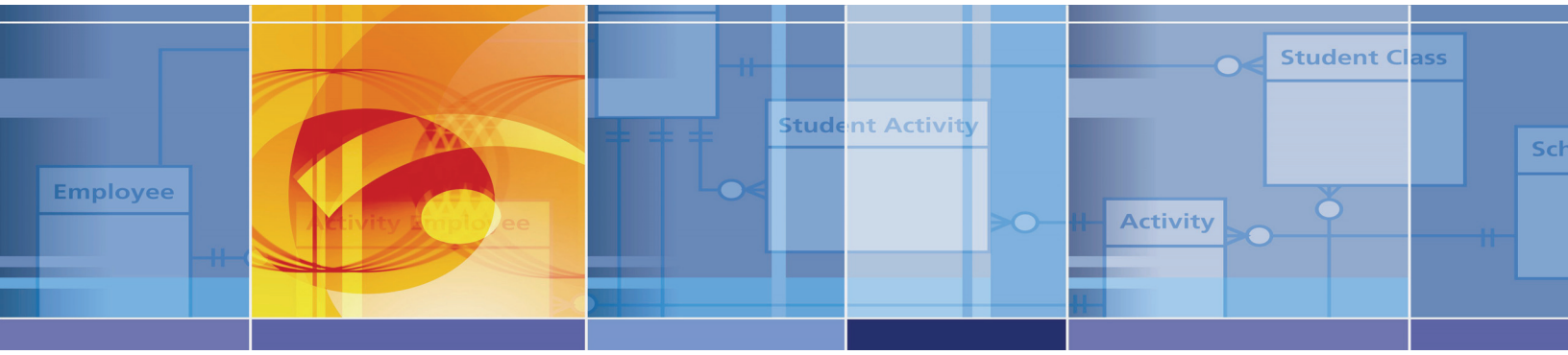



*The Optimal Reference Guide:*

# From RISk to Reward: A Guide to Risk Management for Education Agencies

## Project Management Series – Part II

*Extraordinary insight*™ into today's education information topics

By Glynn D. Ligon, Ph.D, ESP Solutions Group

ESP Solutions Group

# Table of Contents

## About ESP Solutions Group

ESP Solutions Group provides its clients with *Extraordinary Insight*™ into PK-12 education data systems and psychometrics. Our team is comprised of industry experts who pioneered the concept of "data-driven decision making" and now help optimize the management of our clients' state and local education agencies.

ESP personnel have advised school districts, all 52 state education agencies, and the U.S. Department of Education on the practice of K-12 school data management. We are regarded as leading experts in understanding the data and technology implications of the **No Child Left Behind Act (NCLB)**, **ED*Facts***, and the **Schools Interoperability Framework (SIF).**

Since 1993, we have provided education consulting services for large-scale implementation projects. We also develop products and services that help put quality data into the hands of decision makers. We have authored over 30 Optimal Reference Guides on topics relevant to education technology such as data quality and reporting, confidentiality, assessment, accountability, project management, growth models, etc.

To learn how ESP can give your agency *Extraordinary Insight* into your PK-12 education data, email info@espsg.com.

## About the Author

**Glynn D. Ligon, Ph.D.**
**President and CEO**
Dr. Ligon, the president and chief executive officer of ESP Solutions Group, is a nationally recognized expert on issues relating to student record collection and exchange, data quality, data reporting, and large-scale system design.

The National Center for Education Statistics, the U. S. Department of Education and over 25 state education agencies have consulted with Dr. Ligon on various areas of his expertise. He has a Ph.D. in Educational Psychology, Quantitative Methods from The University of Texas at Austin and is licensed to teach in the State of Texas.

Prior to starting ESP in 1993, Dr. Ligon directed the Austin (TX) Independent School District's information and technology organization. As the executive director of management information, he led the district's efforts in developing and reporting on district-wide program evaluations, many of which won national awards from the American Educational Research Association. Dr. Ligon was also a leader in the advent of SPEEDE/ExPRESS, the EDI standard for the exchange of electronic student transcripts.

From 1992 to 2000, he served as a member of the U.S. Department of Education's Planning and Evaluation Services Review Panel. Dr. Ligon's whitepapers; *A Technology Framework for NCLB Success* and *Steps for Ensuring Data Quality* are prominently featured within the U.S. Department of Education's 2005 National

Education Technology Plan, meant to help motivate and incite technology-driven transformation in education.

At the beginning of his career, Dr. Ligon taught in predominantly Spanish-speaking schools near the Texas-Mexico border. He is an experienced evaluator of Title I, Migrant, compensatory education, and bilingual education programs.

# Introduction

*Instead of a forward…a fable.*

## The Risk-Reward Rabbit Tale

Four rabbit families desperately wanted to get to the farmer's new garden to feed their babies. The rabbits were deathly afraid of the foxes in the open fields between them and the garden. They argued loudly about the risks and whined about the rewards they were missing.

The first rabbit family turned around and went back—the veggies in the old garden were small and sparse, but they were available and certainly avoided the risk of the open field.

The second rabbit family sat at the edge of the field and worried—maybe something will change, maybe there's another way, why aren't other rabbits more worried about the foxes?

The third rabbit family was the bravest—no one had ever actually seen a fox out there, what are the chances of getting caught? Rushing on ahead, those rabbits were chased by several foxes of all sizes until, exhausted, the rabbits gave up and scurried back home—the lucky ones.

The two scouts of the fourth rabbit family talked about the risks and even thought there may be others unknown to any rabbit. They spent some time asking the other rabbits about the foxes—when they slept, where they spent the hot afternoon, what they looked for, where the safe places were. They even talked to the third rabbit family to find out what made them turn back. One wanted to hide the risks from the others, but the second thought otherwise. Together they told all the rabbits everything they knew about the risks. The scouts didn't try to merely reassure the others. Armed with all this knowledge, they proclaimed the risks to the entire family. However, the scouts had a plan to run the gauntlet at the perfect time prepared to take cover when a fox spotted them.

Together, the rabbits followed the plan. In the end, the fourth rabbit family earned the rewards of the new garden and raised the healthiest and happiest babies.

**Moral of the Story: The rewards go to those who proclaim the risks <u>and</u> have a plan to confront them.**

This Optimal Reference Guide (ORG) delivers a simple encouragement: Get beyond the fear of risks and find the rewards promised by IS projects.

Getting there calls for an unexpected strategy: Emphasize the risks to win over the fearful. You be the one proclaiming the risks. Scared rabbits are difficult to merely reassure. A concrete plan demonstrates that you are taking risks seriously.

That plan should follow five concrete steps that come directly from the experiences of education agencies—not straight from economics.

In the end, students will benefit from educators' actions to leverage technology in support of quality education.

"There is no security on this earth. Only opportunity."
-**DOUGLAS MACARTHUR**

# Risk in Your IS Projects

Risk lurks around all information systems (IS) projects.

- Fear of risk can stall progress.
- Blindness to risk can result in failure.
- Management of risk can ensure success.

*(Education agencies use both IS, Information Systems, and IT, Information Technology in their lexicon. At times the distinction carefully defines the focus of the information office. At times, as in this paper, IT and IS are interchangeable. This paper uses IS merely to match the style of the word R**IS**K in the title. R**IT**K didn't work.)*

## What do decision makers (e.g., policy makers, finance managers, elected officials) fear the most?

- Risks have been underestimated and will prevent success.
- The project management staff is unprepared to deal with the risks that may occur.
- They, as decision makers, are more concerned about risks than the staff members who are encouraging them to commit to a project.

Decision makers must accept a reasonable amount of risk in order to make a decision. Decision makers must reach a comfort level with risk that allows them to move on and make the best decision possible. For an IS project, risk paralysis can cause damaging delays or even kill a project.

There is a straightforward strategy to move decision makers ahead—beyond their fear of risks.

**Proclaim the Risks (Be the first and foremost to herald the risks)**

- Acknowledge that risks are real and demonstrate that they will be taken seriously
- Identify all possible risks up front
- Analyze and prioritize risks using a "risk index"

**Confront the Risks (Impress decision makers with the priority that risk mitigation receives throughout the project)**

- Mitigate priority risks with a specific plan
- Monitor and report on risks consistently

By the way, this is not all about helping decision makers be comfortable with risk. This is all about raising the probability that an IS project will deliver the rewards promised and expected.

This Optimal Reference Guide (ORG) takes each of these steps and describes how ESP's professionals analyze, plan, monitor, and report risks in our IS projects. This

"There came a time when the risk to remain tight in the bud was more painful than the risk it took to blossom."
-**ANAIS NIN**

paper launches our use of significantly upgraded tools and methods for risk management.

The business management literature is full of advice for risk mitigation. Our ESP project management experts find too little of that wisdom being translated into action within education agencies. Today, with so many major information projects being contracted to outside companies, an education agency must exercise direct control of risk management. The internal education agency project staff must be aware of risks and require the contractor to work with agency staff to monitor and mitigate those risks. This is definitely not a task to delegate to the contractor.

