Acquiring IT Software solutions at the University of Guelph

When considering any IT software solution, due diligence must be taken to ensure that we have done all that we can to protect our investment and UG assets. Whether the solution is to be hosted on University of Guelph premises or up in the “cloud”, the following information may aid in your decision making.

# Requirements Gathering

This document assumes that you already know what you need in a software solution. You should already have documented your business objectives and the functional requirements of your solution.

CCS does offer Business Analysis services where we can assist in your requirements gathering, and deliver a requirements document suitable for use within the procurement process.

# Pre-product search

It is possible that UG already has a product that meets your needs. Check your requirements with any existing product(s) that UG has. Using existing systems can save time in procurement, save money by leveraging existing vendor relationships and product knowledge. Also, using existing systems may mean required integrations with other UG systems are already in place.

Do consider if you are able to modify your requirements or processes in order to accommodate existing solutions.

CCS can assist in this determining whether or not existing products exist, including reaching out to Purchasing and our IT partners on campus.

# Product Search

There are various ways to find the product that best meets your needs (Google searches, Gartner research, asking your peers (on campus and at other Universities), CCS, UG Purchasing tools). In all cases, you must follow UG Procurement Guidelines (<https://www.uoguelph.ca/finance/departments-services/purchasing-services>). Purchasing can be reached at [purchasing@uoguelph.ca](mailto:purchasing@uoguelph.ca).

## Cloud or UG Infrastructure

Products can be implemented on your own infrastructure, CCS infrastructure or hosted in the “cloud”. In all cases you must ensure that the infrastructure meets UG security standards. Guidelines on security are provided later in this document.

If security guidelines are met, cloud can solutions can be a strong option for you to consider.

Benefits of Cloud solutions

* Quick implementations
* Reduced capital investments in infrastructure, including quicker to scale
* Vendor is responsible for infrastructure support, lessening IT knowledge required by UG
* Access to cloud solutions may require less network configuration, especially when accessing remotely

Disadvantages of Cloud solutions

* Loss of control. Often upgrades are implemented by vendor across all clients with no opt out capability. Upgrades can require changes in your workflow process which were not planned
* Integrations with other UG systems may be more difficult
* There may be hidden costs, such as minimum usage charges or other.
* Implementation of Security Vulnerabilities is at the priority of the vendor
* Vendor management can be more challenging

In all cases, customization of any solution can be costly. Are you prepared to modify your business processes if necessary to accommodate the solution?

# Before purchasing

Before purchasing any solution, there are many items that should be considered. Ensure that you follow all procurement policies and procedures of UG Purchasing. There are processes to follow if the cost of the software meets certain thresholds. Contact [Purchasing](mailto:purchase@uoguelph.ca) for details.

## Privacy and the Law

Determine what type of data this solution will be expected to handle. Various laws exist in the definition and protection of private data (consider [PIPEDA](https://www.priv.gc.ca/leg_c/leg_c_p_e.asp)/[PHIPA](https://www.ipc.on.ca/english/PHIPA/)/[FIPPA](http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90f31_e.htm)). If the system that you are considering may contain data that is defined as “private”.

UG has created a [Research Data Classification Guideline](https://www.uoguelph.ca/cio/it-security-pmo/it-policies-guidelines/it-guidelines/research-data-classification-guideline). This document describes guidelines for categorization and security of research data. However, it is also intended to be able to serve as a blueprint for a more general data classification policy or guideline.

If your solution may contain data that is defined as “private”, a formal Threat and Risk Assessment (TRA) and/or Privacy Impact Assessment (PIA) is highly desirable. The objective of a TRA is to evaluate the threats and risks to the University in the use of the proposed solution. A PIA is designed to ensure compliance with the University’s privacy protection responsibilities. The UG Secretariat has stated that “ideally, a PIA will be performed for all systems that handle private information, whether the data is stored on premise or in the cloud”.

