**Risk and Change**

**INLS 582, Systems Analysis**

**Wednesday, 4/4/12**

**Reading:** [Lorenzi, N,. & Riley, R. (2000). Managing Change: An Overview.](http://www.ils.unc.edu/~stephani/sasp12/details/LorenziRiley2000.pdf) Journal of the American Medical Informatics Association, 7, 116-124.
[Sicotte, C. et al. (2007). A risk assessment of two interorganizational clinical information systems.](http://www.ils.unc.edu/~stephani/sasp12/details/SicotteEtAl2006.pdf) Journal of the American Medical Informatics Association, 13, 557-

**Slides:** RiskChange.pptx

**Exercise:** in groups, 2 parts. 1. What are risks to rest of project? 2. client readiness for change.

Risks

You’ve put a lot of work into your project at this point. There’s more to come, of course. You don’t want it to go to waste! A doomed project, or a failed project, is not a good thing.

Recall the various types of feasibility we talked about at the beginning of the term – these are also sources of risk. (technical, environmental, financial, management, economic, operational, motivational, schedule, etc.)

Many serious risks are out of control of project manager. This reflects an important concept in understanding risk management. What can you control (if not entirely prevent, what can you monitor, so even if you can’t control it, you know what it happening and may be able to mitigate its effects, and what is out of your control?

It's important to manage and/or monitor:

* Sources of risk
* Targets of risk
* Severity of risk

Risk is also classified by how serious its effects are. Something may be out of your control, but may not have serious consequences. Vice versa, something may be in your control, and have very serious consequences if it occurs.

Cule et al talk about kinds of risk for IS projects, and how to manage them.

First, it’s important to realize that some risk can be managed, but some risk can only be monitored. Cule et al talk about the project manager’s role in managing risk, but everyone on the team should be aware of what’s going on.

Sources of risk can be internal (to the manager, the team or the task), or external.

Internal risk is inside the project manager’s purview, outside risk is outside.

Self risk is inside, and has to do with the manager’s capabilities and characteristics. Managing these involves assessing these, and improving, learning, ameliorating when possible. Note that many of these could also be applied to team members. Also recall the article on team membership we read at the beginning of the term. Example, include problems of managing change, misunderstanding the requirements, or poor management skills.

Task risk is also inside, and has to do with how the team and project are managed. Examples include poor development methodology, lack of staff or funding. Managing these should be within the control of the manager, but may mean interceding (read “begging” for more resources, time, etc.)

Client risk is outside, and may not be directly controllable by the manager. However, the manager may be able to influence client variables, and therefore may be able to reduce risk. Examples include lack of cooperation, not getting approval from decision makers. Note that changes in the client (personnel, budget, etc.) means that the manager may need to effectively start over in managing a risk factor.

Environment risk is also outside, and concerns completely external factors. These can only be monitored, not controlled or influenced. Examples include technological developments, changes in vendors, new requirements for the system because of legislation, etc.

Of course, risk can not be completely eliminated. Note that even environmental risk must be monitored, so changes won’t be unexpected. Another important point in the article is that managing risk isn’t a one-time effort – it is an important part of the manager’s job every day.

Brown et al (2007) analysed types of problems and where in the stages of a project they occurred. Knowing this would help managers focus their attention on crucial issues at the right points in the project.

Types of problems <slide>

They define stages of implementation:

* Initiation – identifying problems and oportunities – similar to problem definition
* Adoption – commitment to doing the project, gathering resources
* Adaptation – design, development, installation, deployment. Includes modification of processes and routines.
* Acceptance – users begin to use the system
* Routinization – users use the system on a regular basis
* Infusion – organization benefites from the new system (effectiveness, cost, etc.)

What problems occur at what stages?

Results <slide>

Knowledge is important at initiation, becomes less so. <identification of good problems, issues, understanding of feasibility>

Infrastructure becomes more important during adaptation – if the system doesn't work, then people won't use it.

Commitment and communication play an important role all the way through.

<what kinds of risks do you see for your project?>

**Yen and Davis** show the “risk-payoff matrix”, where you situate your project in one of 4 quadrants.

Quadrant 2 is to be avoided

Quadrant 3 is very desirable

1 and 4 may need to be determined by other methods.

 RISK

1.

high payoff,

high risk

3.

 high payoff,

low risk

4.

low payoff

low risk

2.

low payoff,

high risk

PAYOFF

What can you do to move your project into a more desirable quadrant?

You can think about different kinds of risks at different stages in the project.

