CLOUD / HOSTED / SaaS ASSESSMENT

PURPOSE	The purpose of this document is to provide guidance to assess and evaluate the proposed solution's security and other features and determine key risks. Refer to the Cloud / Hosted / SaaS Policy for additional information. Instead of completing this assessment for the proposed service provider, you may submit the service provider's completed HECVAT (Higher Education Community Vendor Assessment Toolkit) version if available. ***Note: portions of this checklist may overlap with Brock's Privacy Impact Assessment (PIA) questionnaire which may be required if the proposed solution stores / processes Personal Information. Where the necessary information has already been provided in the PIA, please refer to the section of the PIA as applicable. Discuss with the University's Freedom of Information and Privacy Coordinator whether a Privacy Impact Assessment Questionnaire should be completed***
INSTRUCTIONS	Information Technology Services will work with the area interested in the Cloud / Hosted / SaaS solution to complete this document. When referencing the solution provider's policy(ies) in the questionnaire below, include the policy name, section number and hyperlink (if available). See **Appendix** for definitions of cloud / hosted / SaaS.

KEY CONTACT INFORMATION

Name	First name, Last name
Title	[enter]
Extension	[enter]
Area	[enter]

KEY STAKEHOLDERS

Name	Title	Extension	Area
[enter]	[enter]	[enter]	[enter]
[enter]	[enter]	[enter]	[enter]
[enter]	[enter]	[enter]	[enter]
[enter]	[enter]	[enter]	[enter]

BACKGROUND INFORMATION OF PROPOSED SERVICE / SOLUTION

Service [enter]

Purpose Identify the Brock asset for deployment
[Note: An asset supported by the cloud / hosted / SaaS solution generally falls into one of two categories: (1) information / data; or (2) transactions / processing (either partial functions or full applications)]

Asset evaluation (risk) Evaluate the importance of the asset to Brock. Consider how Brock would be harmed if:

1. The asset became widely public and / or widely distributed
2. An employee of the provider accessed the asset in an unauthorized manner
3. The data / process / function were manipulated by an outsider
4. The process / function failed to provide expected results
5. The information/data were unexpectedly changed
6. The asset was unavailable for a period of time

BACKGROUND INFORMATION OF PROPOSED SERVICE / SOLUTION

Data	Identify the Brock University data fields that will be stored / processed by the service
Proposed provider	[enter]
Area(s) impacted	[enter]
Number of users	[enter]
Proposed go-live date	[enter]

SERVICE / SOLUTION ASSESSMENT QUESTIONNAIRE

1. Provider	
Consideration	**Response**
1.1 Is the solution provider an industry leader, small player, niche player or new-comer?	
1.2 What is the size of the solution provider's operations – consider number of employees, annual revenues, etc.	
1.3 History: how long has the solution provider been in business?	
1.4 Are there current issues of concern, e.g., negative media / press, data breach, etc.	
1.5 List the provider's current / prior higher education clients, if known.	

2. Terms of service	
Consideration	**Response**
2.1 Explain the limitations to how Brock can use the service as outlined in the provider's acceptable usage policies, licensing rights or other provider usage restrictions.	
2.2 What advance notice will be provided by the provider for any change of terms?	
2.3 Does the contract / terms of service outline meaningful liability for the provider in the event that the Brock environment / data is breached?	

2. Terms of service	
Consideration	**Response**
2.4 Is there a cap on liability?	
2.5 Does the provider have cyber risk insurance in place? If so, please provide coverage details.	

3. Service-level agreement	
Consideration	**Response**
3.1 Does the provider have an active SLA in place that identifies minimum performance (e.g., up time, etc.)?	
3.2 Describe the SLA.	
3.3 Does the provider provide regular service management reports (e.g., SLA performance)? If so, state the frequency of such reporting.	
3.4 Describe penalties associated with SLA non-compliance.	

4. Third party	
Consideration	**Response**
4.1 Does the provider use a third party to provide the required services? If so, explain the services to be provided by the third party, and the type of relationship between the provider and the third party.	

4. Third party	
Consideration	**Response**
4.2 Does the provider monitor service continuity with upstream providers in the event of provider failure?	

