So you wanna buy some IT stuff...

A practical “How-To” guide for UW organizations on IT Sourcing

# Summary

Before starting the approval process, gather materials that you already have. Review and reflect on how you would explain your goals to as broad an audience as possible. At the end of this document you will find a [one-page worksheet](#_r80pd8impenb) to help with this process.

If you:

* Prefer to work directly with someone in UW-IT, *or*
* Have started the worksheet but would like assistance,

Contact: help@uw.edu
Put “ IT Sourcing” in the subject line and ask for “IT Vendor Risk Management” in the message body.

# Overview

* [5 Holistic Strategic Objectives](#_1sd9j0xcp9o) provide a simple and useful way to frame analysis
* [Tell your story](https://tellyourstorymap.eu/en/) helps others help your organization and avoid duplicated effort
* [Guidance on Specific Procedures and Forms](#_hqk09qhb8dwr) with examples
* [Other resources](#_vd83xpbud6h0) because this a brief guide and not an omnibus
* [One-page worksheet (Job Aid)](#_r80pd8impenb)

This guide relies on plain-language explanation, templates and examples. The approach is intended to empower you to understand this heart of the process and use your understanding to give solid and straightforward answers to questions that approvers, auditors, and other stakeholders may ask about your planned IT investment.

Additionally, you can contact help@uw.edu and ask for additional advisory services and/or training from IT Vendor Risk Management.

# Introduction: UW is boundless

Somebody (probably me) sent you this guide because you have a key role in an effort by your UW organization to invest in information technology in order to accomplish something that is important to your organization. You may have heard that the administrative process is tricky. Perhaps your previous experiences included surprises and frustrations. If you are under the impression that making an IT investment at UW is more involved than other major purchasing decisions, such as buying a family automobile, then your impression is correct.

The process can feel overwhelming. This document was written in response to many people saying that they wished that there was a “how to” guide that was helpful, user-friendly, and candid.

I’ll try to keep the asides to a minimum, but to begin with, it is important to humanize the situation. You might be wondering whose fault it is that the process isn’t as easy as ordering pencils on Amazon. But the situation is neither your “fault” nor the “fault” of anyone else.

Consider the following:

* **Scale.** You work for the largest public agency and one of the largest employers in the state of Washington. Regionally, both in terms of the breadth and depth of academic departments we are by far the largest university in the Pacific Northwest. Nationally, we are consistently one of the top five largest research institutes. In terms of the public impact of the institution, on a daily basis, but stretching back for over a century, the education, research, medical care, and other community resources provided here has affected and does affect the lives of hundreds of thousands of individuals and represents billions of dollars.
* **Law.** The people of Washington have, through their officials and legislatures, expressed interest in how the public’s money is spent: in general, specifically for IT, and with special rules applying specifically to higher education.
* **Mission.** As an organization that is part of the University of Washington, the proposed investment will affect and be affected by University values, policies, and the existing UW IT environment. Both the Board of Regents and the Office of the President have designed policy to reflect this.
* **Diversity.** The combination of scale and *breadth* create a tremendous value to a wide array of stakeholders. There are narrower relevant contexts, such as for physical safety, civil rights, preservation of UW assets and security of transaction. There are always unique considerations specific to your organization and specific to the purposes of the investment.

As a practical matter, IT investments are not a totally stand-alone decision. However, normally there is a primary stakeholder who is the most responsible for the overall success of the investment. Therefore, while there are many specialty subject matter disciplines that may become relevant, ultimately a holistic integration is necessary.

# Five Holistic Strategic Objectives

***How will you know if your organization’s IT investment was a good decision?***

The nature of Information Technology itself and the unifying characteristics of our institution provide some framing parameters that help to identify a few overall goals, or *holistic strategic objectives*.

