12 Risk-Opportunity Assessment and Control

In Chapter 4, we noted that when we use the term “risk,” we include not only the negative uncertainties normally associated with risks, but also the positive uncertainties associated with opportunities. Thus, the ICSM is really risk and opportunity driven, in that whenever resources are expended identifying and dealing with risks, they can also be expended in identifying and dealing with opportunities. In this chapter, we address both.

12.1 The Duality of Risks and Opportunities

As discussed in Chapter 4, the generally accepted quantity for reasoning about risk is Risk Exposure RE = Probability (Loss) * Size (Loss). Opportunity can be considered as a dual to risk, as a decision not to pursue an opportunity has a negative expected value equal to the probability of success for the opportunity times its size of gain if it succeeds. This could be called its risk exposure, but it is more positive to call it its Opportunity Exposure OE = Probability (Gain) * Size (Gain).

Robert Charette defines such a holistic view as risk entrepreneurship. While Charette primarily discusses this as an enterprise, CxO-level strategy, the concept operates as effectively for system development within any of the ICSM process instantiations. To Charette, risk entrepreneurship “is as much a philosophy as a business strategy. ... Risk-entrepreneurial companies aggressively pursue risks that others cannot, squander few opportunities, and exploit the mistakes of their competitors. They represent the most competitive form of business that exists. These companies rarely make mistakes, and when they do, they take corrective action immediately. They are constantly positioning themselves to anticipate innovation in their operating environment.”

Risk entrepreneurs are not extreme thrill seekers; they are careful, judicial, value-aware decision makers. They understand the possible costs of risks as well as the return from the opportunities. However, where the business value is sufficiently large and the risk both understandable and within the bounds of the organization's capability to manage if it something goes awry, they have the ability and the courage to embrace the risk.

The ICSM provides an excellent framework for risk entrepreneurship through the intentional use of evidence-based decisions, anchor point milestones, and its fundamental incremental approach. Acknowledging and managing uncertainty is woven throughout the fabric of the 4 principles.

It should be noted that even when holistic in managing opportunities as well as risks, risks generally have a much stronger impact than pure opportunities (those not paired with a risk). The INCOSE/IEEE SEBoK states, not so succinctly, that:

In principle, opportunity management is the duality to risk management..... Thus, both should be addressed in risk management planning and execution. In practice, however, a positive opportunity exposure will not match a negative risk exposure in utility space, since the positive utility magnitude of improving
In other words, the utility function usually applied to project and program managers is strongly weighted toward the negative; that is, making a $1 million loss has about the same negative utility as has the positive utility of making a $5 million gain. Edmund Conrow’s excellent book, Effective Risk Management (Conrow, 2003) has some further cautions about overenthusiastic opportunity management.

12.2 Fundamentals of Risk-Opportunity Management

Most of us by now have been introduced to the fundamentals of risk management. These don’t change dramatically within the ICSM. However, because of the way in which the model is structured, the phase, frequency and execution can be different. There are also more ways to look for opportunities and to better understand risk and risk mitigation. To refresh your memory, we offer a summary of the fundamental activities – Assessment and Control – and the two qualities associated with risk management – Exposure and Leverage. We will use risk as the overarching term, but we will always consider the risk-opportunity dualism in the discussion.

12.2.1 Risk Assessment: Identification, Analysis, and Prioritization

Risk Identification produces lists of the project-specific risks or opportunities likely to change a project’s outcome. Typical identification techniques include checklists, decomposition, comparison with experience, and examination of decision drivers.

Using the ICSM is particularly helpful in risk identification in two ways. One involves identifying conflicts among the success-critical stakeholders’ value propositions. The red lines in Figure 2-2 of Chapter 2, showing instances of conflicts between the value propositions of the Bank of America MasterNet project’s Users, Acquirers, Developers, and Maintainers, are good examples of identified risks. These and their counterparts in other projects need to be addressed early during the ICSM Exploration phase, rather than leaving them to be discovered as expensive rework later on.

The other ICSM contribution to risk identification is via its evidence-based decision criteria, in that shortfalls in evidence are uncertainties or probabilities of loss, which when multiplied by their Size (Loss) becomes Risk Exposure. On the positive side, bringing the stakeholders together to identify and discuss their value propositions often produces opportunities as well as risks, in that their combined experience will often identify synergies or capabilities that can be addressed as Opportunities to be evaluated for probabilities and sizes of gain for the project.

Risk Analysis produces assessments of the gain/loss-probability and gain/loss-magnitude associated with each of the identified risks, and assessments of the compounding that may occur if risks interact to change probabilities or magnitudes when more than one happens to occur. Typical techniques include network analysis, decision trees, cost models, performance models, and statistical decision analysis.