5. Provider administration	
Consideration	**Response**
5.1 Who at the provider can access Brock's environment and/ or data? (Include third party access if applicable)	
5.2 How is their access controlled?	
5.3 What is the provider's downtime plan (e.g., service upgrade, patch, etc.)?	
5.4 What is the provider's peak load, and is there sufficient capacity for this?	

6. Provider disaster recovery / continuity	
Consideration	**Response**
6.1 Does the provider have a disaster recovery plan? If so, attach, if possible and indicate when it was last tested.	
6.2 Does the plan address, at a minimum: • Power or critical service failure • Physical disasters such as fire, water damage or flooding • Civil disobedience encumbering operations	

6. Provider disaster recovery / continuity	
Consideration	**Response**
- Security breaches resulting in the failure of core systems (e.g., Distributed Denial-of-Service (DDOS) attack, etc.)	
6.3 Does the provider have a failover site? If so, is the failover site certified to the same standards as the primary facility? Please describe.	
6.4 Are the same security controls implemented at the failover site as the primary site?	
6.5 Where is the failover site located? Are there separate jurisdictional considerations that should be factored?	
6.6 What service-level guarantee does the provider offer under recovery conditions?	
6.7 Does the provider have a continuity plan? If so, attach, if possible and indicate when it was last tested.	

7. Multi-tenancy (identify if a third party is involved)	
Consideration	**Response**
7.1 Is Brock's environment set up on dedicated hardware, or do multiple tenants exist? If the latter, how does the provider control / restrict access to Brock's environment?	
7.2 How does the provider segregate the Brock environment from other tenants?	

8. Scalability	
Consideration	**Response**
8.1 Are the services provided by the provider scalable? Are there any limits?	

9. Compliance	
Consideration	**Response**
9.1 Have all regulatory requirements been identified? If so, by whom? Outline all regulatory requirements.	
9.2 Provide / attach evidence of PCI-DSS compliance, if applicable. Does the contract state that the provider will provide evidence of compliance to Brock as soon as finalized? If not, why not?	
9.3 Does the proposed solution comply with WCAG 2.0 Level A and AA requirements? If so, provide / attach evidence.	

10 Maintenance and support	
Consideration	**Response**
10.1 What are the provider's customer support hours? Do these work for the University area considering the solution?	

10 Maintenance and support	
Consideration	**Response**
10.2 Are the provider’s routine maintenance windows manageable for Brock?	
10.3 Does the provider have meaningful problem response and resolution commitments?	
10.4 Does the provider give notice of material reductions in functionality?	

11 Termination	
Consideration	**Response**
11.1 Describe the process to terminate the service.	
11.2 What happens to Brock data at service termination?	
11.3 Can Brock data and the service be moved / transferred to another provider at any time?	
11.4 Are export utilities available and easy to use?	
11.5 Will Brock data be permanently erased from the solution, including any backup storage, when this data is deleted or the service ended?	
11.6 Specify any fees that may be incurred at the end of the service.	
11.7 Does Brock have the right to terminate if the provider introduces material modifications to service terms?	

11 Termination	
Consideration	**Response**
11.8 Is there a right of termination for material breach of applicable privacy and security obligations?	

12 Application security (if applicable)	
Consideration	**Response**
12.1 What standards does the provider follow for application development? Do these include rigorous testing and acceptance protocols?	
12.2 What application security measures are used in the production environment (e.g., application-level firewall, database logging / auditing, etc.)?	
12.3 How is data integrity assured? What controls exist over internal processing?	
12.4 Are session timeouts available and customizable?	