This paper shines the light on risks in an education agency's information systems projects. Here we define risk, alert education agencies to potential risks, and detail ESP's methodology for working with an education agency to manage risk in our large-scale IS projects. We have created a comprehensive taxonomy of the risks education agencies face when implementing a major IS project. Individual education agencies no longer need to start from scratch to foresee potential risks. The best practices described here alert education agencies to potential risks and provide a mitigation planning methodology to deal with them.

ESP's experts continually emphasize that education agencies need a customized style of project management for success. See ESP's Optimal Reference Guide, ***Why 70% of Government IT Projects Fail—Quality Project Management for Education Agencies***. Risk management is a significant component of our overall project management methodology.

## Differentiating Project Risk from Security

The rabbits had to actually get to the new garden before security risks became an issue. Getting there is project risk, staying there is security risk.

Most of the references found using the keyword "risk" relate to security risks or disaster prevention and recovery activities. The IS literature is paranoid about security risks, almost to the point of giving too little attention to our topic in this ORG—project risk. Project risk is related specifically to impact on successful implementation of an IS project or failure to deliver anticipated benefits from the IS project. Attachment A provides an overview of security risks and some key references on that topic.

An education agency must pass through the gauntlet of project risks before even getting to the point of managing security risks. Disaster prevention and recovery, on the other hand, begin to impose their risks during the project implementation phases. See ESP's Optimal Reference Guide, ***Disaster Prevention and Recovery for School System Technology.***

# Proclaim the Risks

## STEP 1: Acknowledge that risks are real and demonstrate that they will be taken seriously

The best way to ensure that decision makers believe that the project implementation staff understands the importance of risks is to show them a well-crafted risk mitigation plan. This ORG should be a part of that plan to establish both a theoretical and a best practices basis for the approach adopted.

Does the "plan" need to be a formal document, a slide show, or a description of how risk mitigation is closely integrated within the overall project management plan? That would be determined by the personality and standards of the individual education agency. Assuming a formal plan is the choice, here are the components. Notice they follow the five steps in the overall strategy recommended in this ORG.

Part 1: Statement of the importance of risk mitigation
Part 2: Identification of all potential risks
Part 3: Analysis and prioritization of risks
Part 4: Risk mitigation actions
Part 5: Risk monitoring and reporting plan

The risk mitigation plan should be incorporated into the project statement of work, work breakdown structure, and project management plan.

In presentations to decision makers, take care that risk mitigation does not get relegated to the end or merely handed out as an attachment. Flaunt how much attention is being paid to avoiding risks that might endanger the success of their project.

**An Education Agency's Nightmare Risks**

Decision makers think of risk from a different perspective than do the IS professionals. Being public and having the trust of the public places extreme pressure on education agencies to avoid risks. What are the risks that an education agency's leadership most definitely wants to avoid? Figure 1 describes these public risks.

"One doesn't discover new lands without consenting to lose sight of the shore for a very long time."
-**ANDRE GIDE**

| Risk from the Education Agency Leadership Perspective | Examples *(These "risks" will later be renamed as consequences, i.e., the damage that an occurrence inflicts upon the project's implementation or benefits, or the education agency as a whole.)* |
|---|---|
| 1. Mismanagement | a. missed opportunity for benefits; being exposed as out of date; being inefficient<br>b. waste of money; expenditure without benefits<br>c. going over budget and impacting other activities<br>d. failure to deliver on time, on budget, or on target for functions or benefits<br>e. loss of productivity by staff during implementation, as a consequence of the change, or as a consequence of a disaster/interruption of services<br>f. failure to deliver quality education services<br>g. disaster that interrupts services without an adequate prevention and recovery plan in place |
| 2. Failure of Fiduciary Responsibilities | a. release of incorrect information<br>b. distribution of incorrect dollars<br>c. failure to meet legal deadlines for publishing accountability data and ratings<br>d. failure to balance financial accounts<br>e. exposure of confidential information<br>f. awarding or denial of diplomas or other credentials incorrectly |
| 3. Legal Violations | a. criminal/corruption offense of fraud or theft; corruption, undue influence, conflict of interest<br>b. procedural violation of law, policy, or regulation |
| 4. Consequences and Sanctions from Other Risks | a. harm to students, negative impact on learning<br>b. legal action (civil and criminal)<br>c. protest by public groups or individuals<br>d. news media expose or negative reporting<br>e. loss of certification, accreditation<br>f. loss of employment<br>g. loss of office by elected or appointed officials<br>h. reduction of bond rating and credit |

**Figure 1: An Education Leadership Perspective on Risk**

In an environment led by elected or appointed political figures, an education agency naturally becomes over-cautious about these risks. An education agency independently, by oversight from another state agency, or by legislation deals with these risks like an umbrella policy. These risks are often not cited in an IS project's statement of work, but are assumed.

For an IS project, these risks are equally real and must be acknowledged. As we'll identify later, an IS project attracts its own list of risks beyond these.

## STEP 2: Identify all possible risks up front

The process for identifying and rating risks varies by project. However, the general steps are:

1. Draft a list of potential risks identified from similar projects.
2. Interview key stakeholders for their concerns and ideas.
3. Interview key IS professionals who support those stakeholders.
4. Lead discussions with stakeholders, IS, and advisory groups.
5. Review all identified risks with the education agency staff.
6. Draft the Risk Assessment Profiles.
7. Conduct reviews of the Risk Assessment Profiles with stakeholders and individuals.
8. Incorporate the Risk Analysis Summary into the project management plan.

Not all risks are tracked using the risk assessment process. The vetting process described above prioritizes risks and determines which are either significant enough or important enough to a stakeholder to track formally.

**Risk Factors**

The best way to illustrate risk factors is to examine a taxonomy of them. Figure 2 is a high-level view of the taxonomy ESP designed to clearly differentiate the risk factors that arise from an education agency itself and those that arise from the implementation of a specific information systems project.

Outside the context of this paper's focus on risks, these factors could just as easily be characterized as success factors. For those factors stated as positives, think of the risk as being failure to realize the positive effect.

"Security is mostly a superstition. It does not exist in nature, nor do the children of men as a whole experience it. Avoiding danger is no safer in the long run than outright exposure. Life is either a daring adventure or nothing." **-HELEN KELLER**


**Figure 2: High Level View of Taxonomy of Risk Factors**

Capacity Factors are those risks that share a common basis in the resources, expertise, and leadership of an education agency. Four categories are displayed.

1. Functions and Benefits: These are the bases for justifying the project and the functionality that will deliver the benefits.
2. Expertise to Design and Operate: These are the knowledge resources that must exist to ensure the integrity of the solution.
3. Financial Capacity: These are the financial resources required to fund the project though full implementation.
4. Mandate to Use the System: These are the requirements that ensure participation in the project.

Delivery Factors are those risks that arise during the implementation of a project. Three categories are displayed.

1. Buy-In by Participants: These are the factors that ensure users participate with confidence.
2. Functioning of All Components: These are the traditional risk factors that garner most of the attention. These factors ensure that all components of the solution are interoperable and deliver on their functionality.
3. Project Management: These are the factors that ensure the project is implemented as planned and delivered as promised.

Figure 3 is an enhanced view of the taxonomy showing individual risks within each category. This illustration is not yet comprehensive, but it's getting there.