Even for medium-size projects, Risk Identification can identify up to 100 candidate risks to address. However, about 10 project-wide risks are about the most that a project should
take on simultaneously. The overall objective of risk analysis in the ICSM is therefore to determine the relative risk exposure of each identified risk, initially just accurately enough to separate the “big rocks” from the “pebbles,” and subsequently to provide more insight on how best to reduce the big-rock probabilities and sizes of loss. If these quantities can’t be accurately determined, the project has two main choices. One is to assign relative values for $P(L)$ and $S(L)$, generally on a scale of 0 to 10. The other is to buy information to reduce risk, via stakeholder interviews, surveys, prototypes, or high-level models. These are also forms of evidence generation addressed in more detail in Chapter 15.

**Risk Prioritization** produces a prioritized ordering of the risks to be subjected to budgeted risk mitigation and control, and which are to be monitored for opportunistic risk mitigation or growth to become a serious risk requiring budgeted risk mitigation. The emphasis on risk mitigation budgets reflects the reality that projects have limited budgets, and that the relative cost of risk mitigation is as important as the relative risk or opportunity exposure. This brings into play the second fundamental risk quantity, Risk Reduction Leverage (RRL), basically the ratio of risk exposure reduction to the cost of achieving the reduction for a given risk reduction alternative.

Thus, having a high Risk Exposure may not be a good criterion for choosing risks to be mitigated. If an emerging technology is so immature that a very large budget of long schedule would be required to reduce its risks of performance, reliability, scalability, or maintainability, it would be best to defer consideration of its use until it reached a higher level of maturity. Typical risk prioritization techniques include RRL analysis, particularly involving cost-benefit analysis, and Delphi or group-consensus techniques.

**12.2.2 Risk Control: Risk Mitigation Planning, Risk Mitigation, Risk Monitoring and Corrective Action**

**Risk Mitigation Planning** produces plans for addressing each risk (e.g., via avoidance/assurance, transfer, reduction/encouragement, or buying information), including the coordination of the individual plans with each other and with the overall project plan. As above under Risk Prioritization, it is important to address situations where a risk mitigation threatens a project’s critical path, a particularly frequent occurrence with highly interactive risks that are pushing the technology frontiers in several directions at once. In such cases, it is often best to defer some of the capabilities, or if several are needed for success, to reflect this in the project’s schedule. This was the case of the CCPDS-R project described in Chapter 4, which deferred its Preliminary Design Review from a traditional Month 6 to Month 14, by which time all of the risks had been mitigated.

Typical techniques include checklists of resolution techniques, cost-benefit analysis, and standard Risk management plan outlines, forms, and elements. In many cases, though, the standard forms may be overkills; a lean alternative is provided below.

**Risk Mitigation** produces a situation in which the risks are eliminated or otherwise resolved (e.g., risk avoidance via relaxation of requirements). Typical techniques include prototypes, simulations, benchmarks, mission analyses, key-personnel agreements, design-to-cost approaches, and incremental development for risk avoidance. Opportunity assurance analysis may use technology trend analyses, multi-corporate agreements, acquisition analyses and political activities.
The five primary methods of risk mitigation are buying information, risk avoidance, risk transfer, risk reduction, risk acceptance. They are explained by example in a subsequent section.

Risk Monitoring and Corrective Action involves tracking the project’s progress towards resolving its risk exposure and taking corrective action where appropriate. Typical techniques include Risk management plan milestone tracking and a Top Ten Risk event list whose progress is reviewed and acknowledged at each weekly, monthly, or milestone project review.

A framework and checklist of goals, critical success factors, and questions for risk monitoring at decision points is provided in Chapter 15, and a spreadsheet tool for its use is provided on the book’s web site. Another useful continuous risk monitoring framework is the INCOSE System Engineering Leading Indicators Guide (INCOSE, 2012).

12.2.3 The Fundamental Risk Quantities: Risk Exposure and Risk Reduction Leverage

As discussed above, formulas for Risk Exposure (RE) and Opportunity Exposure (OE) are

\[ RE = \text{Prob}(\text{Loss}) \times \text{Size}(\text{Loss}), \]

where \(\text{Prob}(\text{Loss})\) is the probability of an unsatisfactory outcome and \(\text{Size}(\text{Loss})\) is the loss to the parties affected if the outcome is unsatisfactory; and

\[ OE = \text{Prob}(\text{Gain}) \times \text{Size}(\text{Gain}), \]

where \(\text{Prob}(\text{Gain})\) is the probability that an opportunity is successfully achieved and \(\text{Size}(\text{Gain})\) is the return to the parties affected if the opportunity is successfully achieved. Determining and understanding risk and opportunity exposure and their relationship is a key factor in Risk-driven processes. Balance is everything.