13 Authentication / Authorization	
Consideration	**Response**
Note: The proposed solution must integrate with the current Brock University user authentication protocols in order to be considered. ***Sign-off by the AVP, ITS is required as evidence that ITS agrees on the integration of the proposed solution with Brock's user authentication protocols.***	

13 Authentication / Authorization	
Consideration	**Response**
13.1 Authentication: Check all applicable options and provide an explanation for “Other”.	□ ADFS □ Shibboleth □ SAML □ Other: (Explain below. State any standards used) □ Don’t know
13.2 Authorization: Explain in detail how roles are managed.	
13.3 Authorization: Can roles be managed with an external identity management solution? Please explain.	
13.4 Are “local” user accounts required? Is so, explain the user case and how they are managed.	
13.5 How are user profiles provisioned? Are standards such as SCIM (http://www.simplecloud.info/) followed?	
13.6 How are user accounts provisioned? Are standards such as SCIM (http://www.simplecloud.info/) followed?	
13.7 Does the application support multi factor authentication (MFA / 2FA)? If yes, please elaborate.	

14 Data access	
Consideration	**Response**
14.1 Does the provider have access to Brock data, and if so, what restrictions are there over this level of access?	
14.2 Are there “secondary uses” of the area’s account information or Brock data without the area’s knowledge or consent by the provider and / or affiliates?	
14.3 Can any third party access Brock data, and if so, how?	

15 Data ownership	
Consideration	**Response**
15.1 Does the provider reserve rights to use, disclose or make public the area’s account information and / or Brock data?	
15.2 Do the intellectual property rights of Brock data remain intact (if applicable)?	
15.3 Does the provider retain rights to Brock data even if data is removed from the provider?	

16 Data transmission	
Consideration	**Response**
16.1 What security features exist for data transmitted back and forth between the user and the provider?	
16.2 Are data transfers manual or automated?	
16.3 What security features exist if the provider transmits data from one location to another (if applicable)?	
16.4 What are the provider's data leak prevention capabilities?	

17 Data integration	
Consideration	**Response**
17.1 Attach both a process flow and a detailed data flow diagram.	
17.2 Will the service / solution require integration with other Brock solutions / data, either on-premise or in the cloud? If so, please describe.	
17.3 Does the service / solution support automated file transfers or web service calls? Is there a secured location to store files that can be picked up?	
17.4 In what format(s) can data be delivered (e.g., files on secure FTP or service calls)?	
17.5 Is a third-party involved in the integration process?	

18 Data storage / backup (identify if a third party is involved)	
Consideration	**Response**
18.1 Where and how will Brock data be stored? Are there impacts on security in light of the differences in legal / regulatory compliance requirements depending on storage location?	
18.2 What is the frequency of Brock data back-ups?	
18.3 Are data back-ups stored on-site or off-site? If the data is stored off-site, does a sub-contractor store it? If so, list all relevant sub-contractors.	
18.4 Is there controlled access to the data and storage media? Please describe.	
18.5 How is stored data protected / secured by the provider (e.g., encryption)?	
18.6 Will a local backup (i.e., at Brock) be made of data stored by the provider? If so, by whom, how often, where will it be stored and how / how often will it be tested?	
18.7 What is the process to restore data from the provider's back-up?	
18.8 Can data be recovered for a specific customer in case of failure or data loss?	

19 Data retention (identify if a third party is involved)	
Consideration	**Response**
19.1 What specific fields will be retained?	
19.2 What is the retention period for each data field?	
19.3 How often does the provider delete data?	
19.4 Is verification provided that data has been securely deleted?	
19.5 What happens to Brock data when the provider is terminated?	

20 Security (identify if a third party is involved)	
Consideration	**Response**
20.1 Explain the provider's available security features, and whether these are supported by an independent information security management certification (e.g., ISO/IEC 27001).	
20.2 Does the provider have a cyber plan in place? If so, please provide details.	
20.3 Have there been any major security incident(s) reported with the provider in the last two years? If so, detail the incident(s) and resolution(s).	
20.4 What activities are logged by the provider? Consider: • Network traffic, file and server access • Security systems • Databases and servers • Active directory	

20 Security (identify if a third party is involved)	
Consideration	**Response**
• Web and mail servers • VPN systems • VM systems.	
20.5 Does the provider's logging and monitoring framework allow isolation of an incident to specific tenants?	
20.6 Who can set up activities to be logged?	
20.7 Who has access to these logs?	
20.8 How long are logs maintained by the provider?	
20.9 What alerts can be set in the system?	
20.10 Who gets notified by the alert?	
20.11 If virtual machines are in use by the provider, does the provider's virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/ configuration of the virtual machine?	
20.12 If using virtual infrastructure, does the solution include hardware independent restore and recovery capabilities?	
20.13 Does the provider leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	