In developing IT Vendor Risk Management, the UW-IT Senior Leadership Team were each interviewed separately and asked to describe their overall goals for all IT Vendor relationships. The answers consistently focused around five objectives:

1. Vendor products and services deliver high **quality** performance.
2. The vendor has **accountability** to UW for their behavior and performance quality.
3. The investment is a good **value**.
4. The **operability** of the technology and vendor support is reasonable for IT service teams.
5. Technology is used in ways that satisfy both regulatory **compliance and ethical** factors affecting UW stakeholders.

Before we go into more details about objectives, it’s important to understand that the value of the consensus amongst UW-IT Senior Leadership Team is in their collected expertise. Under UW policy ([APS 2.6](https://www.washington.edu/admin/rules/policies/APS/02.06.html)), the Executive Head of the Major University organization ultimately owns the risk associated with their IT assets within that organization. This federated governance structure enables each UW Organization to tailor their IT priorities to better align with their approach to the UW mission.

-Before using the Five Holistic Strategic Objectives, you’ll want to brainstorm about your desired outcomes and how you will know those outcomes have been achieved. This is a “big buckets” approach and it is okay to place the same idea under more than one objective.

###

### Objective 1: Quality

***How well does this technology work?***

It is necessary to have a standard of quality that is focused on UW stakeholder interests and evaluated holistically, but this simply cannot be expected to come from the vendor.

That is not a pejorative statement. Vendor sales representatives will suggest a definition of quality that is calculculated to emphasize the strongest features and best functions of their products and services. A subtle version of this marketing effort takes the form of vendors demonstrating that they are “certified” against a particular industry standard, or when the vendor carefully metrics some aspect of their operation as a way to provide performance data (e.g., availability). While this information is both useful and relevant to collect and review, it is not sufficient to simply look at desirable features.

Instruments and evaluations by experts can help to assess technical design, accessibility, security, privacy, PCI, et cetera. When relevant, it is important to have these considerations inform the balance of risks to your organization.

Therefore, the idea of **Quality**, as presented in this guide, should be broad. Beyond just a particular feature, or a specific compliance worry, the real-world effects on your organization and others should be considered.

|  |
| --- |
| **Rule of thumb**:When technology is well designed, a high level of quality is the default assumption; both users and system administrators will assume that the product “just works” without feeling unduly impressed or pleasantly surprised.  |

###

### Objective 2: Accountability

***How mature is the vendor? How much control is granted to the customer?***

These determining factors can be evaluated both in terms of the vendor’s technology and the vendor’s business. It can be helpful to visualize this as a matrix:

|  |  |  |
| --- | --- | --- |
|  | **Technical** | **Business** |
| **Control** | *e.g.* System administrators can programmatically make API calls or retrieve system logs and obtain relevant information. | *e.g.* In the event of vendor’s breach of contract, the vendor is nevertheless required to continue to provide services during some period of transition.  |
| **Maturity** | *e.g.* “Out of the box” instrumentation makes sense in the context of the product’s actual use. | *e.g.* The vendor warrants that the product will work in accordance with their documentation and has mature DevOps patch management practices. |

Accountability tends to be an especially pernicious risk for IT investment projects. The structure of the matrix itself lends insight into some reasons why this is:

* The horizontal divisions of the matrix deal with the difference between accuracy and precision. Although insufficient levels of control granularity may be frustrating, for both a technological platform and a business operation, there are challenges to ensuring that these controls are ubiquitous, pervasive and consistent.
These challenges vary, but they aren’t inherently more difficult for a large vendor versus a small vendor, nor for an established vendor versus a start-up.
Finally, it is rarely the case that a vendor’s overall accountability is uniformly one way or another: Some control areas will have more depth, some control areas will have a more mature implementation.
* The vertical division is an observation that there tends to be a difference between vendor personnel who are oriented towards technical operations or engineering and those who are oriented towards sales or customer service. While this ought to be a false dichotomy, as a practical matter, it is often necessary to take an interdisciplinary approach to assessing how accountable the vendor is to its customers.

|  |
| --- |
| **Rules of thumb:** * The vendor systems’ actual control interfaces and the technical documentation tend to be good evidence of the vendor’s technology.
* The vendor’s contract (both what is in it and what is omitted) and the vendor’s behavior during the solicitation process are good evidence of the vendor’s business.
 |