To relate risk exposure to project situations, we need a definition of "unsatisfactory outcome." Given that all projects involve several classes of stakeholders (customer, developer, user, maintainer, and often others such as interoperators, regulators, and venture capitalists), each with somewhat different but highly important satisfaction criteria, we can see that "unsatisfactory outcome" is multidimensional. For customers and developers, budget overruns and schedule slips are unsatisfactory. For users, products with the wrong functionality, user interface shortfalls, performance shortfalls, or reliability shortfalls are unsatisfactory. For maintainers, poor quality and bad design are unsatisfactory.

One way to look at risk exposure in context is to construct a decision tree similar to that shown in Figure 12-1. It illustrates a potentially risky situation involving the software controlling a spacecraft experiment. The software has been under development by an experiment team who understands their experiment well, but are inexperienced and somewhat casual about software development. As a result, the satellite platform manager
has obtained an estimate that there is a probability $\text{Prob}(\text{Loss})$ of 0.1 that the experimenters' software will have a critical error: one which will wipe out the entire experiment and cause an associated loss $\text{Size}(\text{Loss})$ of the total $20$ million investment.

The satellite platform manager identifies two major options for reducing the risk of losing the experiment:

- Convincing and helping the experiment team to apply better software development methods. This incurs the test cost of $500K$, and from previous experience the manager estimates that this will reduce the error probability $\text{Prob}(\text{Loss})$ to 0.05.
- Hiring a contractor to independently verify and validate (IV&V) the software. This costs an additional $300K$; based on the results of similar IV&V efforts, the manager estimates that this will reduce the error probability $\text{Prob}(\text{Loss})$ to 0.01. Also, the strongest IV&V contractor is able to perform value-based testing to reduce the test costs from $500K$ to $300K$.

The decision tree in Figure 12-1 then shows, for each of the two major decision options, the possible outcomes; their probabilities; the losses associated with each outcome, the risk exposure associated with each outcome, and the total risk exposure (or expected loss) associated with each decision option. In this case, the total risk exposure associated with the experiment-team option is $1.5M$. For the strongest IV&V option, the total risk exposure is only $0.8M$; thus it represents the more attractive option.

Besides providing individual solutions for risk management situations, the decision tree also provides a framework for analyzing the sensitivity of preferred solutions to the risk exposure parameters. Thus, for example, the experiment-team option would be preferred if the IV&V team were unable to reduce the test costs; and if the loss due to a critical software error were less than $7.5M$, if the experiment team could reduce their critical-software-error probability to less than 0.03, if the IV&V team cost more than $800K$, if the IV&V team were unable to reduce the probability of critical error to less than 0.03, or if there were various partial combinations of these possibilities. However, even with this sort of sensitivity analysis, there may not be enough information available to quantify the risk exposure parameters well enough to perform a precise analysis.
A similar approach can be accomplished to evaluate the benefit of a pure opportunity or to analyze the risk-reward balance of compound opportunities and risks.

The second fundamental risk quantity is the leverage available based on mitigation or assurance costs. **Risk Reduction Leverage** is defined as follows:

\[
RRL = \frac{RE_{before} - RE_{after}}{Risk \, Reduction \, Cost}
\]

With an \(RE_{before}\) of \(0.1 \times 20M = 2M\), the corresponding RRL values for the “No IV&V” and “Do IV&V” options are:

\[
RRL \ (\text{No IV&V}) = \frac{2M - 1M}{500K} = 2; \text{ and}
\]

\[
RRL \ (\text{Do IV&V}) = \frac{2M - 0.2M}{600K} = 3.
\]

Even without the reduced test costs, the “Do IV&V” option comes out ahead:

\[
RRL \ (\text{Do IV&V}) = \frac{2M - 0.2M}{800K} = 2.25,
\]

but the comparison is much closer.
12.2.4 The Fundamental Risk Mitigation Strategies

There are five fundamental strategies that can be used to mitigate a risk: Buying Information, Risk Avoidance, Risk Transfer, Risk Reduction, Risk Acceptance. Like the decision tree, these are equally useful in investigating opportunities.