21 Physical security (identify if a third party is involved)	
Consideration	**Response**
21.1 Is the location where Brock data is stored secure?	
21.2 Does the provider have a rigorous physical access protocol? Consider: • All secure areas use card swipe technology / biometric scanners / other technology to control access • A sign-in process exists for third-party individuals (visitors, providers, couriers, etc.) • Visitors to secure areas are escorted by authorized personnel at all times • All employees / contractors / etc. must display security ID badges at all times • All secure and perimeter areas are monitored 24x7x365 by CCTV.	
21.3 If a third party is involved, will Brock have access to the third party's SOC 2 and / or any other independent security / control audit / assessment report(s)?	

22 Incident management	
Consideration	**Response**
22.1 What is the provider's incident response procedure for handling a security or data breach?	
22.2 Does the provider's incident response plan comply with industry standards for legally	

22 Incident management	
Consideration	**Response**
admissible chain-of-custody management processes and controls?	
22.3 Is the provider capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?	
22.4 Describe Brock's process to report an incident to the provider.	
22.5 Describe the provider's process to report an incident involving Brock's environment / data to Brock.	
22.6 Describe the provider's reporting mechanism for security and / or other incidents. In what format do notifications go out, and what information do they contain?	

23 Independent audit / assessment	
Consideration	**Response**
23.1 When are audits conducted (i.e., frequency)? What standard / certification is used to conduct audits (e.g., ISO 27001, SSAE 16 SOC 2, etc.)? Will Brock receive a copy of the audit report when finalized? Is this requirement outlined in the contract with the service provider?	

23 Independent audit / assessment	
Consideration	**Response**
23.2 Does Brock have the right to audit the provider? If so, is this right outlined in the contract / terms of service? If not, why not?	
23.3 Does the provider perform regular vulnerability assessments / penetration tests to determine security gaps? If so, state the date of the most recent vulnerability assessment / penetration test and provide a comprehensive list of all security risks / gaps identified.	
23.4 Have the most recent security risks / gaps identified been mitigated?	
23.5 If a third party is involved, will Brock have access to the third party's SOC 2 and / or any other independent security / control audit / assessment report(s)?	

24 Relationship management	
Consideration	**Response**
24.1 Will the area assign a Vendor Relations Manager (VRM) to oversee the relationship with the provider?	
24.2 Has an internal process been established to formally review the provider's performance at least annually against the contract and Service Level Agreement in collaboration with Information Technology Services? If so, attach the Procedure. If not, please explain.	

24 Relationship management	
Consideration	**Response**
24.3 Has an internal process been established to formally review the contract with the provider at least annually? If so, attach the Procedure. If not, please explain.	

25 Local administration	
Consideration	**Response**
25.1 Who will be the local administrator in the department / area? Consider: • Set-up and configuration of Brock's environment in the solution • Ongoing maintenance and administration activities • User set-up and administration • Roles set-up and administration • Monitoring and oversight including periodic reviews of access rights to data. If a consultant will be involved in any of the activities outlined above, detail the consultant's role and turnover to Brock (if applicable).	

26 Area's business continuity	
Consideration	**Response**
26.1 Will the area be developing a business continuity plan for when the solution / service or data is not available? If so, by when? If not, why not?	

Date submitted: [enter]

Appendix: Definitions

Cloud computing service models		
Service model [1]	**Description**	**Considerations**
IaaS	Capability to provision processing, storage, networks and other fundamental computing resources, offering the customer the ability to deploy and run arbitrary software, which can include OSs and applications. IaaS puts these IT operations into the hands of a third party.	IaaS can provide infrastructure services such as servers, disk space, network devices and memory.
PaaS	Capability to deploy onto the cloud infrastructure customer-created or customer-acquired applications developed using programming languages and tools supported by the provider	PaaS is designed for developers.
SaaS	Capability to use the provider's applications running on cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based e-mail)	Applications are complete and available on demand to the customer. Traditional licensing and asset management are changed.
Source: Pijanowski, Keith; "Understanding Public Clouds: IaaS, PaaS and SaaS," Keith Pijanowski's Blog, 31 May 2009, www.keithpij.com/Home/tabid/36/EntryID/27/Default.aspx		