According to the UG Information Security Office a TRA/PIA must be performed if your application will involve payment services ([PCI standards](https://www.pcisecuritystandards.org/security_standards/index.php), described below), provides a competitive advantage (such as research data) or in any way could put the University at a disadvantage should there be a data exposure.

“[Privacy by Design](https://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf))” by Dr. Ann Cavoukian, Ontario’s Information & Privacy Commissioner from 1997 to 2014 provides 7 excellent guiding principles on ensuring privacy is designed into your processes.

To better understand what data is considered private and how to engage in a TRA and/or PIA, discussions should be held with the [UG Information Security Office](https://www.uoguelph.ca/ccs/infosec) and [UG Secretariat](https://www.uoguelph.ca/secretariat/office-services-privacy-and-access-information/privacy).

## Payment considerations

If your system will provide payment capabilities you must verify the vendor’s [PCI compliance](https://www.pcisecuritystandards.org/security_standards/index.php). There are strict legal and audit requirements to ensure safe payment processes. You should also discuss your application payment process with UG’s [Revenue Control](https://www.uoguelph.ca/finance/departments-services/revenue-control/credit-and-debit-card-payments-and-processing/web-based-e-comme) (ext. 56768) for guidance on proper accounting and setup procedures.

## Data Privacy and Best Practices

Ensure that you minimize the private information collection. You also have a responsibility to inform those that have their data stored on your system be informed of what you collect and for what purposes.

Considerations:

* Are you keeping the minimum personal information necessary? Make decisions on what data you keep based on value and risk. If you have a privacy breach, what is the potential liability to the university (reputational and monetary)?
* Will there be limited access to the personal information and only by those employees authorized to access? Consider a formal process to authorize access.
* Are there any audits to verify or report on access? Consider access by:
  + UG affiliated – staff, faculty, students
  + The vendor
  + The public
* Does the person whose information you have understand what you are doing with this information? How will they be informed?
* How will you ensure that the data will only be used for purposes for which it was intended?
* How long will the personal information be kept for? What processes do you have in place to ensure that it is deleted when it should be?

## Data and Security Access

Consider the following if the software solution resides in the cloud or if the vendor has the ability to access the solution:

* You should ensure that UG retains all rights, ownership and control of the data.
* Ensure that you read and can accept the vendor’s statements on privacy.
* Does the vendor have any rights to use and share our data (aggregated or not)? Where ever possible you should limit the service provider to using your data for your purposes only, and for no other purpose unless you explicitly consent.
* Include a provision that the service provider holds your data “in trust” for you, making it a legal fiduciary.
* What policies and procedures does the vendor have in place to ensure that their own staff do not have access to our data?
* What policies and procedures are in place to detect, prevent, and mitigate identity theft?
* Will the data reside on UG-premise, within Canada, the USA, or other country? Is this a concern? Why?
* Discuss how the vendor provides backup and recovery of your data. Are backups stored off-site in a physical location away from the “live” data?
* Discuss how the vendor provides disaster recovery and business continuity of their environment.

## General Security

Irrespective of the type of data that you store (private or not), security of the data should be a high priority. The university will want to ensure that your vendor is following best practices when it comes to the protection of UG information.

If the software solution will reside in the cloud, have the vendor:

* Indicate if the vendor has filled out the self-assessment form of the STAR registry on the Cloud Security Alliance (CSA) site (<https://cloudsecurityalliance.org/star/?r=2523#_registry>). If not, request that they do so (<https://cloudsecurityalliance.org/star/self-assessment/>). CSA STAR Self-Assessment is free and open to all cloud providers and allows them to submit self-assessment reports that document compliance to CSA-published best practices.
* Discuss their security policy and provide any IT Security Whitepapers that they have.
* Provide all security certifications and audit results.
* Discuss how they separate UG data from their other clients (data segregation).
* Discuss what security controls they have in place including physical access, Next Gen firewalls, Intrusion Detection Software (IDS), Intrusion Prevention Software (IPS), network segmentation, threat detection tools, vulnerability scanning, penetration testing. Does UG have access to any of these reports?
* Discuss their Security incident event management - logging security incidents
  + Do they use SIEMs to detect incidents?
  + Can their log data be utilized by UG’s SIEM?
* Discuss the security patching process of their systems (OS and application). Ensure they include frequency, how they address critical security patches, impact to the availability of their system and testing.
* In case of a security breach, what is their incident response plan? How and under what circumstances do they notify UG?
  + Who is liable for any breaches or unapproved exposure of our data?
* Have there been any instances of identity theft experienced by the vendor in the last two years?

