SaaS Solution Evaluation Criteria

SaaS Solution Evaluation Criteria

The purpose of this article is to describe the criteria that should be considered when evaluating a new software-as-a-service (SaaS) product for use at MIT. Technical, business, and legal criteria must all be considered as part of product selection; the criteria outlined here fall into 4 overall categories: Licensing methodology, contractual terms & conditions, security & data protection, and integration requirements.

Requesting a vendors SOC 2 Type 2 or equivalent report will tell you how a company safeguards customer data and how well their protections are operating. The HECVAT (Higher Education Community Vendor Assessment Toolkit) is also a valuable tool when evaluating Cloud or SaaS vendors.

Licensing

There are a number of different licensing models under which SaaS products are made available:

1. Site license / unlimited usage – under this model, all MIT faculty, students, and staff are entitled to use of the product under MIT's negotiated license without MIT paying a per-user fee. This is generally MIT's preferred model for obtaining SaaS products due to predictability of costs, simplicity of license management, and ease of access for the community. Depending on the product and vendor, this model may not be available or may be financially non-viable for reasons of cost. One common scenario when acquiring a new product is an initial purchase of a fixed number of user licenses for a "proof of concept" or pilot launch, with the ability to expand to a site license at a future data if there proves to be widespread product adoption at MIT; for this reason, vendor evaluations should always include a discussion of the availability of an unlimited license, even if this model is not selected for the initial acquisition.

2. User count – under this model, licensing is based on the number of users with access to the system, either as an upfront count of the total number of users permitted (capacity-based licensing) or the number of users who have provisioned / activated accounts (utilization-based licensing). This is the most common model for SaaS product licensing, and while it is not preferred, it is considered acceptable. If the licensing is capacity-based, thought should be given to the demographics most likely to make use of the product (i.e., students vs. administrative staff) when arriving at the initial license count to be purchased. If the licensing is utilization based, the terms & conditions should specify the reporting period and process for a license count "true up".

3. System usage – under this model, licensing is based on a pre-determined usage metric other than user count, e.g. total quantity of storage used. This is MIT's least favored model, as system usage is difficulty to quantify in advance for products used by the entire MIT community and may fluctuate rapidly, resulting in unpredictable demand / cost spikes. If this model is used, the terms & conditions should specify a pre-determined rate for the acquisition of additional resources to ensure the most favorable costs to MIT.

MIT Procurement & Strategic Sourcing should be consulted when discussing licensing options with a new vendor.

Contractual Language

Any contract signed by MIT will be subject to final review and approval by MIT's legal counsel. Several key issues to be aware of when reviewing a new product are:

- **Data ownership** – all data stored by the vendor as part of offering the SaaS solution must remain owned by MIT with no access, usage, or ownership rights granted to the vendor beyond those required to operate the service on behalf of MIT.
- **Use of name** – the governing contract must not grant the vendor any right to use MIT's name, logo, or other distinguishing marks for any purpose.
- **Incorporation of URL terms** – all terms that govern MIT's use of the product and obligations to the vendor must be incorporated directly into the document and may not be referred to via a URL on the vendor's web site that may be updated without prior notice to MIT.
- **Service Level Agreement** - the amount of guaranteed uptime, the process and timeline for dealing with downtime and the consequences for failing to meet these standards must be clearly stated.
- **Warranty** - contract should warrant that the service conforms to and will perform in accordance with its specifications and that it does not infringe any third party IP rights.
- **Indemnification** - Vendor should indemnify MIT for all its actions and omissions. It is critically important in two areas: third-party IP infringement and inappropriate disclosure/data breach.
- **Governing law** – Ideally, contract should specify that Massachusetts state law will govern in the case of any disputes. Alternatively, a stipulation that all disputes will be handled under the state law of the defendant's state is acceptable.

MIT's Office of General Counsel should be consulted when reviewing contractual language provided by a new vendor. Proposed contracts should be provided in Microsoft Word format, not PDF, for ease of annotation.

Security & Data Protection

Data Classification

When evaluating security of a new SaaS offering, the most crucial issue is the type of data being stored. MIT routinely deals with several kinds of regulated data and while these data are generally not prohibited from being stored in a hosted or “cloud” solution, appropriate safeguards must be confirmed as being in place. With appropriate contractual language in place, all of these classifications of data may be stored in a “cloud” solution.