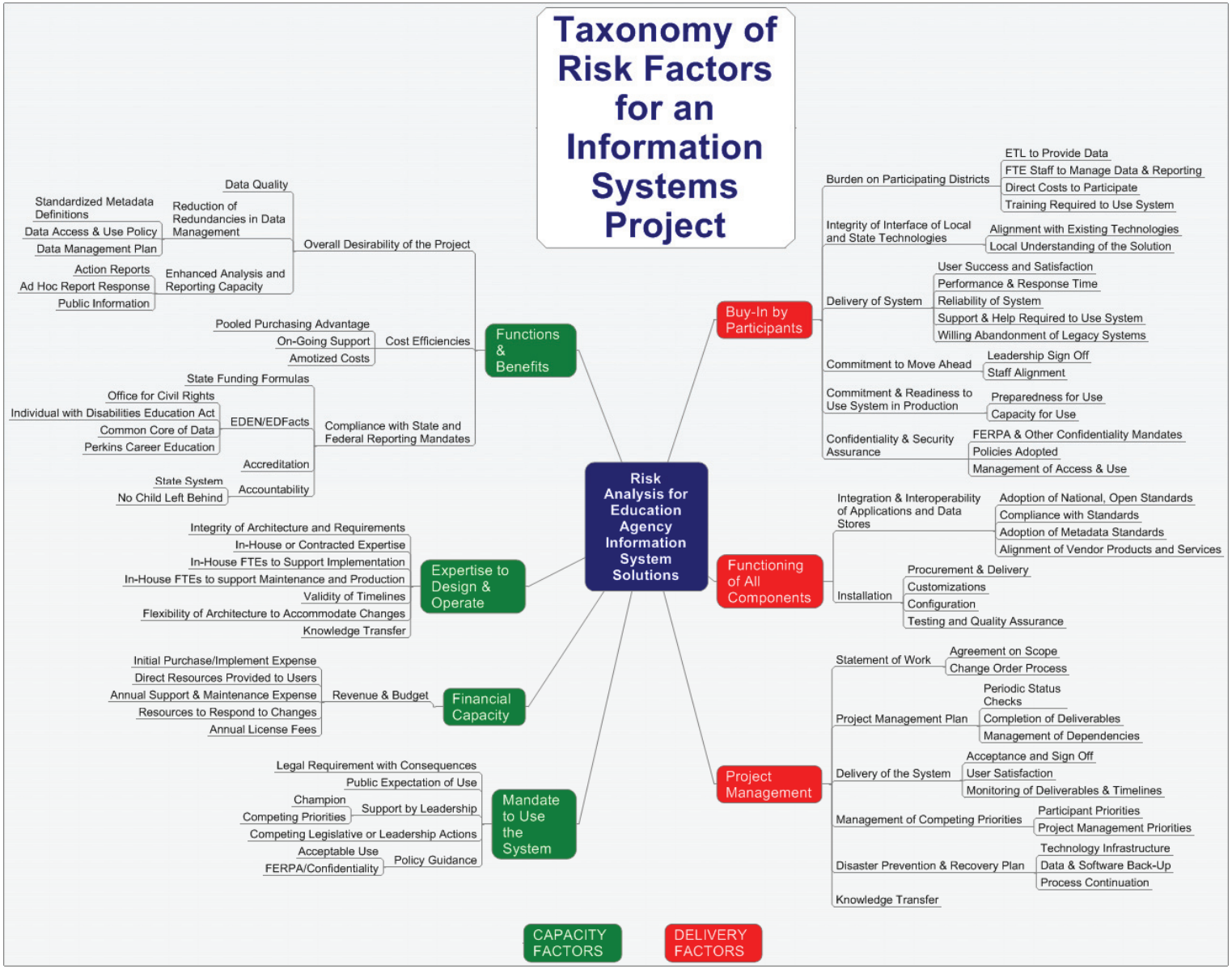



**Figure 3: Detailed Taxonomy of Risk Factors**

**Knowledge Transfer—Day 366**
One factor is found on both sides of the taxonomy—knowledge transfer. This risk factor consistently rises to the top of reasons IS projects fail in the long run. The knowledge of the IS solution's creator and builder must be transferred to those who will run it and those who will use it. The technical documentation is often a transfer of knowledge between a contractor and internal education agency staff. The user documentation must typically be transferred to a wider range of people. In both cases, the tacit knowledge—how the system really works and how to get the most benefit from it—must be transferred in more personal ways. Knowledge transfer is too major of an issue to address sufficiently here. This paper can merely emphasize its importance.

In our client engagements, ESP project managers visualize knowledge transfer as "Day 366." Assuming a one-year implementation, how is the education agency going to be independent to continue managing and using its own system the day after the contractor walks out the door?

**Disaster Prevention and Recovery—Business Continuation**
As soon as an IS project begins implementation, the risk of a disaster from natural or human causes exists. A previous Optimal Resource Guide details the methodology that ESP has developed specifically for education agencies. (***Disaster Prevention and Recovery for School System Technology***, ESP Optimal Reference Guide, 2005. Available for download at www.espsg.com/resources.php.)

The probability of a disaster may be thought of as low; however, the potential impact is too great to ignore. In the implementation phases of a project, disaster recovery processes are often discounted because the full project is not yet functional—and on-going transactions are not yet dependent upon the new system. However, the impact of a disaster in terms of delays and costs can result in substantial impact on operations.

**Rating the Risk Factors**
For a specific project, the Risk Assessment Profile (see Step 3) would be used to generate the appropriate value, then those values would be averaged (with weights assigned if desirable) across all categories to arrive at an overall risk level for the project.

## STEP 3: Analyze and prioritize risks using a "risk index"
Before analyzing and prioritizing, we need to step back and define what a risk is. This gets a bit complicated because so much has been written in the business literature, but still we find the need to add to these definitions to really characterize how risks must be managed in an education agency.

**Defining Risk**

When asked, "What is the risk?" IS professionals might answer in three ways.

1. 50%
2. Cost over-runs
3. Losing support of policy makers

Risk has the same three connotations in everyday conversations. One is the probability of something happening (50%), another is the occurrence itself (cost over-runs), and the third is the consequence of the occurrence happening (losing support of policy makers). So the complete answer is that the risk is a 50% probability that there will be cost over-runs resulting in the loss of support by policy makers.

Figure 4 lays out the terms and the relationships used throughout this paper. *Reading the definitions will help you understand the text of this paper. Not all terms are defined in the text.*

"The important thing is this: To be able at any moment to sacrifice what we are for what we could become."
**-CHARLES DUBOIS**

R**IS**K is the **Probability** of a negative **Occurrence (Trigger)** having a negative **Consequence** that **Impacts** the **Implementation** and **Benefits** of an IS project.
*(For this definition, we have blended traditional economics with ESP's Quality Project Management methodology that always focuses on delivering the intended benefits rather that on merely implementing the IS solution.)*

R**IS**K = **Impact X Probability**
*(This is the traditional definition found in the economics literature.)*

**OR**

R**IS**K **= (Impact X Probability) – Risk Mitigation – Risk Tolerance**

**Risk Mitigation** = Effectiveness of efforts to avoid or reduce consequences.

**Risk Mitigation Strategies** = What the education agency does to avoid, reduce, or respond to the occurrence

**Probability** = Percent chance of an occurrence happening

**Uncertainty** = Unknown probability of an occurrence happening

**Occurrence** = Trigger
*(Occurrence is the event that triggers the consequence.)*

**Consequence** = Damage
*(Consequence is measured by the damage from the event on implementation and benefits.)*

**Implementation** = Timeliness + Cost + Quality
*(Replacing the traditional "You can have only two of these three" perspective with "These three dynamically influence each other," the influence of an occurrence is measured for each one and in relationship to the other two.)*

**Benefits** = Expected Rewards (Improvement or Reduction in Pain)
*(The consequence of an occurrence on implementation must be translated to its ultimate influence on the delivery of expected benefits from the IS project.)*

**Risk Tolerance of the Agency** = The degree to which risk is accepted (high tolerance) or feared (low tolerance) when decisions are made.

**Figure 4: Terms and Relationships**

In economic circles, the term impact encompasses both the occurrence and the consequence. For education agencies, separating the two is useful to emphasize that a negative occurrence must be evaluated within the context of its consequence. The occurrence must also be characterized accurately by the degree or extent that the occurrence happens. For example, if the negative occurrence is late delivery of hardware, the degree of the occurrence is related to how late the delivery is and how much of the hardware is late.

Neither the probability nor the occurrence itself is of much significance if the consequence is slight. The essential question that we need to ask ourselves when considering a risk is, "So what?" If the "what" is important, then the risk is important, regardless of the probability or the extent of the occurrence itself. In IS project management, we must prioritize to avoid or mitigate risks that have a significant negative consequence.

We can't avoid any and all risks, but we must focus on those that would have consequential impact rather than those that could be handled with acceptable harm. Defining acceptable harm falls to the education agency itself.

Acceptable harm might be:

- A month's delay
- A 10% cost over-run
- Loss of one key person
- Using an underperforming application

Unacceptable harm might be:

- Inability to ever use the application
- A cost over-run greater than the capacity of the organization to cover
- Loss of a person with the key vision or institutional knowledge for success
- An application that is less desirable than what was replaced

The following is a composite scenario from our actual client engagements.

> *The risk is 90% that not all schools will be converted to the new system by the target date, resulting in continued maintenance of the old system. The negative occurrence is very likely to happen. However, because the old system was scheduled to run in parallel as a back-up for another year, the impact is minimal.*
>
> *If all schools are not converted within the next year, however, the impact becomes significant. Therefore the risk skyrockets. If the old system cannot be shut down, then license fees, staff support positions, and other costs will occur. In addition, the benefits of more timely and quality data will be delayed.*

"Cautious, careful people, always casting about to preserve their reputation and social standing, never can bring about a reform. Those who are really in earnest must be willing to be anything or nothing in the world's estimation, and publicly and privately, in season and out, avow their sympathy with despised and persecuted ideas and their advocates, and bear the consequences." -**SUSAN B. ANTHONY**

Impact can be rated for the ultimate benefits to be realized or for the influence on the implementation of the project itself. Realistically, a project should be abandoned if the benefits no longer justify it; however, project risk analyses often look merely at the impact on implementation—getting the project completed irrespective of the level of benefits to be derived upon completion.