Cloud Deployment Models	
Deployment model [2]	**Description**
Private cloud	• Operated solely for an enterprise • May be managed by the enterprise or a third party • May exist on- or off-premise
Public cloud	• Made available to the general public or a large industry group • Owned by an organization selling cloud services
Community cloud	• Shared by several enterprises • Supports a specific community that has a shared mission or interest • May be managed by the enterprises or a third party • May reside on- or off-premise
Hybrid cloud	• A composition of two or more clouds (private, community or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)

Reference: http://www.erpsoftwareblog.com/2011/05/cloud-saas-and-hosted-whats-the-difference/

Hosted

[1] IT control objectives for Cloud computing, ISACA, 2011, Figure 1.2, p. 11

[2] IT control objectives for Cloud computing, ISACA, 2011, Figure 1.3, p. 13

"… Hosting essentially means you buy your software solution from a publisher or Value Added Reseller (VAR) …. You would then have the software installed at a data center or 'hosting center' where either physical or virtualized servers that you own/lease/finance are setup. You then would implement the solution very much like it would be implemented 'on premise' or at your offices.

Payment stream wise, you would have a large upfront software payment, a price for hourly or project based implementation, possibly an initial provisioning fee from the hosting center, and then a monthly fee for the rental/usage of the hosting center's equipment, people, and bandwidth. Your long term ongoing fees would including the monthly hosting fee, an annual software 'maintenance' fee which covers bug fixes and new versions, and any hourly billed or annual contracted phone support from your VAR. You may have a cost every few years to the VAR to upgrade the software to the latest version along with moving any modifications you had done.

Advantages:

- *You 'own' the software (actually indefinite license). You only pay once beyond the maintenance which is usually between 15% and 20% depending on software publisher. If you stop paying maintenance the software will continue to work at the version you are on.*
- *Your data is in a very secure data center which may also have/offer multi-site redundancy in case of disaster. Backups are being made reliably and you can connect from almost anywhere*
- *You can still bring your application back in house down the road with little interruption. Most hosting centers use "Virtual" servers like VMWare or Microsoft Hyper-V. You can take your 'server' and run it on your own physical hardware quickly if you use VMWare or Hyper-V*

Disadvantages:

- *The monthly hosting cost may exceed in house costs long term, depending* [on] *variables such as other non-hosted solutions you have in house, etc.*
- *If your office Internet connection goes down, you have no access to your system (redundant internet lines to your office can help alleviate this risk)*
- *If you want to integrate other solutions to your ERP system, you usually have to have that solution supported and installed at the hosting center as it is difficult for local applications to real time integrate with hosted applications.*
- *You need a fair amount of bandwidth. Especially if your application works with scanned images and photos as the upload and display of those can clog your Internet 'pipes.'*

Cloud Computing

Cloud computing usually refers to deploying software similarly to hosting, but the servers are very virtualized … Your application isn't really running on any one server, but rather is 'shuttled around' or even spread over multiple servers in real time as demand requires it. Most applications need to be modified or written to fully take advantage of the cloud so that they can run across multiple servers … You 'rent' servers, communications and messaging capacity, data storage capacity etc. Usually you are charged based on usage in tiny increments that add up to real dollars but scale well from trial environments up to global solutions.

A solution that can be 'hosted' could also be put 'in the cloud' and it is that deployment model that is easier to resell to end user customers since it is more scalable and can be duplicated more easily for new customers.