Design and development

Technical, scheduling, uncooperative clients or project staff, lack of skills, too long to complete (being beaten by a competitor), cost overruns…

Deployment

Scheduling, running behind. Unanticipated problems (e.g., discovering asbestos), technical problems, resistance on part of clients, users, …

Operation and maintenance

System failures of various kinds, infrastructure failures, disasters (natural and manmade), sabotage, obsolescence faster than planned, unexpected growth of system demands (remember the first year of online shopping, and the difficulties toys-r-us had in delivering toys ordered online?), …

Some risks can be managed. For example, monitoring technical developments can help you keep your project up to speed technically. Competitive intelligence can help you keep ahead of competitors. Working actively with clients can help avoid acceptance problems. Monitoring employ job satisfaction to minimize loss of employee (or poaching by competitor.

Some risks can be recognized but not managed. For example, you may know that there are power struggles in the client company, but not have a lot of leverage. You may know the economy is shaky, but there is likely little you can do to change or avoid it.

As we talk about communicating change, think about communication as a means of managing risk.

**Lorenzi et al. Managing Change: an overview**

Written in 2000; if anything the environment is even more complex, thus managing change is still crucial,even with employees who are supposedly comfortable with complex systems and expect change.

This is an overview of managing changes involved with adopting health information systems into clinical settings. Issues are universal however. covers conceptual frameworks for considering change.

"medical informatics has had many successes—probably more than should have been expected, given the challenges.."

But early systems were more isolated, stand-alone. often with champions.

Now, complex systems, deeply embedded in practice, interactions with other systems, processes.

Technical challenges are expected; organizational and cultural challenges are surprisngly important.

Table 1 reasons for system failures. usually many factors contribute to failure.

competing ideas: resisting change vs. seeking out novelty and change. people are a combination. perceived threat, motivation, risk of failure, all play a role.

"Organization change normally involves some threat, real or perceived, of personal loss for those involved."

increasing rate of change – difficulty in adjusting, increased pressure.

"change management is the process by which an organization gets to its future state, its vision"

 -- create a vision for change

 -- empowering individuals to act as change agents to attain that vision.

first order change – change to how thiings are done within an existing system

second order change – change to the system itself – the whole framework.

Who is affected by change? who must make effort to learn or re-learn? who perceives loss of skill, expertise, authority, control, impact? who percieves gain? who percieves lack of support (time, training, reward) for making the effort to change?

Types of change:

operational change – how operations are done

strategic changes – direction/emphasis of business

cultural changes – business philosophy or approach

ppolitical changes – impact of leadership changes

**Sicotte et al (2006). A Risk Assessment of two interorganizational clinical information systems.**

This study compares implementation of 2 systems in 2 settings; 1 was considered a success, 1 a failure.

Figure 1 is the one to discuss (see slides). Both systems started with same risk profile, but the risk management strategies differed, and they ended up with quite different profiles.

Starts by discussing type of risk in system implementation.: technological, human, usability, managerial, strategic and political. These are drawn from literature review.

Rainbow Network. Regional EMR data warehouse, 7 organizations. users = 39 pediatricians, project took 40 months. outcome: technical success, but failure in adoption/use, and it came in very late. Considered a failure.

Primary Care network. also regional EMR data warehouse. 12 organizations, 105 general practitioners. 26 months. outcome: technical and adoption/use success, moderate success in schedule. Considered a success.

in both, EMR was reports of lab tests and radiology, with CPOE expected in subsequent phase.

Data collection for study:

* semi-structured interviews with users and project team members.
* structured questionnairs to measure users' attitudes toward new system. (before and after)
* system usage measured with logs.
* observation during steering committee/user committee meetings
* artifact analysis.

case and cross-case analysis and comparison.

risk analysis on 5 dimensions of risk, 5 point scale from very low to very high at 2 critical moments: project onset (initial risk level) and end of implementation (final risk level) Figure 1.

technical success: systems were operational and usable. this was recognized as risk; lots of effort was invested to minimize it. outside experts, testing, etc.

adoption/use, Rainbow failed to meet expectations. very few adopters. 13/22 physicians occasionally used the new system on a weekly basis. in clinics, medical secretaries used the system to print the data that was then filed in papery.

Primary Care 69% physicians used it intensively.

human risk. Rainbow dedicated little effort to this. PCN had physician project champion in each clinic. they felt they had good understanding of system.

usability risk. Rainbow, implementtation delays. no support for new users, it was easier to keep using the old system. PCN did usability testing, intensive monitoring during deployments, responsiveness to problems.

and so on.

risk is multi-dimensional. Some can be limited proactively, other types of risk require fast and effective response. can analyse risk potential in the beginning of a project, and determine where to put resources, but must also monitor throughout to respond.

# Change and communicating change

In addition to actually building your system, you have to think about deployment. Even though you aren’t necessarily going to do that yourself (for your projects), you still need to think about how you will do this. In fact, this is something you should be thinking about all along, because this can make or break the success of your system. Revamping, updating, re-engineering, introducing a new system – this is all about change, and people react to change in a variety of ways. Your goal is to make it easy, interesting, exciting, rather than threatening and a nuisance. You want to make change an opportunity, not a threat.