**Remember the Rewards—Benefits?**

There is a danger that the intended benefits or rewards from an IS project will be forgotten in the intense focus on implementation. In our model for managing risk, the realization and delivery of expected benefits are highlighted independently from the success of the implementation. There have been IS projects that are considered by some to be successfully implemented without the intended benefits accruing to the users. An example from multiple states and school districts is the launching of an on-line decision support system with access to reports produced from a new data warehouse. Success! Well, not completely. The real reward was intended to be improved data-driven decision making. However, the training required and the complexity of navigating the reporting interface resulted in such low use that the impact on decisions was minimal. The implementation was successful, but the benefits were not delivered.

The following scale rates the level of benefits delivered by an IS project. Are these equal intervals? The statisticians can argue this one. Consider this now as a way to describe the levels of benefits.

Benefits Scale:

| | | |
|---|---|---|
| **10** | = | Benefits far exceed expectations. |
| **9** | = | Benefits exceed expectations. |
| **8** | = | Benefits meet expectations. |
| **7** | = | Benefits are enough to consider the project a success. |
| **6** | = | Benefits are enough to consider the project as functional, but not a full success. |
| **5** | = | Benefits are reduced to the point that the costs to implement and change equal the benefits realized, and the project may not have been undertaken if this had been known. |
| **4** | = | Benefits are reduced to the point that the costs to implement and change are greater than the benefits realized, and the project would not have been undertaken unless significant changes had been made in the plan. |
| **3** | = | Benefits are reduced to the point that the costs to implement and change somewhat exceed the benefits realized, and the project may not have been undertaken if this had been known. |
| **2** | = | Benefits are reduced to the point that the costs to implement and change significantly exceed the benefits realized, and the project would not have been undertaken if this had been known. |
| **1** | = | Benefits expected could not justify the cost or effort to implement the project, so the project is abandoned. |

Because this ORG's perspective is risk, this scale must be reversed into one that reflects the expected loss of benefits resulting from a negative occurrence. These scale points will be useful when considering the Risk Assessment Profile methodology described later.

Benefits Risk Scale:

| | | |
|---|---|---|
| **0-10** | = | Benefits will still far exceed expectations. |
| **11-20** | = | Benefits will still exceed expectations. |
| **21-30** | = | Benefits will still meet expectations. |
| **31-40** | = | Benefits will still be enough to consider the project a success. |
| **41-50** | = | Benefits will still be enough to consider the project as functional, but not a full success. |
| **51-60** | = | Benefits will be reduced to the point that the costs to implement and change will equal the benefits realized, and the project may not have been undertaken if this had been known. |
| **61-70** | = | Benefits will be reduced to the point that the costs to implement and change will be somewhat greater than the benefits realized, and the project would not have been undertaken unless changes had been made in the plan. |
| **71-80** | = | Benefits will be reduced to the point that the costs to implement and change will be greater than the benefits realized, and the project would not have been undertaken unless significant changes had been made in the plan. |
| **81-90** | = | Benefits will be reduced to the point that the costs to implement and change will significantly exceed the benefits realized, and the project would not have been undertaken if this had been known. |
| **90-100** | = | Benefits expected will not justify the cost or effort to implement the project, so the project should be abandoned. |

**Risk vs. Reward**

The greatest risk is that we'll get to the end, and the new system will be disappointing—it does not inform any actions. This perspective assumes a different attitude. No longer is it acceptable to merely make work more efficient. A new IS application must be justified by how much it improves the educational experience of students, and how much it contributes to the overall mission of the organization.

For example, certainly a conversion to electronic records/transcript exchange brings with it significant benefits in efficiency—and calculable cost savings. However, the real benefit is the reduction in the cycle time for records exchange. Instead of mobile students spending days or weeks in a new school before their official records join them, their new school staff can make informed decisions immediately about course enrollments, special programs—even acceptance of currently suspended students.

Maybe it's a bit of a stretch to propose reserving the term "reward" for these

mission-critical benefits.

Imagine the IS professional who knows, believes without any doubt, that a new IS project will benefit everyone; however, no one else thinks the rewards outweigh the risks. How can there be such a difference of opinion? Figure 5 shows the rewards as they may be envisioned by IS—and the perspective on each by others. Up front, let me say, this is rather negative, not all stakeholders in IS projects think this way. However, the reality is that all of these comments come straight from actual experiences with clients.

| Reward—as seen by IS | Reward—as seen by others | Perceived Risk—as seen by others | IS Response |
|---|---|---|---|
| Money will be saved. | Someone else gets any dollar savings. There's really nothing in this for my budget. | My budget will get hit by unfunded requirements and the other changes imposed. | Identify unfunded mandates as a risk factor and include a mitigation strategy in the project management plan. |
| Increased information will better inform decisions. | Abstract concepts don't help make my job any easier. | Increased information will merely add to the amount of reports we must manage. | Include decision makers in the design of action reports that they will use. |
| Work will be done more efficiently. | If my work diminishes, something else will be added to keep me overworked; or worse, my job will be cut. | I will probably need to keep the old system going to ensure nothing gets lost. | Ensure the legacy system disappears. Include concerned staff in training and support sessions to identify how they will avoid this risk. |
| Students will benefit and achievement will improve. | That's very theoretical—no research basis—and the impact would be a drop in the bucket compared to other needs the money could go to meet. | All this effort will not result in any change in student achievement. | Create a clear and widely distributed benefits statement. Obtain the involvement of leadership in "marketing" the new application. |

**Figure 5: Perspectives on Risk**

This comparison seems overly negative, but it represents what I have seen across multiple education agencies. "My risk, your reward." The perspectives in the "others" columns create an inertia that challenges the establishment of buy in for IS projects. Whereas educators can get enthused by the latest instructional innovation, technology innovations can be scary. Educators are convinced by the endorsements and positive experiences of other educators. IS projects should use this strategy as well. Information technology at times appears to be held to a higher standard. This is probably only a perception, not a reality. However, the fact

is that IS projects have an obligation to justify their risks with promised rewards. Proclaim the risks rather than allowing the naysayers to capture the spotlight. First, however, have a plan.

**Risk vs. Caution**

Another distinction in both the economics and psychology literature is between "risky shift" and "cautious shift."

> Risky Shift: The tendency for people in group situations to take more risks than they might as individuals.
>
> > Education Agency Example: Adopting Schools Interoperability Framework (SIF) as an interoperability standard is accompanied by risks. Adopting SIF becomes easier as neighboring districts or states make the commitment.
>
> Cautious Shift: The tendency for people or agencies to be overly cautious because any risky decision or stance can open them up to criticism by opponents.
>
> > Education Agency Example: Education agencies seek stakeholder input before publishing final requirements for most projects. They may delay the publishing of standards for a new data collection to allow time for public comment or review by oversight groups. These delays may at times look like a way to avoid making an unpopular decision among competing alternatives advocated by different groups.

These shifts determine whether or not the people within an education agency tend to be risk averse or risk tolerant. Within IS, there may be considerable tolerance for risk while in the policy offices on the upper floors, there may be resistance to an aggressive implementation schedule for fear some unknown issue will arise.

So risk factors can be rated along a scale that classifies them for a specific project as to the significance of the perceived consequence.

| | | |
|---|---|---|
| **0** | = | No consequence, the project continues without notice. |
| **50** | = | Meaningful consequence, the project loses benefits for which it was initiated and may require significant changes. |
| **100** | = | Critical consequence, the project ends in failure. |

Why do we care about identifying risks with very low probabilities? Chicken Little can answer this one for us. In an education agency, especially with the public nature of IS projects and the participation of stakeholder advisory groups, there is always the necessity to document that due diligence has been exercised in the planning for risks. Someone may raise an alarm saying that the agency has not considered a risk that they see as significant. Being prepared to silence this alarm

"Creativity requires the courage to let go of certainties."
**-ERICH FROMM**

without being leveraged into making it a priority over other documented higher risks is an important contribution by the project management team.

**Uncertainty**

Data-driven decision making assumes that we have data upon which to base our decision. What if we had no data? We typically must make a decision. Unfortunately, when it comes to assessing the risks associated with a major information system project, having reliable data about the probability of occurrences is rare.

Going back to economics, some experts (Based upon Frank Knight's 1921 distinction[1]) differentiate risk and uncertainty. Risk is reserved for use only when a reliable probability can be established for an occurrence. Without a probability, uncertainty is the preferred term. In reality, in education agencies, we seldom can place a probability on an occurrence. Therefore, we are technically almost always dealing with uncertainties. The best approach is to be aware of the negative impact of a circumstance and determine how acceptable it is—and the response to it.

So we recommend focusing more on the impact component of the risk equation, the potential negative consequence, the damage that might happen. Establishing probability is difficult, but we can get our minds around what it would mean if a negative occurrence happened.

Because risk in education agencies is really uncertainty, every decision maker, policy maker, stakeholder is free to attach whatever level of concern desired to the project. How can we manage this? Be as negative in our assessment as the most negative person is? No, but we should identify and acknowledge every possible risk.