###

### Objective 3: Value

Value is a calculation of the total cost of ownership and return on investment that goes beyond the invoice cost for licensing and support. Considerations here include:

1. How well will the system scale or perform under different conditions and workloads?
2. On an annual basis, how often will the system need to be taken down for maintenance or to resolve unplanned issues?
3. What is the expected severity and complexity of unplanned issues?
4. What is the expected lifespan of the system?
5. What is the estimated cost of implementation divided over the lifespan of the system? (Amortized implementation cost)
6. Is the sum of the annual maintenance and amortized implementation costs greater than the ongoing costs associated with the legacy system?
7. What is the value to the organization of new functionality from the proposed system that is not currently a function that the legacy system is capable of fulfilling?
8. How long will it be before the functional equivalents of the bespoke capabilities of the legacy system are fully implemented in the new system?

|  |
| --- |
| **Rule of thumb:**Inherent in analysis of **value** is the search for costs and benefits that are hidden. **“Hidden”** has several practical implications:* Identifying costs and benefits requires making inferences.
* Certain predicted costs and benefits can only be identified qualitatively and not estimated quantitatively.
* Qualitative values are often **incommensurable** and not **fungible**.
* The same empirical evidence can be evidence of different values and measures differently for each.
 |

###

### Objective 4: Operability

Even if the vendor and/or the vendor’s technology is considered the reference for its field, it is important to consider the amount of immediate and long-term strain on the existing environment that is being introduced with the new technology.

|  |
| --- |
| **Rules of Thumb:*** The vendor’s proposed allocation of risk should seem intuitively **fair**.
* The vendor’s service structure should be **relevant** to your day-to-day operations.
* In the context of how often and how significantly you expect to need to change (e.g. daily, each term, annually, never, etc.), the vendor’s **change control** mechanisms should be appropriate.
 |

###

### Objective 5: Compliance and Ethics

Consider how the technology works and how the vendor operates. Specifically, when assessing vendor proposals and counter-proposal, consider the potentially adverse impact on the interests of University stakeholder communities.

The vendor starts demonstrating their culture, value, and character from the very first interaction and, in some way, recapitulates it with every contact; *and vice versa*.

It is not realistic to expect that UW’s pro forma contract documents are a perfect fit for every vendor. However, there is a big difference between a vendor who reads our documents with the goal of creating a pragmatic contract and a vendor who summarily rejects our documents.

It is also important to recognize that UW values are not a homogeneous monolith. Often there are organization-specific and use-specific contexts. For example, *physical safety is* related by different considerations in the context of a venue versus human subjects research.

|  |
| --- |
| **Rule of Thumb:*** Relative to vendor’s other customers and business lines, UW ought to be part of the vendor’s core market or a target vertical market. There is greater risk of serious value tensions when the vendor’s Higher Education service offerings are tangential to the vendor’s core business.
* Be aware of when a plain-language term is used to describe an ethical principle because it may have different meaning to different disciplines. For example: **Good**.
 |

##

# Tell Your Story

## Background information to gather about the environment and stakeholders

Avoid reduplicating past efforts and instead try to use existing data and documents. Almost every source of information that you have will help: Internal documentation, web pages, presentations, artifacts of work processes (e.g. closed help desk tickets) and correspondence are all valid. In gathering these materials, try to find either the most “canonical”, most clear or most accurate description of each of the following:

|  |  |
| --- | --- |
| **Information to gather** | **What/Why** |
| **Organizational Mission** | This could be as concise as a single phrase on your organization’s internet-facing home page.  |
| **Program or Service** | What your UW organization is offering to those communities that your organization helps. Specifically, those offerings that will be changed by the proposed IT system. |
| **Duties to customer** | How the communities of stakeholders are helped by your organization’s programs, especially where those communities rely upon your organization’s program. |
| **Legacy system**  | Is this a totally new capability with no previous legacy? Is the “legacy system” not really a formal IT system? (e.g. There is a living document in Excel that tracks a pipeline of Word documents through a hierarchy of subfolders in a shared file directory, and over the years a shared understanding of how to navigate this has evolved between colleagues.)Otherwise: What is the name of the existing system(s) that everyone uses? Often this is the name of the vendor rather than the product name (e.g. Oracle) |
| **Workflow (Architecture)** | Is there any documentation that identifies:* The systems upstream and downstream of the proposed system?
* The system boundaries and interface points?
 |
| **Team Roster** | Identify the people in your organization that will use and/or support this system. However identify them by **role name** rather than individual name. (e.g. “There are two *reviewers*” rather than “Waldorf and Stadler will use this system.”) |
| **Executive Head of the Major University Organization** | Who within the organization will formally own the risk? |

It is likely that you will discover *other relevant information* that does not fall into any of the above categories. It is also likely that you will have *little or no information* written down about some of the above categories. This is not a bad thing! It turns out that both of these are important discoveries:

* The *other relevant information* tends to be **organization specific** **considerations** that need to be explained to a wider audience who may not appreciate the proposed IT investment without this additional context.
* Discovering that there is *little or no information* about something is a way of identifying a **known unknown.**

|  |
| --- |
| **Rule of Thumb:*** The proposed investment is a plan that starts in the current state of your organization and goes from there.
 |

##

## Situational Narrative (Motivation)

In parallel with gathering background material, it helps to compose a brief *situational narrative* that you can adapt and re-use at various points throughout the process. The situational narrative describes the driving *motivation* behind the IT investment effort. IT investment tends to be driven by a combination of two factors:

* A new or developing situation creates a need or opportunity.
* The organization hopes that an IT investment will improve the organization’s ability to bring benefits and reduce harms to constituent stakeholders.

Ideally, the explanation for the motivation can be understood by a broad and diverse audience.

|  |
| --- |
| **Sample motivations:*** **A last straw event will affect the rights of a large number of stakeholders:**UW’s legacy system was developed in-house many decades ago. Although it has been stable for a long time, once *the WA legislature enacts its new regulation on this activity,* it will not be possible to continue to operate the legacy system. This system is needed for *all undergraduate students* for *civil rights protections***.**
* **Developing situation**Because of *COVID-19*, the *venue* needs to be able to offer a *tool/capability* to *faculty* that enables them to *design immersive online experiences for distance learning.*
* **End of support life**UW has operated the on-premises version of *vendorname productname* for many years. On December 31st of this year, no more security patches or technical support will be available from the vendor. All of our *specific types of records* needed for an *essential activity* are stored and processed on this system.
* **Funding is dependent on using this vendor***NIH* has specified that all participants in a multiple institutional study must contract with a *vendor* to use a *specific* *platform*.
* **Funding is dependent on picking any vendor**The project sponsor has required that to obtain funding for the next phase, there must be a working prototype…
* **Regulatory requirement**To comply with a *law* it is necessary for the department to maintain a database of *specific types of records* and to enable *individual* *members of the public* to request information that UW may be holding about them and why UW is holding that information.
 |

#

# Guidance on Specific Procedures and Forms

This guide does not focus on the specific thresholds for review. Strictly speaking, under either the laws of Washington state or University policy, *any and all* IT investment might be subject to further review. Instead, this guide sheds some light on the general rationale behind why additional reviews happen and their function. Having this understanding will empower you to work through any and all additional reviews in the ordinary course. Additionally, the basis of your investment will be better informed, and you will have opportunities to cultivate intra institutional support that will benefit your organization throughout the life of the system.

As a practical matter, the occurrence and extent of further review tends to be a function of three things:

1. Clarity and transparency of all information provided.
2. Extent and breadth of impact on stakeholder communities.
3. Estimated total cost of ownership.