If the software solution will reside on UG Premise

* There will be an expectation that CCS will perform a Security Vulnerability Assessment on the product. The vendor must agree to work with UG to remediate any critical or high impact vulnerabilities after installation is complete, preferably before payment is issued for the product.
* Have the vendor discuss the security patching process of their systems
  + If the vendor is contracted to patch our systems what access does the vendor require? Ensure that access is through secure protocols and that the vendor does not require unmonitored access
  + If UG IT staff will patch the systems, ensure that the IT staff have the required skillsets

Regardless where the solution resides (cloud or on UG premise) ask the following of the vendor:

* Do they encrypt data at rest (where it’s stored, including the database layer) and through transmission ([HTTPS](http://en.wikipedia.org/wiki/HTTPS) ; [TLS/SSL](http://en.wikipedia.org/wiki/Transport_Layer_Security)).
  + How are encryption keys stored and secured?
  + What encryption technologies are used?
* Have the vendor discuss authentication method to their application:
  + If they have their own authentication, what is it:
    - Password reset process
    - Password strength
    - 2-factor authentication
  + If they will be integrating with UG’s authentication, have the vendor discuss what they support:
    - Single Sign On (SSO) vs LDAP vs Active Directory (AD)
* Have the vendor discuss their practices around software development
  + Independent audit
  + Segregated duties and development platforms
  + Software Development Life Cycle

## Vendor Considerations

Having a solid product which meets your business and security needs are vital. However, it is also critical that you select a product backed by a vendor which will meet UG needs. You will need to work with the vendor to develop acceptable working relationships. Consider the following:

### Vendor – General Considerations

* Utilize our [Gartner](https://ja.lib.uoguelph.ca/gartner/gartnerlogin.cfm) subscription to research the vendor and its position in the market place.
* Understand the vendor’s ability for scalability and redundancy.
* Can they handle your business cycles?
* Evidence of commitment to high quality standards ISO 9001, ISO 14000/14001, Six Sigma
* Review the vendor’s customer base (including Canadian Higher Education clients).
* Do reference checks.
* Understanding the vendor’s history and financial position may be useful. Is the vendor a likely acquisition target or is the vendor large enough and growing (acquiring other players within the industry)? Often changes in company ownership leads to ‘licensing model changes’ that will may impact your costs.
* Does the vendor hold product conferences?
* Are there user groups in existence and are they affiliated with the vendor?
* What is the quality of the vendor’s documentation, online support portal, etc.?

### Vendor – Support Model

* When is the vendor available for support and does it meet your needs
  + e.g. 24 x 7 response based on urgency levels
  + e.g. 9:00am to 5:00pm Pacific Time Zone
  + How do we escalate issues to vendor management, if required
* What are the expected response times
  + Look for a SLA that documents different response times and resolution goals based on the severity of the issue. Look for definitions on what determines a Severity 1 vs 2 vs 3, etc.
* How are known issues communicated to their clients
* If your solutions requires customization of the application, how is support impacted?
* Have the vendor explain their change management process
* Does the vendor allow the customer access to the vendor’s database of known problems?
* If the system is installed on UofG systems – how is vendor remote access provided?
  + VPN access – consider what level of access they should be provided
  + How does the vendor ensure that the workstations that will connect to our infrastructure meets acceptable standards (i.e. antivirus, up to date patches and OS, password policy, encryption, etc.)
  + Can UofG monitor their access during support and/or receive an audit of activity, including changes made?
* Not only should you ensure that the vendor provides you adequate support, you must also consider what resources, skills and time the vendor requires from you. Do you have the in-house IT expertise to support the system?