**Risk Assessment Profile (RAP Sheet)**

ESP uses the Risk Assessment Profile to describe a specific risk factor. Figure 6 is an example of a high-risk factor, Figure 7 is a marginal risk factor, and Figure 8 is an acceptable risk factor.

The Risk Index (RI) measures the overall real and perceived risk potential from a negative occurrence. The scale goes from the lowest level of risk at 1 to the highest level at 100. The RI is determined by estimating the probability of the occurrence; then estimating the full impact; then scaling that down by the estimated severity of the occurrence for both implementation and benefits; and finally backing out the effectiveness of mitigation efforts. For example, by looking at the graphics in Figures 6-8, the risk level is evident by how much red fills the graph. As the combination of impact and the risk mitigation effectiveness lessens, the proportion of red on the risk side of the graph reduces.

The RI represents a value between the maximum potential risk and the certain risk, determined by the tolerance of the agency for this risk. If an agency has zero tolerance for the risk, then the maximum risk value becomes the RI. If the agency has complete tolerance, then the minimum risk value becomes the RI.

---

[1] Knight, Frank H. *Risk, Uncertainty, and Profit.* Boston, MA: Hart, Schaffner & Marx; Houghton Mifflin Company, 1921.

## Risk Assessment Profile

Name of Risk: **Hardware Delivery** **Risk Index: 88%**

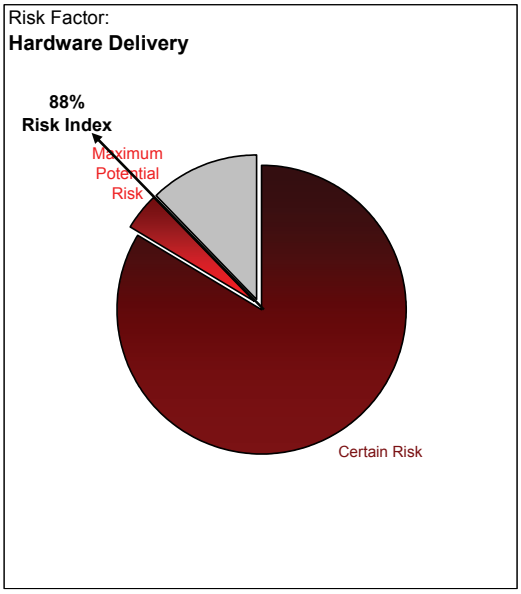
Negative Consequence Assessed: Late installation of hardware prevents on-time implementation.

What event or action would trigger this consequence? Notification by vendor of delay or failure of hardware to arrive on time.

| | | |
|---|---|---|
| What is the probability this event or action will occur? | 95% | **A** |
| **What is the consequence or damage that might occur to...?** | | |
| The Implementation of the project? | 100% | **B** |
| What weight does implementation have? | 90% | **C** |
| The ultimate benefits of the project? | 25% | **D** |
| What weight do benefits have? | 10% | **E** |

C + E = 100

| | | |
|---|---|---|
| **What mitigation efforts will be implemented?** | Weekly confirmation with vendor. | |
| How effective might these be? | 5% | **F** |
| How tolerant of this risk and the negative consequences is the agency? | 0% | **G** |




**Hardware Delivery Risk**

| | |
|---|---|
| Certain Risk | 83% |
| Maximum Potential Risk | 88% |
| Tolerance | 0% |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Maximum Potential Risk = | [(BXC) 90% | + | (DXE)] 3% | X | A = 95% | 88% | **H** |
| Certain Risk = | H 88% | - | (H*F) 4% | = | | 83% | **I** |
| Risk Index = | H 88% | - | [(H-I) 83% | X | G] = 0% | 88% | **Risk Index** |

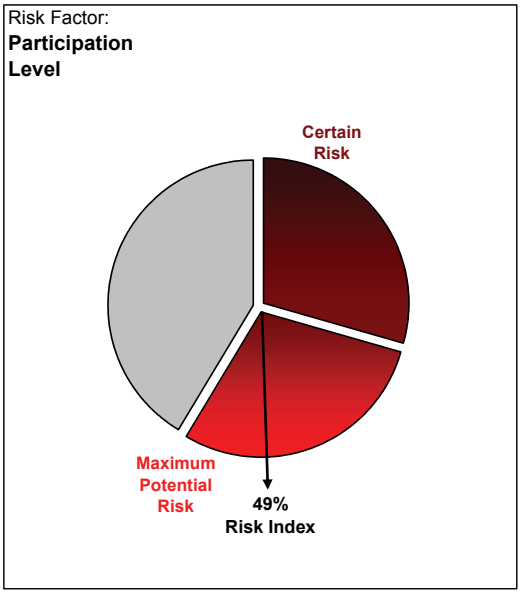
**Figure 6: High-Risk Factor**

"A life spent making mistakes is not only more honorable but more useful than a life spent in doing nothing."
**-GEORGE BERNARD SHAW**

## Risk Assessment Profile

Name of Risk: **Participation Level** **Risk Index: 49%**

| | | |
|---|---|---|
| Negative Consequence Assessed: | Participation by schools will be too low to maintain the support for the project. | |
| What event or action would trigger this consequence? | Memoranda of Understanding unsigned by more than 75%. | |
| What is the probability this event or action will occur? | 67% | **A** |
| **What is the consequence or damage that might occur to...?** | | |
| The Implementation of the project? | 100% | **B** |
| What weight does implementation have? | 50% | **C** |
| The ultimate benefits of the project? | 75% | **D** |
| What weight do benefits have? | 50% | **E** |
| | C + E = 100 | |
| **What mitigation efforts will be implemented?** | Marketing campaign to be designed and implemented. | |
| How effective might these be? | 50% | **F** |
| How tolerant of this risk and the negative consequences is the agency? | 33% | **G** |




**ParticipationLevel Risk**

| | |
|---|---|
| Certain Risk | 29% |
| Maximum Potential Risk | 59% |
| Tolerance | 33% |

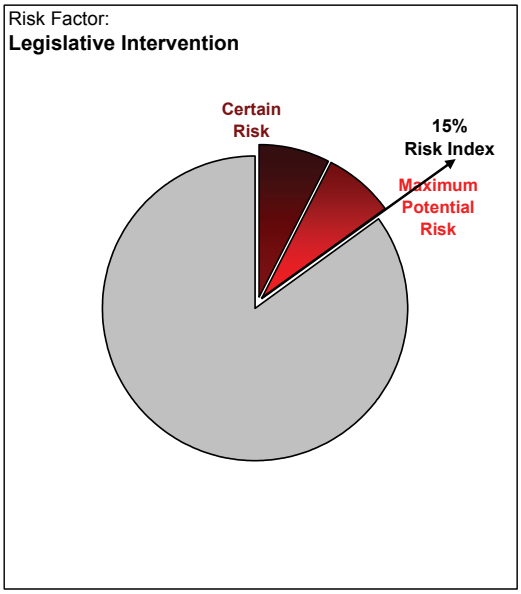
| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Maximum Potential Risk = | [(BXC) 50% | + | (DXE)] 38% | X | A = 67% | 59% | **H** |
| Certain Risk = | A 59% | - | (A*F) 29% | = | | 29% | **I** |
| Risk Index = | H 59% | - | [(H-I) 29% | X | G] = 33% | 49% | **Risk Index** |

**Figure 7: Moderate-Risk Factor**

## Risk Assessment Profile

Name of Risk: **Legislative Intervention** **Risk Index: 15%**

| | | |
|---|---|---|
| Negative Consequence Assessed: | Legislature will pass a law that funds a competing project. | |
| What event or action would trigger this consequence? | Governor's signature on legislation. | |
| What is the probability this event or action will occur? | 20% | A |
| **What is the consequence or damage that might occur to...?** | | |
| The Implementation of the project? | 75% | B |
| What weight does implementation have? | 50% | C |
| The ultimate benefits of the project? | 75% | D |
| What weight do benefits have? | 50% | E |
| | C + E = 100 | |
| **What mitigation efforts will be implemented?** | Lobbying with legislators. | |
| How effective might these be? | 50% | F |
| How tolerant of this risk and the negative consequences is the agency? | 0% | G |




**Legislative Intervention Risk**

| | |
|---|---|
| Certain Risk | 8% |
| Maximum Potential Risk | 15% |
| Tolerance | 0% |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Maximum Potential Risk = | [(BXC) 38% | + | (DXE)] 38% | X | A = 20% | 15% | H |
| Certain Risk = | A 15% | - | (A*F) 8% | = | | 8% | I |
| Risk Index = | H 15% | - | [(H-I) 8% | X | G] = 0% | 15% | **Risk Index** |

**Figure 8: Low-Risk Factor**

"Whatever you do, you need courage. Whatever course you decide upon, there is always someone to tell you that you are wrong. There are always difficulties arising that tempt you to believe your critics are right. To map out a course of action and follow it to an end requires some of the same courage that a soldier needs. Peace has its victories, but it takes brave men and women to win them."
**-RALPH WALDO EMERSON (PROBABLY ERRONEOUSLY)**

**Impact Indicator**
Estimating impact is difficult. Often this is measured as merely high, medium, or low based upon a professional judgment. For this indicator, we illustrate using a 101-point scale, 0 being no risk, and 100 being high.