## Procurement

Procurement Services at the University of Washington have the responsibility for helping UW organizations achieve their strategic objectives from the vendor relationship and to deliver that benefit to the state of Washington. Washington public procurement law reforms went into effect in 2013 and they deal with how competing vendor bids are to be compared, communication with vendors and parameters for good faith negotiation. Depending on the context of the procurement, there are other laws which may apply to public records, accessibility, Information Technology, payment, and many other regulated aspects of how the University does business. Additionally, Procurement Services administer the policy directives of the Board of Regents and President of the University. As such the contract managers within Procurement Services bear a significant responsibility for verifying that the information provided to explain why the University’s (and the public’s) money is being invested is in order and that the process of selection is fairly and consistently applied and administered.

Towards this end, the procurement services provide a tremendous amount of liability protection for the University and for the Executive Heads of University Organizations. Largely, the timeline for proceeding through the procurement process is determined by the level of clear and transparent disclosure by the requesting organization and the level of alignment between the vendor with UW values as demonstrated by their behavior during the sales cycle.

|  |
| --- |
| Rule of Thumb:* Engage Procurement Services as early on in your selection process as possible in order to get the maximum benefit.
 |

### Initiating the RFx process form

In terms of the information collected and analysis process, there is not a huge difference between formal and informal competition. However to determine the correct course of action, Procurement Services may ask for some initial information in order to understand what the required processes are for administering the procurement process.

An example of the **Initiating the RFx process** form can be found here [[LINK](https://drive.google.com/file/d/13bZzMEGrb1Pg7FvlP8t-d62TLlAESk3E/view?usp=sharing)]

The information requested in the form corresponds to your preparation as follows:

* **Purpose and Background**, corresponds to the **narrative**, supplemented by the specific **background information** preparatory material.
* **Selection Criteria** and **Functional, technical and performance requirements** both correspond to the **5 Holistic Strategic Objectives.**

### RFx Guidance and Bid Tabulation Job Aid

If a formal competition is the appropriate course of action, then it will be necessary to draft a formal RFP or RFQ document. The UW IT Vendor Risk Management services team has written specific guidance that provides slightly more detail about how to utilize the **5 Holistic Strategic Objectives** to meet the formal drafting requirements. That guidance can be found here [[LINK](https://docs.google.com/document/d/1KdNan9-7l-zH7gkgXwhv8rOfD9uSgvGrPnhk6AF_u3s/edit?usp=sharing)].

Additionally, you can contact help@uw.edu with the subject line “IT Sourcing” and request supplemental coaching and training for yourself or other personnel within your organization, or you can request drafting assistance. Within RFQs the objective of **Accountability** is expressed as **Design Maturity,** but all 5 Evaluation Criteria in the RFP guidance are substantively identical to the **5 Holistic Strategic Objectives** and the same rules of thumb described in this guide all apply.

Whether you do a formal or an informal bid competition, you will want to be able to do a side-by-side apples-to-apples comparison of the vendor offerings. Towards that end, an **RFx Bid Tab Scoring Worksheet** was created as a job aid. That spreadsheet can be downloaded here [[LINK](https://drive.google.com/file/d/1150OgS7TXkP1_T__ULvlEQJ9YZWYYdc9/view?usp=sharing)].

##

## Information Technology

UW-IT is responsible for conducting IT projects and IT acquisitions as part of its role as strategic stewards of UW’s information technology resources. The scope of this review is broader than purely system engineering or IT operational risks. Topics such as sustainability, accessibility and consideration of other individual civil rights are also in scope. As such, the substantive focus of the inquiry are the **5 Holistic Strategic Objectives**.

### Concept Briefing Document

The concept brief is a short, high-level description of the proposed IT investment project. An example of this form can be found here [[LINK](https://drive.google.com/file/d/1jQeHGqKodnBebsunsRzOcmD_k9wOi7P5/view?usp=sharing)].