### Vendor - Service Level Agreements - Cloud Specific

* If the application is considered highly mission-critical, then consider adding contractual incentives and/or financial penalties to ensure that the provider is duly motivated to support your required service levels.
* What are their guaranteed uptimes and how is it defined and monitored?
* What monitoring is in place?
* What is the escalation process?
* When does the vendor do (scheduled) maintenance on the system?
  + Will the system be unavailable?
  + What notification do you receive?

### Vendor – Implementation services

What does the vendor provide in terms of: business analysis, project management, training (onsite, webinars, vendor locations, etc.), documentation, and statement of work (SOW)?

SOW Considerations:

* Setting out the scope of the work and all the deliverables required from the vendor. How are scope changes addressed?
* Roles and responsibilities of both parties
* Testing and the acceptance process for services
* Payment for expenses (according to Public Sector rules)
* Data access rights of vendor
* How system access is provided to vendor
* Success criteria
* How well does vendor understand the Canadian Higher Education landscape and culture?
* Risk management
* Does the vendor provide a Project Manager? Can you obtain a default project plan?
* Does the vendor provide any architectural documentation?

## Product Considerations

### Accessibility requirements

Does the vendor comply with the Province of Ontario’s AODA legislation?

### Branding

Do you need U of G branding? Does the product support the level of branding that you desire. Also, you should work with Communications and Public Affairs on branding restrictions.

### System Access

How do you gain access to the vendor’s application?

* If web-based, determine what browsers the vendor supports including Safari, Firefox, Explorer and Chrome, including versions. Do you need a new website URL? Work with CCS to understand its feasibility and Communications and Public Affairs to obtain approval for its use.
* If the software requires desktop software to be installed, determine how this will be completed and who will provide ongoing support, including patching.
* If the software offers a mobile version, does it include Blackberry, Windows, IOS, Android versions? Some vendors do not offer mobile apps, but design their product to be “responsive” to the screen sizes accessing the product. Check with your vendor.
* If you will allow access to the product from off campus, is VPN or other secure access required.
* If you only wish to allow access to the product from on-campus, CCS can assist in the appropriate network configuration.

### Integration

Often you will need to integrate data from other systems into your product. Consider the following:

* What data do you need from other systems (student / staff / faculty)? Do you have the correct approvals. Contact the data owners (staff/faculty = HR ; student = Registrar) and complete the required Information Sharing Agreements. Ensure that CCS is aware of these requirements early in your process so that they can plan for the resources required to meet your request.
* At what frequency do you need this data (real time, daily, on-demand). Often exports/import functionality is adequate, otherwise you may need to determine if the vendor provides API (application program interface) capabilities. Ensure that they provide this documentation up front.
* Does your staff have the technical expertise to write API’s?

### Peripheral Equipment

Does your product require additional equipment such as scanners, printers or point-of-sale equipment? If so, determine if the product will work with existing equipment or if you need to make additional purchases.

### Reporting and Customization

Ask yourself if the product’s built-in reporting functions are adequate for your needs. Sometimes vendor off-the-shelf or customized reports are not enough. Consider if you need special reporting tools. Also determine if you can securely export data to UG systems for backup/reporting/other needs.

Does the product require any customization (functionality or within reporting). Ensure that you understand how this is prioritized and billed by the vendor. Understand the process required by the vendor, including timing considerations and cost.

## Infrastructure and Operational Considerations

### Data Centre

Not only must an application be secure, but the physical access to the supporting infrastructure must be secure as well.