Our Impact Index has two components—damage to the implementation of the project and reduction in the ultimate benefits of the project. An occurrence can impact one or the other or both. Each of the two can be weighted or considered equally important.

**Risk Mitigation Indicator**
Reducing the overall risk index is accomplished by anticipating that even if the occurrence happens, the risk mitigation efforts that will be implemented will have a positive effect. Because we seldom know probabilities and can only estimate the extent of potential damage or the effectiveness of our best efforts to mitigate risk, professional judgment and experience with similar circumstances must be relied upon heavily.

**Risk Tolerance**
Another variable in the determination of risk for an education agency is how tolerant the agency is to the risk. Some consequences (e.g., implementation delays) may be tolerated more than others (e.g., cost over-runs). In Figures 6 and 7, the difference between the maximum risk level and the potential minimum mitigated risk level becomes the possible range for tolerance. With zero tolerance, the full potential risk becomes the value. With complete tolerance, the value is the minimum risk level.

**Too Complicated?**
This full methodology does require a bit of dedicated effort. Even if you do not use the full model, walking through a few examples will help you understand the components and the dynamics that make risk assessment so complex. Keep in mind as well, estimating is often the best approach. Don't worry too much about the exact numbers. From the business literature, it's quite evident the major corporations don't have the desired level of precision they would want either.

**Buy vs. Build**
The degree to which an IS project is innovative influences risk. Innovative projects can find fewer best practices to mimic. They can expect fewer vetted solutions to be available. Risks are just higher with innovation. One strategy to avoid innovation is to look for a solution to buy. Maybe someone else innovated before you.

Whether to buy an information systems solution or to build one has become a classic question across education agencies. However, the experience of ESP professionals has been that education agencies seldom have the capacity to design and build the sophisticated systems demanded by schools and their administrative support departments. Instead of assuming this conclusion is correct, let's examine the choice from the perspective of risk. We'll begin with some definitions.

**Design/Build:** Starting from scratch, describing the requirements desired, then building the solution. A design/build project may be performed totally with in-house staff or contracted out—or a combination.

**COTS:** A commercial off-the-shelf solution that is purchased as a completed solution, but may be configured somewhat to meet local needs.

- Configure: To select settings available within the established design of a COTS solution.
- Customize: To change something about a COTS solution. This may impact the availability of support and maintenance from the solution provider. Some COTS sellers are willing to customize their product—for the right price.

Is the risk level higher or lower with a COTS solution? Figure 9 compares the two approaches.

| Risk | Risk Level | |
|---|---|---|
| | COTS | Design/Build |
| **Localization**: The solution will require retraining to replace local terminology, processes, formats, etc. | Higher | Lower |
| **Benefits**: The application will not meet all of the needs of the users and the education agency. | Similar | Similar |
| **Time**: The implementation will take longer than planned—maybe too long—maybe never get done. | Lower | Higher |
| **Quality**: The final IS application will not perform up to expectations. | Lower | Higher |
| **Cost**: The solution will cost more than expected. | Lower | Higher |
| **Maintenance**: After initial implementation, the maintenance of the system will be adequate. | Lower | Higher |
| **Enhancements**: Enhancements will not occur within reasonable limits of time, quality, and cost. | Lower | Higher |

**Figure 9: Comparison of Risks for COTS vs. Design/Build**

The COTS alternative wins **IF** there is an acceptable one available.

The design/build alternative looks great mostly as a last resort—when no acceptable COTS is available. If chosen, the risks should be carefully understood. For a risk-averse education agency, the COTS choice is hard to beat—especially if the vendor is willing to make reasonably-priced customizations.

Before you write off this assessment as self-serving coming from a vendor of commercial solutions, don't forget that ESP's professionals have been in every state education agency and a large number of districts documenting how effective their

information systems—COTS and in-house—turned out to be. Unfortunately, it is true that both vendors and in-house education agency staff typically overestimate their capacity to build the perfect information system. The bottom line, however, is that you can look at and test out a COTS product, while an in-house development project is always speculative.

# Confront the Risks (Impress decision makers with the priority that risk mitigation receives throughout the project)

## STEP 4: Mitigate priority risks with a specific plan

**Risk Mitigation Strategies**
In finance, there are four main methods with which risks can be dealt within the context of an organizational risk management strategy. Risks can be:

- Reduced or eliminated
- Transferred
- Avoided
- Absorbed or pooled

For education agency IS projects, these strategies translate as follows:

- Reduced or eliminated: Mitigation strategies are implemented throughout the project management plan.
- Transferred: The responsibility for the risk is assigned to another entity through the use of a performance bond, insurance policy, or a contract with another agency or company.
- Avoided: The risky action is not taken or the project is abandoned.
- Pooled: A partner entity is recruited to share the risk, such as a collaborative consortium, or professional organization.
- Absorbed: The risk is merely accepted. More dollars are appropriated: expectations or requirements are adjusted; more time is allocated; etc.

**Proactive Strategies vs. Reactive Ones**
Each of these five strategies can be practiced proactively or reactively as shown in Figure 10.

| Strategy | Proactive | Reactive |
|---|---|---|
| Reduce or eliminate the risk. | Create a project plan including avoidance and mitigation strategies. | Use change orders or implementation adjustments to respond to events. |
| Transfer the risk. | Contract with another entity or vendor; Negotiate with another agency to accept responsibility for the project. | Use the same strategies but they are more difficult to implement. |
| Avoid the risk. | Forego the project or the tasks that generate the risk. | Abandon the project or the tasks that generate the risk. |
| Pool the risk. | Create a collaborative to share the risk; purchase insurance; require a performance bond; require contractor insurance. | Use the same strategies but they are more difficult to implement. |
| Absorb the risk. | Build in contingency resources; transfer resources from other projects. | Increase the budget; add resources; increase revenue or fees; add time; lower expectations; reduce requirements; change contractors; change products. |

**Figure 10: Risk Mitigation Strategies**

Education agencies use all of these strategies, but only well-planned projects include the proactive strategies that are more effective.

## STEP 5: Monitor and report on risks consistently

Figure 11 is an example of a Risk Management Report that can be maintained continually throughout a project. Risks to be tracked are described along several dimensions.

- Priority
  - Unacceptable Risk: Direct project management strategies are applied and monitored continually.
  - Marginal Risk: Project management must determine the cost-benefit of applying resources to these risks.
  - Acceptable Risk: Factors are monitored to ensure risks remain acceptable.

"You won't skid if you stay in a rut."
**-KIN HUBBARD**

- Risk Rating
    - 1 – 9 Rating from the scale
- Potential Risk Description:  Brief narrative describing the risk
- Triggers:  The occurrences that create damage
- Mitigation Strategy:  Brief description of the actions to be taken
- Status:  Current status of the actions
- Rating History:  Tracking of changes in the ratings over time

Only those risks that warrant continual monitoring need to be charted.  The format of the report should vary to include information desired by the project oversight group.

| Current Risk Rating | | Potential Risk | Mitigation Strategy | Status | Rating History |
|---|---|---|---|---|---|
| **Unacceptable Risk** Education agency must take some additional action to lower the risk. | 9 | Knowledge transfer will not occur at the right times and with enough depth to allow the education agency to continue the project independent of contractor's assistance. | 1 Knowledge Transfer Plan by contractor and education agency<br>2 Documentation of knowledge transfer activities. | 1 Not completed<br>2 Not ready | 7/12/07 9 |
| | 8 | Burden on districts to implement or participate (e.g., provide data, learn to generate reports) will outweigh the perceived benefits. | 1 Clear participation guidelines<br>2 Accurate burden assessment and forecasts<br>3 Alignment with existing requirements. SIS vendors will be informed of the requirements.<br>4 ETL processes for the major SIS products are being developed. | 1 In Progress<br>2 Planned<br>3 In Progress<br>4 In Progress | 6/6/07 8 |
| | 7 | Participating districts will not have the resources required to provide the data necessary for useful reports. | 1 Data requirements aligned with inventories of available data<br>2 SIS and other software vendors informed of the data requirements so they can support their client districts<br>3 Districts supported with financial assistance for needed resources | 1 In Progress<br>2 Planned<br>3 Planned | 6/6/07 7 |
| **Marginal Risk** Risks that should be looked at on a case by case basis to determine whether additional education agency efforts are required. | 6 | Contractor and education agency will encounter difficulties in communication and working together. | 1 Non disclosure agreements<br>2 Status meetings<br>3 Document sharing<br>4 Timely calls | 1 Completed<br>2 Ongoing<br>3 Ongoing<br>4 Ongoing | 6/6/07 6 |
| | 5 | Changes to data requirements will demand continuous updating of the data model and table structure. | 1 One of the four education agency support positions to manage these changes | 1 Planned | 6/6/07 5 |
| | 4 | SIF capability will become a burden on districts and their SIS vendors and add to the cost and complexity of participation in the project. | 1 SIF company contracted to plan the implementation and infrastructure<br>2 Education agency monitoring SIS vendor capabilities<br>3 SIF an option not a requirement for participation | 1 Completed<br>2 In Progress<br>3 Ongoing | 6/6/07 4 |
| **Low Risk** Risks have a low probability and low impact. No action by the education agency is required. These issues should be monitored. | 3 | Legislature could pass legislation that establishes competition for this project without providing a way for the project to compete for internal development and management. | 1 Monitoring of Legislature<br>2 Partnership with other agencies<br>3 Roll out of project and establishment of credibility before action is considered by the Legislature | 1 Ongoing<br>2 Not Started<br>3 In Progress | 6/6/07 3 |
| | 2 | Planned venue for training will be unavailable during high-demand months. | 1 Alternative sites identified and reserved. | 1 Completed | 6/6/07 2 |
| | 1 | New version of SIF standard will be released before training and require revisions to documentation. | 1 Resources reserved to make last-minute changes to documentation. | 1 Completed | 6/6/07 1 |