The information requested in the form corresponds to your preparation as follows:

* *Describe the business problem you are trying to solve with this project.*
The **situational narrative** tends to be the answer to this question.
* *...describe any additional relevant factors that further motivate this project…*
Here is where you may want to add additional detail from the **background information.**Identify the extent to which the motivation is purely about the **organizational mission** versus other practical considerations of a particular **Program or Service**, **Duty to customer**, **legacy system**, pressure on the existing system **architecture** due to changes in an adjacent or external system, **resource constraint**, or new strategy from the **executive head** of your unit.
If there are **organization specific** **considerations**, then this is a good place to discuss them.
* *Describe how this concept aligns with your unit’s or UW’s Strategic Objectives*.
From your collected **background information**, point out the aspects of the proposed plan that improve UW’s position vis-a-vis performance **quality**, vendor **accountability**, investment **value,** practical **operability** issues, or consideration of **ethical** human values.
* *What are the biggest concerns about the project at this point in time?*
1. If this implementation project does not occur or the outcome of this effort is not adequate, what will be the adverse effects on the **mission, programs** and **duties to the customer** ?
2. What are the scariest known issues arising from the **legacy** system or the interconnection with systems upstream and downstream in the **workflow**?
3. If there a **known unknowns**, then this is a good place to discuss them.
* *Describe project outcomes and how they will be measured.*
If the IT system will support a specific **Program or Service**, then which existing metrics of that **Program or Service** will the IT investment have an effect on?
If the IT investment will modify/replace a **legacy system** or is being driven by an upstream or downstream change in the **workflow**, then what existing metrics are already in place that the IT investment have an effect on?
* *Will this project deliver customer-facing value?*
This is a question about the relationship between the **duties to customers** and the **quality** of the proposed system.
* *What discovery or market analysis will you do to inform the technical solution?*
Here is where you describe the results of engaging with Procurement Services.

### IT Project Assessment

The IT Project Assessment is a multiple-choice questionnaire; very little writing is required. However it is necessary to make a realistic guess about the *five year operations cost*, which (roughly) corresponds to the **Holistic Strategic Objective** concept of **value**, or more specifically, *total cost of ownership*.

|  |
| --- |
| **Rules of Thumb:*** **Total cost of ownership** is **never** just the cost of the license and maintenance. Limiting the calculation and disclosure to the cost of license and maintenance sometimes indicates that the organization has a limited understanding of their own total cost of ownership and would benefit from more support.
* The estimated range of cost outcomes tends to be greater (or at least lower confidence) if the investment involves something *new* in the sense of either this is a totally new capability with no previous legacy or the existing system is not a formal IT system.
* The more resources on the **team roster** who are familiar with the technologies required to implement and operate the system, the narrower (and more confident) the estimate tends to be.
* If the investment requires ***vendor resources (professional services and consultants)*** either to implement or operate the investment, the total cost of ownership tends to be higher. The **team roster** can be familiar with technologies and still need more help.
* If the investment is replacing a **legacy system**, whether in whole or in part, then the total cost of ownership tends to be both greater and more difficult to estimate in relation to both: the amount of turnover there has been on the **team roster** since the initial implementation of the **legacy system** and the number of **known unknowns**.
* If the investment is primarily driven by changes in the **workflow** either upstream or downstream of the system and some ***other organization***owns the upstream or downstream system, then both the cost containment and the confidence in the estimate are directly related to the amount of support that the **team roster**gets from the ***other organization.***
 |

#

# Other Resources

## For more information...

Sources directly used in this “How to Guide”