Ch. 10 talks about ways of communicating with your organization and clients. You want to build some interest, support for what you’re building. Think about who needs to know what you’re doing outside of your immediate clients and management contacts.

“The communication that a project creates must be designed to inform each external group what the project is doing, to provide details that allow the group to understand the project’s design direction, and to provide meaningful ways for the group to comment and contribute ideas with knowledge of the customer data.” (p. 200)

What are your goals for communication?

With whom, why, when, and how should you communicate with them?

or

What do you need to communicate, and to whom?

To whom do you need to communicate, and what?

How can you get people to interact with your system ideas, or the system itself? Don’t just think in terms of meetings or talks – demos, manipulation, models, prototypes, asking for feedback are all ways of getting people involved.

B&H suggest letting others walk the affinity and consolidated models, tour your design room.

Come up with compelling scenarios, or inspirational prototypes.

What are the milestones you want to communicate?

# [Regan & O’Connor, 1994, Organizational Change

They talk about the well known model of adopting innovation (Rogers – are people familiar with this? They should be.) <champions; opinion leaders; early adopters, innovators>

This and the Markus and Benjamin article both talk about IS people (designers, managers, etc.) as agents of change – people who can actively foster change. This is an important thing to think about, given that much of what you do is involved with changing how people do things.

<who are change agents in LIS world, locally or anywhere in the profession?>

R&O encourage planning for change, as opposed to responding to unexpected change. In introducing a new IS system, or way of doing/organizing work, you’d like to be able to do the former, but you may sometimes be forced into the latter, for example if your company is bought out, if a direction for change comes down from upper management, or if a disaster of some kind occurs.

They list several considerations that can affect the success of change. Recall our discussion of avoiding, managing, or monitoring risk – change is a risk, so you want to manage it to the greatest extent. In our business, it’s probably impossible to avoid it.

(p. 395-397)

* ability of employees to conceptualize change – can people really envision it? Envision the end product?
* Employee’s readiness for change (intellectually and emotionally)
* Employees capacity for change – how do people handle uncertainty?
* Individual differences – learning style, uncertainty, frustration tolerance, etc.
* Environmental uncertainty and complexity – may help foster acceptance of change. If things are good, why change?
* Change itself – how much are you changing? How fast? What is the scope of the change? (recall scope of problem definition)
* Organizational structure – how conducive is it to change? Organizational culture will also play a role
* Distribution of power. Will the propose change upset the status quo? Would that be good?
* Experience of change agent – is agent good at it? Willing to work at it?
* Risks involved – to individuals, organization, etc.
* Required resources – money, people, space. How are limitations going to affect the plans?

]

**Exercise.** Regan & O’Conner mention Lewin’s Three Phases of Change model, and how that can be used to help plan and foster acceptance of change.

1. Unfreeze phase – creating readiness for learning, foster awareness of need for change, talk about options. Your information gathering work is one place where this can happen, as well as in more deliberate campaigns.

2. change phase – learning occurs, attitudes change, people learn new work habits, skills, see demonstration, start adopting the new system

3. refreeze phase – new behaviors become habits, system is integrated and becomes “normal work style”. Modifications can still occur, but the big change is over.

On the other hand, some organizations prefer a model of continuous change, where small changes are constantly occuring, rather than periodic big changes.

In your project groups: Which model best fits your client?

If phased:

What stage were your clients at the beginning of the project?

Where are they now?

What can you do to move them through the phases? What do you need to do to help acceptance of the proposal?

If continuous:

How can/should you break up your proposal to fit continuous change?

Is there a reason you should advocate for a single big change intead?

Consider: client organization, client individuals, client customers, others who will be affected

Remember that you need to think about both “we need a change” (undirected dissatisfaction with current system) and “here is the change we propose” (readiness for specific solution).

# [Markus & Benjamin, 1996, Change Agentry – the Next IS Frontier

After the rather passive analysis of R&O, M&B have a much more active set of recommendations for the role of IS developers and systems folk in change. They see two important issues in being a change agent – determining what the change agent actually does (the role he/she plays) and how the structural conditions of the organization will interact with that. The relationship and conditions will help determine how the agent can intervene to help foster change, and therefore the acceptance of the system.

What are the forces for change?

What do people perceive as the forces for change?

What are the role and actions of the change agent?

<ask project groups to discuss these>

p. 388 has a very nice matrix on it – could put up the top row, and have people see how they’d like to work, where their projects lie, etc.

Think about these two statements <email to class beforehand, to think about>

People cause change

Technology causes change

What are the implications of these beliefs? Are they in opposition?

The other issue they mention is the need for IS people to build their credibility with other members of the organization or client. The better your credibility, the better you’ll be able to work as an agent. ]