* The following links give insight into Physical Access considerations
  + <http://en.wikipedia.org/wiki/Data_center#Data_center_tiers>
  + <http://www.sans.org/critical-security-controls/>
  + <http://www.sans.org/reading-room/whitepapers/awareness/data-center-physical-security-checklist-416>
* External certification in the form of a SAS 70 Type 2 audit is helpful
* Obtain all data centre certifications from the vendor (SOC2, SOC3, ISO, etc.)
* If possible, have a site visit
* Is the Data centre owned and operated by the vendor or outsourced to a third party such as AWS or a hybrid? Is this acceptable to you?

### Storage and Backup

Do investigate your storage and backup options. Whether cloud solutions or hosted on premise, consider the following.

* Who’s responsible for storage and backup?
* Are backups stored offsite and in a secure location?
* How will it be tested?
* What is the recovery process - at what level (record, day, entire system, checkpoint recovery)?
* Disaster recovery – how is it tested?
  + what are the contingency plans
  + what are your business continuity plans
  + how does one request restore (SLA) – back to a date, or a transaction.

### UG Hosting Considerations

If system will be installed onsite at UG what infrastructure is required (e.g. CCS data centre, networking considerations)? Keeping infrastructure compatible to a CCS supported environment will reduce costs, improve reliability and performance. Ensure that CCS is well informed of your requirements.

Will the solution require formal Production / Development / Test environments? Although there are cost implications, having multiple environments allows for proper testing before moving changes to a production environment.

Other considerations:

* Can the OS of this server be patched automatically? If not what schedule is required? Do patches need to be tested before deployment on production server? Who will do these tests?
* Who will do service / server performance monitoring?
* What resources are required and who will monitor these resources and do capacity planning?
* Who will do the lifecycle planning for the Application Software, Operating System Software, and underlying hardware
* Are the servers required to be under maintenance? 4 hour? Next business day?
* When there are performance issues with the system, who will do the issue management?
* In what intervals does the vendor perform requested changes (i.e. requested changes to functionality or content/fields)? Does this meet your requirements for flexibility on a day to day operational basis?

## Licensing and Contract

### Licensing

Vendors often offer various cost options. Consider the following

* Can you leverage existing licenses, including any consortium agreements that may be in place?
* Does the product require other software products to be acquired? For example, you may be required to purchase Windows or Red Hat OS, Tomcat, Microsoft Visual Studio, reporting tools, etc.
* Some vendors require you to license your own database. CCS can assist with this.
* Concurrent vs named licensing. What is the model offered and how does the vendor track usage or compliance to the licensing model selected?

### Contract Considerations

Review the vendor contract carefully. Not surprisingly, vendors will attempt contract language that favours their own company. Consider the following in your contract negotiations.

* Ensure that the contract is in compliance with UG’s Purchasing policies and procedures.
* The University does subscribe to [Gartner](https://ja.lib.uoguelph.ca/gartner/gartnerlogin.cfm), who can review some vendor contracts and provide feedback. CCS can assist with this.
* Ensure non-automatic renewal. Often vendors will attempt to automatically renew your contract unless you provide written notice of termination 60 days prior to the contract expiration. Do not allow this.
* The contract should have a clear start and expiry date.
* No term greater than 5 years should be accepted
* Changes to contract require written notification/acceptance
* Any schedules or appendixes referenced in the document must be attached to the contract
* If possible, request that the vendor accepts Ontario as jurisdiction in legal matters
* Ensure Non-Disclosure Agreements and/or Confidentially Agreements are signed by the vendor.
* What are the Terms of Use of the product? Do you accept them?
* Ensure you understand if the contract is priced in Canadian dollars or another currency. It would help if the contract is payable in Canadian dollars (minimizes the exchange rate risk).
* Can you cap price increases on yearly maintenance or subscription fees. An increase tied to an annual rate of inflation (or less) is reasonable.
* Understand the preferred length of contract. You may be required to complete a competitive bidding process just to renew the license for an existing piece of software, so the length of the contract is important to understand for planning purposes.
* Payments – verify terms
  + Standard paying term is net 30 but some vendors are more aggressive to collect payments. If so, they should be asked to sign up for [EFT](https://www.uoguelph.ca/finance/departments-services/procurement-and-payables/payments-reimbursements). This will ensure payments with tighter deadlines (i.e. net 15) are promptly completed.
* Ensure you consider additional costs - Professional Services for implementation, hardware, software, maintenance, ongoing internal/external support
* Is the vendor permitted to bring in additional third party resources without your approval?
* Do not have statements allowing the other party to use the University’s name in any advertising, endorsement or promotion
* Do not have wording to allow the other party to assign the contract to a third party without written consent.
* How can the contract be terminated, and what are the penalties?
* How do you get your data back after termination?
* How will the vendor delete your data from their systems after termination? Will the vendor provide a certificate of destruction?
* If you are acquiring a custom developed application, does the University own the application code base? Consider how you will ensure that the software is enhanced, supported and patched for the lifetime of the application.
* If the company goes bankrupt, what happens to the application code base and your data and how do you continue to do business?