1. FERPA – student records and similar data. Contracts for services housing FERPA-protected data must designate vendor as a “school official” with “legitimate educational interests.” This ensures that vendor will not use the data for any other purpose, such as data mining for the vendor’s own benefit or redisclosure to others.

2. PHI / HIPAA – patient / health record data. For this data to be stored in a SaaS solution, a HIPAA BAA (Business Associate Agreement) must be completed between both parties. If the vendor is unwilling to sign such a document, prospective users of the service should be made aware that it is not suitable for storing HIPAA data.

3. Personally Identifying Information (PII) - Massachusetts data protection regulations require that any entity collecting certain categories of personal information must ensure the data is appropriately secured and protected.

4. Human Subject Research data - All information collected from human subjects in research projects is subject to the CONSENT forms executed by the participants, which may place additional restrictions on how and where data is stored. In addition, this data may also be considered personally identifying or PHI and be subject to the considerations of one or more of the categories detailed above.

Several kinds of data are never appropriate for storage in a SaaS solution:

1. Export-controlled data - There may be additional considerations for ITAR or EAR data please contact exportcontrolhelp@mit.edu

2. PCI (Payment Card) / Financial data – If you are taking credit card payments, please contact VPF's Merchant Services chargemit-help@mit.edu

3. Social Security / Driver’s License / Passport Number – End users should not be collecting and storing this data under any circumstances.

Vendor Security & Data Protection Evaluation

When evaluating a new vendor’s security, MIT should request and review appropriate audit documents from the vendor, such as a recent SOC1, SOC2, and / or SOC3 reports, ISO27001 certification report, or equivalent documents issued by an external auditor as proof of sufficient procedures and controls within the vendor’s organization. In reviewing these documents, the following criteria should be considered and explicitly clarified if the document does not cover them:

- **Data location** – all MIT data must remain resident within the United States and may not be relocated to another jurisdiction without advance written notice to MIT and sufficient time for MIT to object and seek an alternate solution.
- **Encryption** – all MIT data should be both stored and transmitted encrypted, using a modern cryptographic cypher, i.e. AES128 or AES256. Use of algorithms known to be weak, i.e. DES, RC4, SHA1, and MD5, is strongly discouraged. Any data not stored encrypted should be explicitly spelled out.
- **Use of subcontractors** – any third party hosting services used as part of providing the service, i.e. Amazon AWS, Microsoft Azure, etc. should be disclosed.
- **Vendor data access** – approximate number of vendor employees with direct access to customer data and the situations / processes by which it will be accessed. Employees with direct access should be limited and consist of staff in operations roles. Procedures for access to customer data should require authorization from the customer’s designated administrator prior to access.
- **Security testing** – the vendor should specify what ongoing security testing they perform on their product, such as static and / or dynamic code analysis and any automated or manual penetration testing.
- **High-availability / Disaster recovery** – the vendor should detail their HA and DR plans, including recovery point objective (RPO) and recovery time objective (RTO) targets, geographic diversity in their hosting arrangements, and any periodic testing that takes place.
- **Backup retention** – the vendor should detail how frequently backups of customer data are made, how long they are retained, and how soon customer data is purged following deletion by an end user.
- **Data extraction** – the vendor should detail the process by which data can be removed from their environment in a portable (i.e., not proprietary) format should MIT wish to discontinue use of their service.

Integration

In order to operate in MIT’s IT environment, prospective SaaS solutions should be evaluated to ensure that they integrate appropriately with MIT’s identity and authentication solutions, and provide appropriate extension points for future integration needs. Specific considerations are:

1. Authentication / Single Sign On (SSO) – products should support the SAML2 standard, known at MIT as “Touchstone”. Products will ideally provide documentation for SAML integration including the type and format of user attributes that must be released by an enterprise’s identity provider service. Additionally, the vendor should support the Service Provider initiated SSO workflow, and will ideally be a member of the InCommon federation to simplify MIT’s identity services integration process.

2. Directory Services – products should support user directory integration via LDAP or Microsoft Active Directory to simplify the user provisioning process. If this is unavailable, the product should supply an administration API for provisioning users via a central MIT service such as Moira.

3. RESTful API – products should supply a comprehensive REST-based API that allows for all actions that can be performed via the UI to

be executed programmatically. Ideally, products will also provide hooks allowing them to consume APIs exposed by other services.

Additional integration requirements may exist depending on the product's use cases; for example, products considered for part of MIT's administrative systems portfolio may require SAP integration. The IS&T Architecture Review Board (ARB) should be consulted when considering potential integration needs and methods.