**Figure 11: Sample Risk Management Report**

**Risk Priorities**

ESP built its Quality Project Management methodology around the tenets of the Project Management Institute (PMI), a certifying body for project managers. Within PMI's methodology are six stages of project management. These are defined and discussed in their relationship to education agency projects in ESP's Optimal Reference Guide, ***Why 70% of Government IT Projects Fail—Quality Project Management for Education Agencies***. Here, our interest is when within these phases is risk most significant. Figure 12 illustrates the changing priority of the four Capacity Factors of risk across the six stages. Figure 13 illustrates the changes for the Delivery Factors.

Capacity factors vary widely in their risk profile across the implementation phases. Funding is significant before the project begins and when the bills become due during implementation; however, expertise is a significant risk at every stage.

Delivery factors vary less dramatically, increasing in importance as the project progresses.

A skilled project manager with expertise in education agency projects will understand these cycles and ensure that risk factors receive due attention at their crucial stages.

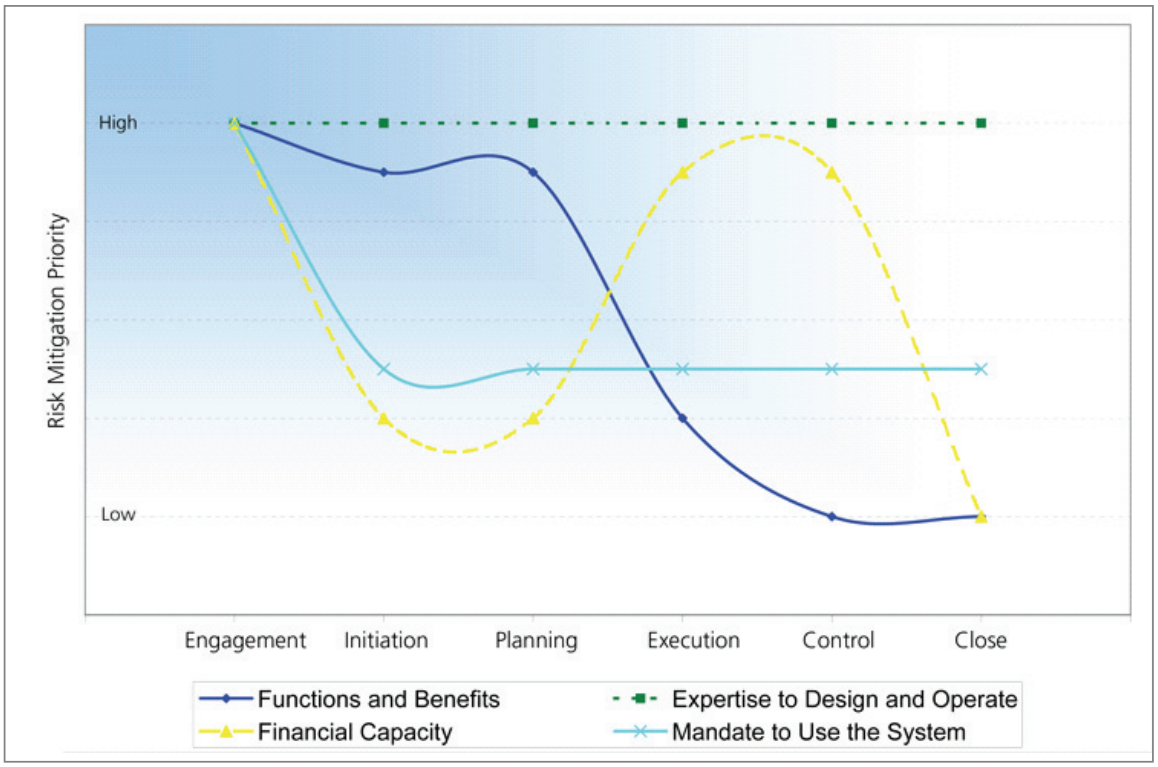



**Figure 12: Risk Mitigation Priority**

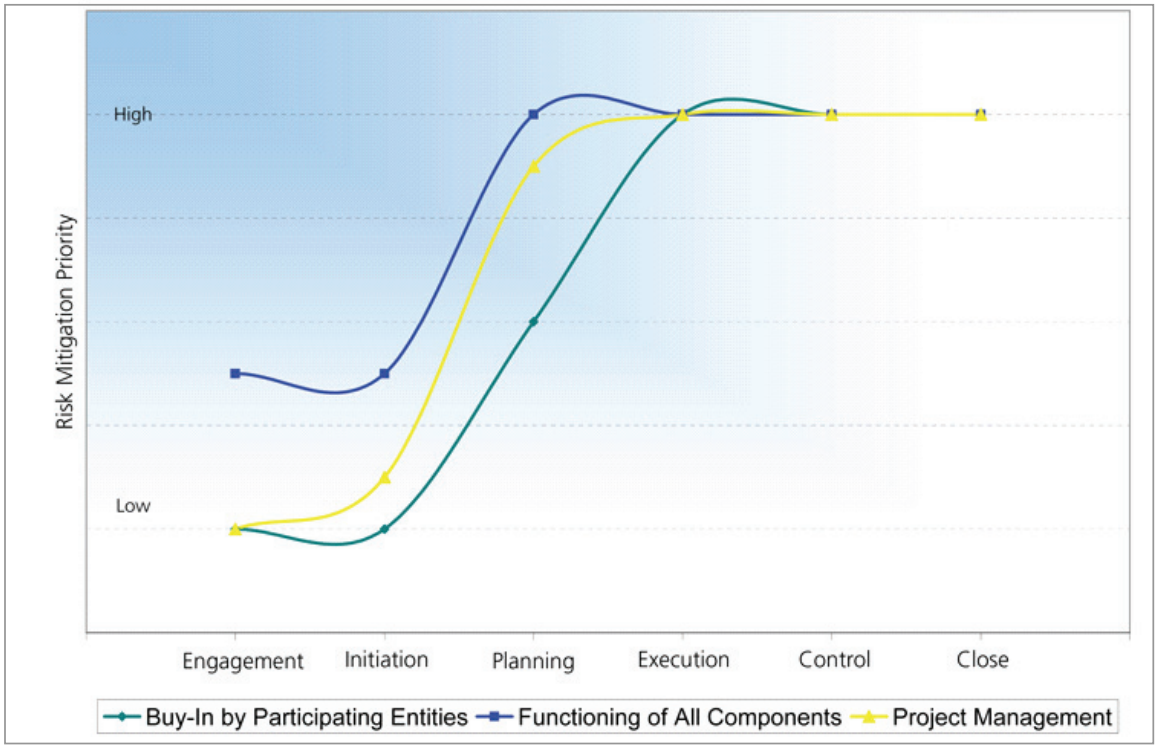



**Figure 13: Risk Mitigation Priority**

## Conclusion

Risks should not be downplayed. Decision makers should not merely be reassured that all will be fine. Both these strategies by project managers have caused decision makers to be reluctant, hesitant, and over-cautious. All these characteristics are dysfunctional to the implementation of an IS project that has definite timelines and high expectations. The success strategy advocated here is for the project managers to be the ones proclaiming the risks, ensuring every risk is known and acknowledged. When this strategy is accompanied by a well-crafted risk-mitigation plan that is published and monitored continually, successful implementation is more likely.