Advantages:

- *Cloud computing allows small developers to provide a software application to customers at a very affordable price … Facebook uses cloud computing … Even Google can be defined as cloud computing as your search is handled by thousands of different servers at any instant based on worldwide demand.*
- *It's not difficult to make a traditional in house solution work in the cloud. The rewriting is minimal.*
- *You usually don't have significant upfront hardware setup or acquisition costs as is often the case with hosting.*
- *Like Hosting, you get data security (hopefully), redundancy, and unlike hosting, you get almost unlimited scalability.*
- *Software can be outright sold, or 'rented' in this model*

Disadvantages:

- *Over time the transaction costs that are passed through to the customer from a company that uses Cloud architecture can exceed on-premise solutions.*
- *Existing applications often need some rework to properly take advantage of the cloud.*
- [It’s] *not so easy to take a cloud hosted application and bring it back on premise due to the distributed nature of the architecture.*
- *It's even harder for disparate applications that need to integrate (such as an ERP & CRM) solution to work in the cloud unless both vendors work together to make that happen. Software vendors can do this, but it's not easy for end-users.*
- *Each application often has* [its] *own fees so if you run many applications in the cloud, the costs can be steep since you don't pay per server, but rather per unit of data or CPU power cycles used.*

SaaS or Software as a Service

SaaS is a hybrid of both a financial and architectural model. As most industry pros describe SaaS, it's usually a situation in which an application was written from the ground up for this model. Cloud and Hosted applications can either be traditional Windows applications accessed via technology such as Citrix, or Terminal Services, or an application that is HTML browser based. SaaS is almost always a pure Web/HTML based solution and is almost always sold on a rental model, typically. X dollars per month, per user. The biggest difference with SaaS applications is that they are usually 'multi-tenant.' This means that one database shares multiple end user customers and they are 'partitioned' from each other via a security model in the application, not via separate virtual servers.

Advantages:

- *SaaS solutions can be financially attractive. You typically have no upfront costs to start using and they are usually 'self provisioning.' SAP Business By Design or Epicor Express are examples of a true SaaS solution. With SAP, you can fill out some basic information and be in a test environment in under 30 minutes.*
- *Multi-tenant applications tend to cost less to maintain and run and can have a lower monthly cost to customers because of this due to the common database.*
- *Often, the services component of implementation and future upgrades is bundled into the monthly fee. It may be easier to swallow $200/user/month than $150,000 for a new ERP solution. Even if the $150,000 is actually cheaper over 5-10 years, the savings of cash is very attractive to some companies.*
- *Since, to be truly SaaS, it's likely the applications were recently developed,* [this] *gives many SaaS applications a 'fresher' look and feel and more modern technology than older applications that were moved into the cloud or are hosted.*
- *The integration between more than one SaaS application (such as ERP & CRM) can be done by the vendors, but is usually difficult for end users. However, when done properly, it can look and work seamlessly, almost as if one solution.*

Disadvantages:

- *Although cheaper up front, the monthly fees, can add up over time to be substantially more than an 'on premise' solution. There are complex ROI spreadsheets done by parties who have interests in both scenarios. SaaS vendors will typically over-inflate the cost of in house IT and upgrades, and premise vendors will typically underestimate those costs. Do your own realistic analysis of the whole picture and look at it over 10 years which seems to be the life of a major ERP system these days.*
- *There is nothing to keep a SaaS vendor from jacking up the monthly fees a year or two down the road after you have invested time and money in implementing the system. With SaaS, if you don't pay, you lose access to your system, period. With on-premise, if you stop paying maintenance, your software continues to operate at the current version level.*

- *Some SaaS vendors have contracts that don't even allow you to retrieve you own data until they are paid in full. This possession of data can be a big sticking point once the lawyers start looking at the contracts.*
- *When the interface is HTML/Web only, many solutions are slower for 'heads down' data entry or are missing the richness of a traditional windows application such as right mouse click drill downs, etc. If you bring up a customer list, many systems will show you 20 records at a time and you hit a 'next' button to browse the next set whereas a Premise/Windows application can scroll through thousands of records quickly.*
- *Since SaaS vendors are popping up quickly and many are only operating due to Venture Capital or other equity money, their long term survival is questionable as the inevitable consolidation occurs. If your SaaS vendor goes belly up, even if they give you a chance to get your data, it could take months to re-implement a new system. Can your business survive that interruption? With premise systems, if the publisher goes out of business, you can move to a new solution at your own pace"*