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.

by IT Vendor Risk Management (rev 1, Nov 18, 2020)

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), 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:

a) How well will the system scale or perform under different conditions and workloads?
b) On an annual basis, how often will the system need to be taken down for maintenance or to resolve unplanned issues?
c) What is the expected severity and complexity of unplanned issues?
d) What is the expected lifespan of the system?
e) What is the estimated cost of implementation divided over the lifespan of the system? (Amortized implementation cost)
f) Is the sum of the annual maintenance and amortized implementation costs greater than the ongoing costs associated with the legacy system?
g) 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?
h) 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**.