vendors with a better functional fit can be found.

Verbal Representations by Vendors
Vendor employees may make verbal representations about compliance, service levels, security and other key topics. Unless these statements are included in the license agreement and signed by appropriate personnel of the vendor and the University they are not enforceable.

Service Level Agreement (SLA)
Confirm that the vendor's standard SLA terms meet your requirements. SLAs for Cloud vendor agreements are difficult to change – so it is best to confirm that you understand the vendor's commitments and that they will meet your needs.

If the vendor is ever in breach of their SLAs, they typically must be notified within a predefined period per the contract for you to qualify for service credits.

Buy

Considerations for when it is time to purchase

PCards
The use of a PCard to purchase SaaS solutions does not remove any of the obligations for compliant use of SaaS resources.

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 need to be reviewed by University Procurement Contract Group.

Overview of Stanford's SaaS purchase checklist
To make a compliant SaaS purchase at Stanford, follow these six steps:

1. Security Review
2. Contract Review
3. Accessibility Review
4. SLA Review
5. Vendor Negotiation
6. Purchase requisition

A detailed version of this checklist is on the back of this card.

Manage

Manage the vendor relationship to ensure success

A Good Vendor Relationship Starts with a Good Contract
Negotiate the best deal possible when starting a relationship with a vendor. A good contract will anticipate and avoid future misunderstandings or issues. Suggestions for how to do this are on the back of this card.

Track Your Use of the Application
Exceeding user counts or resource levels as defined in your PO or contract can put you in a breach situation. Remediation can be costly, as vendors can apply penalties or change deal terms per their rights in the contract.

Know your Escalation Path
Learn the escalation path for service outages or customer service issues before they happen – so if an issue occurs you can get help quickly.

Build a Positive Relationship
Find ways to partner with your vendor to build a positive relationship. If issues arise in the future, it will be easier to resolve them. Build executive level relationships with strategic vendors.

Regular Business Reviews
Hold regular business reviews with Strategic vendors to identify and resolve issues before they become unsolvable.

New Feature Introductions
When new features are released, you may be required to license them to get access. Understand the cost implications before agreeing to add new features.

Renew

Best practices for renewing a SaaS solution

Start the Renewal Process Early
Give yourself and the University sufficient time to prepare for a renewal (months). With more time before the deadline you are in a stronger negotiating position and have more options.

Negotiation is Possible
Renewal rates can often be negotiated even though vendors would have you think otherwise. It is also a good practice to negotiate and lock in the renewal rate at the time of initial purchase whenever possible.

Renew on-time
Renewing a license or subscription on time helps your project and the University by avoiding late payment charges or cancellation fees, and ensures there won't be interruptions in service.

Co-Term
If there is an opportunity to co-term multiple renewals with a vendor, you may be able to reduce cost and administrative overhead.

Upgrades
SaaS vendors frequently upgrade their applications. When major upgrades are released, be aware that there may be a significant amount of resources required for change management, technical and business training, fixing broken integrations with existing University resources and more.

End of Life

Prepare for the end of the vendor relationship

End of Life
It takes time and preparation to properly exit a relationship with a Cloud vendor - or transition through the end of life of a product. Some key points to consider during a transition include:

Preservation of Data
At the End of Life the user is responsible for ensuring the vendor is obligated to return all data in a useable format under any possible termination scenario.

Sanitization of Data
At the end of Life when data is to be sanitized (deleted/ destroyed), it must be done so in accordance with the relevant ISO policy. *[uit.stanford.edu/security/data-sanitization]*

Contract Compliance
In some End of Life scenarios the vendor may have been acquired, or gone out of business, which can change the rights and responsibilities of the University and the vendor. Depending on the situation, seek help from Stanford legal counsel.

Turn card over for more information and helpful resources

Steps to SaaS purchase success at Stanford University

The procurement cycle for a SaaS purchase can vary from weeks to months depending on factors like size, soliciting competitive bids and more. You can help facilitate a successful SaaS purchase by being prepared for the following steps.

Security Review	***Have your use of the SaaS resource reviewed for compliance with University data risk classifications and security policies***
	Data Risk Assessments are conducted by the Information Security Office (ISO)
	Start by completing the brief pre-screening questionnaire: https://uit.stanford.edu/security/dra
Contract Review	***Have the appropriate Stanford organization review the vendor's contract***
	Conduct competitive price benchmarking to inform your negotiation by checking with peer universities and on the internet.
	Contemplate future growth scenarios to see if there is any need to build in tiered pricing / volume discounts to accommodate future footprint growth.
	Build in Renewal price protection at the time of purchase - it is the most advantageous time to get the lowest possible renewal price.
	Contracts should first be reviewed by the business owner to identify any issues with business terms.
	Legal review of the contract is performed by authorized personnel in the Procurement contracts department.
Accessibility Review	***Products should be evaluated to ensure that they comply with University accessibility standards***
	Evaluate use cases of the SaaS product to ensure that all users will have equal access to the solution: https://ucomm.stanford.edu/policies/accessibility-policy.html
SLA Review	***A review of the Service Level Agreement (SLA) in the vendor agreement is important to confirm that your SaaS resource uptime will support your business requirements***
	Understand the vendor's commitment to system availability, and how to notify the vendor of any outage. Learn how to make a reimbursement claim if your contract has a provision for one. Know your escalation path with the vendor in case of an outage.
	An excellent article and chart on Availability are available on Wikipedia: https://en.wikipedia.org/wiki/High_availability
Vendor Negotiation	***Assistance is available for negotiating with SaaS vendors***
	Check with UIT Vendor Management to see if there is already an agreement in place with your preferred vendor that you can leverage.
	Contact UIT Vendor Management if you need help negotiating with a vendor: UITVendorManagement@Stanford.edu
Purchase Requisition	***The purchase requisition process involves financial approval and results in a purchase order***
	To learn more about the purchasing process, competitive bids, Sole Source Justifications and more visit: web.stanford.edu/group/fms/fingate/staff/buypaying/contract_purchases.html

Additional Resources

Information Security
Risk Classifications
UIT SaaS Considerations
HIPAA Security & Privacy Policies
Accessibility
Procurement Policies and Purchase workflow
Free Third Party Cloud Vendor Research

Nan's weblink goes here:

uit-stage.stanford.edu/cloud-transformation/additional-resources

-- Send UIT a SNOW ticket to request help related to Evaluating, Acquiring or Managing a Cloud solution