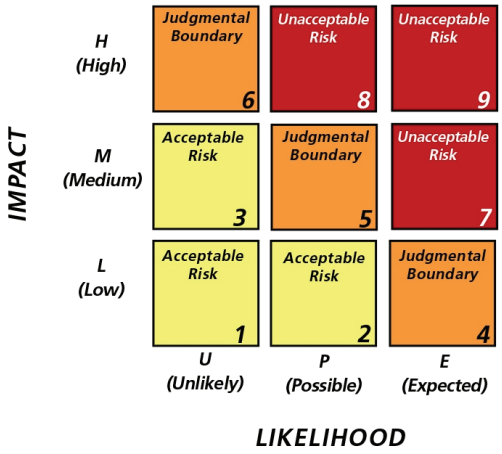
Risk will always accompany an IS project. Identifying and understanding the significance of each risk is the shared responsibility of the education agency and a contractor. ESP has thought carefully about our role in risk mitigation to ensure that we are valuable partners in the success of every IS project we implement. In the final analysis, the benefits to the students served by the education agency will always be the primary focus when assessing the risk-benefit equation of any IS project.

# ESP RISK Assessment Matrix

**Probability:** To assess likelihood you should ask the following: Given the current situation is there a low, medium, or high likelihood that the risk will be realized and become an actual problem?

**Impact:** The assessment of impact and the specific definition created for "low," "medium," and "high" should consider impact from several perspectives including:

- Damages and liability (e.g., financial, health and safety, environmental, legal)
- Operational effects (e.g., disruption in service, loss of knowledge, under-achievement of corporate objectives)
- Credibility loss (related to the USED, SEA, districts, schools, vendors, other stakeholders, the public, and legislators)




**Example of a Risk Matrix**
Here is an example illustration of a "Risk Matrix." Note that the areas identified as "acceptable" or "unacceptable" will vary depending upon how the scales for "probability" and "impact" were defined and what level of risk education agency is willing to accept.

**Acceptable Risk:** No further education agency action is required.

**Marginal Risk:** those risks that should be looked at on a case by case basis to determine whether additional education agency efforts are required. The education agency will have to decide whether it is cost-effective to take further actions to mitigate this risk.

**Unacceptable Risk:** The education agency must take some additional action to lower the risk.

**Definition of Probability:**

- Unlikely (The risk is unlikely to occur in the course of the IS project);
- Possible (The risk could possibly occur in the course of the IS project); and
- Expected (The risk is expected to occur in the course of the IS project)

**Definition of Impact:**

- Low (The consequence will create a challenge for the education agency that could be easily rectified with reasonable resources);
- Medium (The consequence will create some problems for education agency that will require moderate effort and resources to rectify.); and
- High (The consequence will create major damage that will require significant education agency effort and resources to rectify.)

**Definition of Status:** Descriptor of the current status of the risk mitigation

"You've got to jump off cliffs all the time and build your wings on the way down."
-**ANNIE DILLARD**

strategy planned, ongoing, not ready, not completed, in progress, complete.

# ATTACHMENT A – Security Risk Resources

This ORG specializes in risk analysis during the implementation phases of an IS project. After the project has been launched, a different perspective on risk emerges. This attachment provides some of the resources focused on operations and maintenance that were found during our preparation of this ORG.

The Software Engineering Institute, Carnegie Mellon University, developed the OCTAVESM Method, which can be explored at http://www.cert.org/octave/methodintro.html.

The Facilitated Risk Analysis Process (FRAP), is explained at http://csrc.nist.gov/nissc/2000/proceedings/papers/304slide.pdf.

Security risks are a priority in the banking and other industries. ESP has found the recommendations of the American Bankers Association to be useful in this area. In addition, these other references are often cited by other agencies and organizations.

## Recommended Resources for IS Risk Assessment and Information Security by the American Bankers Association

Common Criteria (International Standards Organization (ISO) 17799): The common criteria represents an international standard for testing the effectiveness of most security systems. Information about the criteria can be found on the Internet at: www.commoncriteria.org, however, a copy of the criteria must be purchased from the ISO (their web site is at: www.iso.org).

Control Objectives for Information Technology (COBIT): Developed by IT auditors and made available through the Information Systems Audit and Control Association (ISACA). Available on the Internet at www.isaca.org/cobit.htm. COBIT provides a framework for assessing a security program, developing a performance baseline, and measuring performance over time.

SysTrust: Developed by the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Public Accountants and available on the Internet at: www.aicpa.org/assurance/systrust/index.htm. SysTrust provides a framework for evaluating controls for information systems assurance.

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE): Developed by the Computer Emergency Response Team at Carnegie Mellon University. Available on the Internet at: www.cert.org/octave. OCTAVE provides measures based on accepted best practices for evaluating security programs.

NIST Documents on Risk Assessment: The US National Institute of Standards and Technology has published several documents that outline frameworks for conducting technology risk assessment and evaluating information security. The publications are available on the Internet at: csrc.nist.gov. Two of the most helpful documents are Special Publication 800-26, "Security Self-Assessment Guide for

Information Technology Systems," and Special Publication 800-30, "Risk Management Guide for Information Technology Systems."

## Other Recommended Web Sites for General Information Security Information

*Industry and Professional Associations (including Academic Institutions)*

- CSI (Computer Security Institute): http://www.gocsi.com
- SANS Institute: http://www.sans.org
- CIS (Center for Internet Security): www.cisecurity.org
- FS/ISAC (Financial Services Information Sharing and Analysis Center): www.fsisac.com
- BITS (Technology Subgroup of the Financial Services Roundtable): www.bitsinfo.org
- CERT (Computer Emergency Response Team): www.cert.org
- CERIAS (Center for Education and Research in Information Assurance and Security): www.cerias.purdue.edu
- NT BugTraq: http://www.ntbugtraq.com

## U.S. Government and Law Enforcement Organizations

- Federal Computer Incident Response Center (FedCIRC): www.fedcirc.gov
- NIPC (National Infrastructure Protection Center): www.nipc.gov
- Infragard: www.infragard.net
- Computer Crime and Intellectual Property Section (CCIPS) of the U.S. Dept. of Justice: www.cybercrime.gov
- CIAO (Critical Infrastructure Assurance Organization): www.ciao.gov
- National Institute of Standards and Technology: www.nist.gov
- Computer Security Resource Center: csrc.nist.gov
- National Security Agency: www.nsa.gov


# ESP Optimal Reference Guides and Optimal Reference Books

ESP covers a wide variety of education topics with our series of informational whitepapers called Optimal Reference Guides (ORGs) and Optimal Reference Books (ORBs). All are available for free download at *www.espsolutionsgroup.com/resources.php*. You can also subscribe to our monthly newsletter to have ORGs and ORBs emailed to you as soon as they are published. Just visit the link above for more information.

### Data Quality
- The Data Quality Imperative, Data Quality Series—Part I
- The Data Quality Manual, Data Quality Series—Part II

### Data Management
- Actions Speak Louder than Data
- From Information to Insight—The Point of Indicators
- Aligning Indicators and Actions
- Data Management Strategy for States and Districts
- Defining Data
- Management of a Education Information System
- Our Vision for D3M
- Using Assessment Results to Get Performance Results
- Why Eva Baker Doesn't Seem to Understand Accountability—The Politimetrics of Accountability

### Longitudinal Data Systems
- D3M Framework for Building a Longitudinal Data System
- The Dash between PK and 20: A Roadmap for PK-20 Longitudinal Data Systems
- What's Really "In Store" for Your Data Warehouse? Data Warehouse Series—Part I
- What's Behind Your Data Warehouse, Data Warehouse Series—Part II
- Accessing Student Records in a State Longitudinal Database, Data Warehouse Series—Part III

### Project Management
- Why 70% of Government IT Projects Fail, Project Management Series—Part I
- From Risk to Reward: A Guide to Risk Management, Project Management Series—Part II
- Marketing Your Field of Dreams, Project Management Series—Part III

### Electronic Transcripts
- Electronic Student Records and Transcripts: The SEA Imperative
- Why Your State Needs a PK-20 Electronic Record/Transcript System

### Standards
- Articulating the Case for Course Numbers
- Confidentiality and Reliability Rules for Reporting Education Data
- FERPA: Catch 1 through 22
- Graduation Rates: Failing Schools or Failing Formulas?
- National Education Data Standardization Efforts
- Racial/Ethnic Data Reporting in Education
- Recommended Data Elements for EDEN Reporting
- Revisions to FERPA Guidance

### Trends in Education
- Data-Driven Decision Making 2016
- How Education Information Fared in the Last Decade
- IT Defined…for the Educator
- Why My Space Matters to the K-12 Space

### Student/Staff Identifiers
- Requirements for an RFP for Student Identifiers
- Statewide Student Identifier Systems

### Disaster Prevention & Recovery
- Disaster Prevention and Recovery for School System Technology

### Growth Models
- Growth Model Growing Pains, Growth Model Series—Part I
- Comparison of Growth and Value-Add Models, Growth Model Series—Part II
- Making a Year's Growth and Performing on Grade Level: Muddled Definitions and Expectations, Growth Model Series—Part III
- Growth Models—Finding Real Gains

**ESP Solutions Group**

**(512) 879-5300**

**www.espsolutionsgroup.com**