* UW-IT, **IT Sourcing,** https://itconnect.uw.edu/work/it-sourcing/
* UW-IT, **What Information will I need?** <https://itconnect.uw.edu/work/it-projects-and-acquisitions/what-information-will-i-need/>
* UW-IT, **Sample Concept Briefing Document,** <https://drive.google.com/file/d/1jQeHGqKodnBebsunsRzOcmD_k9wOi7P5/view>
* UW-IT, **Sample IT Project Assessment,** <https://drive.google.com/file/d/1IrvDCgeMCz5mirRSJYE1bhE_30D5PCO1/view>
* UW Policy and Rules Office, **PO No. 63 The Vice President for UW Information Technology and Chief Information Officer**, <https://www.washington.edu/admin/rules/policies/BRG/RP1.html>
* UW Policy and Rules Office, **APS 2.3 Information Technology, Telecommunications and Networking Projects and Acquisitions Policy**, <https://www.washington.edu/admin/rules/policies/APS/02.03.html>
* UW Policy and Rules Office, **APS 2.6 Information Security Controls and Operational Practices,** <https://www.washington.edu/admin/rules/policies/APS/02.03.html>
* UW Procurement Services, **How to Buy,** <https://finance.uw.edu/ps/how-to-buy>
* UW Procurement Service, **Initiating the RFx process for campus**.pdf, <https://drive.google.com/file/d/13bZzMEGrb1Pg7FvlP8t-d62TLlAESk3E/view?usp=sharing>
* WA Department of Enterprise Services,**WA-State Contract Management Manual** (Jan 2019), <https://drive.google.com/file/d/15C7TO-S4RtSZl66HGlUa_W7IwlwSJ9f-/view?usp=sharing>

For a deeper understanding:

* Boyens, J., Paulsen, C. et al, **NISTIR 8276 (Draft) Key Practices in Cyber Supply Chain Risk Management: Observations from Industry** (NIST), <https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8276-draft.pdf>
* Friedman, B., Hendry, D. G., **Value sensitive design: shaping technology with moral imagination**, <https://alliance-primo.hosted.exlibrisgroup.com/primo-explore/fulldisplay?docid=CP71330489910001451&vid=UW&search_scope=all&tab=default_tab&lang=en_US&context=L>
* ISO/TC 262 Risk Management,**ISO 31000:2018 Risk management — Guidelines** , <https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en>
* Ross, R., **Building Cyber Resilient Systems: A National and Economic Security Imperative** (NIST), <https://csrc.nist.gov/presentations/2018/building-cyber-resilient-system>s
* UW-IT Accessibility, **IT Accessibility Guidelines**, <https://www.washington.edu/accessibility/checklist/>
* UW-IT, **UW-IT Partnerships**, <https://www.washington.edu/uwit/partnerships/>
* UW-IT Office of the CISO, **Security Planning “How To” guide**, <https://ciso.uw.edu/site/files/security_plan_how_to_guide.docx>
* UW Policy and Rules Office, **BRG No. 1** **Role and Mission of the University**, <https://www.washington.edu/admin/rules/policies/BRG/RP1.html>
* UW Policy and Rules Office, **BRG No. 2 Statement of Ethical Principles**, <https://www.washington.edu/admin/rules/policies/BRG/RP2.html>
* UW Privacy Office, **Personal Data Processing Agreement and Resources**, <https://privacy.uw.edu/design/agreements/pdpa/>
* UW Procurement Services, **UW Supplier Code of Conduct,** [https://finance.uw.edu/ps/sites/default/files/Resources/charts/Code%20of%20Conduct%207-29-16.pd](https://finance.uw.edu/ps/sites/default/files/Resources/charts/Code%20of%20Conduct%207-29-16.pdf)

# Step 1

Before starting the approval process, gather materials that you already have. Here is a table to help organize what you find.

|  |  |
| --- | --- |
| **Information to gather** | **Link** |
| **Organization Mission** |  |
| **Name of program or service** |  |
| **Duties to customers** |  |
| **Description of Legacy system**  |  |
| **Workflow (Architecture)** |  |
| **Team Roster** |  |
| **Executive Head of the Major University Organization** |  |

# Step 2

Review and reflect on how you would explain your goals to as broad an audience as possible. Then, Write down your “off the cuff” answer to each of the following:

1. **Why are you motivated to buy some IT stuff?**
2. **What are your expectations for using this system?**
3. **What are your expectations regarding system maintenance?**
4. **Using nouns or adjectives, list the core values which are driving your decision.**

# Help!

If you:

* Prefer to work directly with someone in UW-IT, *or*
* Have started the worksheet but would like assistance,

Contact: help@uw.edu
Put “ IT Sourcing” in the subject line and ask for “IT Vendor Risk Management” in the message body.