# Conclusion

This document provides many areas for consideration when choosing both vendor and software solution. These guidelines should not be considered complete or a guarantee of success – however, following these guidelines will certainly improve the likelihood of success.

Engage in your campus partners for assistance:

* **Computing and Communications Services** – CCS is the central IT department on campus, providing IT infrastructure and central technology services to the U of G community. This includes network and telephony, infrastructure hosting and management, helpdesk functions.
  + Website = [www.uoguelph.ca/ccs](http://www.uoguelph.ca/ccs)
  + Email = [58888help@uoguelph.ca](mailto:58888help@uoguelph.ca)
  + Phone = 519-824-4120 ext. 58888
* **Information Security** - The CCS Information Security team is responsible for administering the University of Guelph's comprehensive IT Security program, which includes support for technology, policies, and guidelines, such as the Acceptable Use Policy for Information Technology.
  + Website = [www.uoguelph.ca/infosec](http://www.uoguelph.ca/infosec)
  + Email = [infosec@uoguelph.ca](mailto:infosec@uoguelph.ca)
* **Purchasing** – Within UG Finance, Purchasing is responsible for procurement services.
  + Website = [www.uoguelph.ca/finance/departments-services/purchasing-services](https://www.uoguelph.ca/finance/departments-services/purchasing-services)
  + Email = [purchase@uoguelph.ca](mailto:purchase@uoguelph.ca)
* **Treasury Operations** – Within UG Finance, this group can assist in the e-commerce payment process of your product.
  + Website = [www.uoguelph.ca/finance/departments-services/revenue-control/credit-and-debit-card-payments-and-processing/web-based-e-comme](http://www.uoguelph.ca/finance/departments-services/revenue-control/credit-and-debit-card-payments-and-processing/web-based-e-comme)
  + Phone = 519-824-4120 ext. 56768
* **UG Secretariat Office** – Among other responsibilities, the Secretariat has responsibility for UG privacy governance, including privacy breaches. UG must comply with [PIPEDA](https://www.priv.gc.ca/leg_c/leg_c_p_e.asp), [PHIPA](https://www.ipc.on.ca/english/PHIPA/) and [FIPPA](http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90f31_e.htm) legislation.
  + Website = [www.uoguelph.ca/secretariat/office-services-privacy-and-access-information/privacy](http://www.uoguelph.ca/secretariat/office-services-privacy-and-access-information/privacy)
  + Email = [univsec@uoguelph.ca](mailto:univsec@uoguelph.ca)
* **IT Special Interest Group** – ITSIG members comprise of the many IT professionals on campus. They possess much knowledge about the business unit that they support and the IT components within their unit. They can be reached for general inquiries.
  + Email = [itsig-d@listerv.uoguelph.ca](mailto:itsig-d@listerv.uoguelph.ca)