- **Buying Information.** Sometimes, the best way of mitigating a risk is to gain more insight into the problem. Often prototyping to learn more about requirements or a specific COTS product can reduce or eliminate risks.
- **Risk Avoidance.** Avoiding a risk means taking actions that remove the risk from the critical path or the project. For example, negotiating with the customer to support a reduced performance should certain risks occur effectively mitigate the risk.
- **Risk Transfer.** Transferring risk involves an action that moves the risk from one party to another, or shares the risk exposure between several parties such that no single party is overly burdened.
- **Risk Reduction.** Actions can be taken that reduce the risk exposure by lowering the probability or the magnitude of loss.
- **Risk Acceptance.** This is a decision that the risk exposure is low enough that the project can succeed even if the risk occurs.

Here is an example of how each of these might be used for a fairly common problem in system development – COTS Selection. Suppose that at the beginning of a project, there is an opportunity to choose either a higher-performance COTS product B or a comparable but lower-performance COTS product C. Without further evidence about the relative merits of COTS products B and C, the project would choose B. However, in this case, the project then finds out during integration that B has serious architectural mismatches with another project-essential COTS product A. This will cause the project to overrun by 3 months and $300K.

At this point, the probability of this is 1.0, so it is not a risk but a problem. But earlier, its nature was uncertain and should have been identified as a risk item during an early ICSM milestone review by the experts reviewing the evidence that the selected COTS products would successfully interoperate. It would then need to be covered by a risk management plan in order to meet the review success criteria. A risk management plan can use one or more of the main risk mitigation strategies. In general, the best one to try first is buying information, which will provide more insight on which of the other strategies to employ.

**Buying Information.** The project decides to spend $30K prototyping the integration of COTS packages B and C with COTS package A. It finds the architectural mismatches between A and B, and the likely resulting costs and schedules needed to resolve them, and also finds that COTS package C would integrate easily with A, but with a 10% performance loss. This information enables the stakeholders to better evaluate the other risk mitigation strategies.

**Risk Avoidance.** This option would be best if the customer agrees that the reduction in performance is preferable to the prospect of late delivery, and agrees to go with COTS product C rather than B.

**Risk Transfer.** However, if the customer decides that the increase in performance is worth the extra time and money, the customer should establish a risk reserve of 3 months and $300K to be used to the extent that it will be needed during integration, but with award fees for the developer to the extent that less resources will be needed.
**Risk Reduction.** In order to eliminate the schedule risk, the developer and customer agree to perform a parallel integration of A and B early in the project with the added cost but with no delay in delivery schedule.

**Risk Acceptance.** The developer decides that having a proprietary solution to integrating A and B will provide them with a competitive edge on future projects, and decides to fund and patent the solution, while giving the customer a royalty-free license to use it. From a risk/opportunity standpoint, the business case for having a proprietary solution to integrating A and B would have given the developer a sufficiently high payoff to generate a positive Opportunity Exposure for taking this option.

Usually, some combination of the risk mitigation strategies will prove mutually acceptable to all of the stakeholders. However, there will be some situations in which there are irreconcilable differences between the stakeholders that leave the project with no feasible options. In this case, it is best to have found this out early rather than at the end of the project, and based on Principle 1, the ICSM decision for the milestone review is to discontinue the project with no further expenditure of stakeholders’ resources, or to redefine the project scope in a way that is mutually satisfactory to the stakeholders.

### 12.3 Risk Management within ICSM

As described in the introduction to this chapter, the ICSM provides a sound foundation for risk entrepreneurship by placing risk and opportunity at the center of the decision process. To support these decisions, evidence-based reviews provide sound data about technical progress, risks and opportunities.

Many risks stem from stakeholder concerns, misunderstandings, and inconstancy. The incremental commitment and win-win approaches are a significant mitigation for these risks, and provide a means for discussing business and technical risks before they become problems.

ICSM’s incremental development and deployment approach enables feedback and supports adaptability. Providing value early to the customer and users provides for early discovery and fixing of unsatisfactory requirements, allows for tuning of capabilities or functions to meet changing needs, and offers the chance to respond to risks that materialize late in the project or unforeseen issues that may arise.

The team structure inherent in the model’s *evolutionary view* (Figure 4 of the ICSM Distilled overview) provides a virtual “crow’s nest” for scanning the project horizon. As described, this approach establishes a separate engineering team specifically tracking sources of unforeseeable change or possible opportunities, and adjusting later increments’ specifications and plans accordingly. This focused, continuous environmental surveillance provides an ideal tool for risk entrepreneurship at the development level.

### 12.4 Risk and Opportunity Management Tools

There are a number of useful tools that can be applied within the ICSM framework.
12.4.1 Top Ten List

This is a mainstay of many risk management approaches. In essence, the project maintains a current list of the most critical risks along with associated risk management plans. The status of the risks and the mitigation activities are reviewed at least monthly. The risks on the list will evolve. Some will not occur and become moot. Others will stop being uncertain risks and become problems, and so are taken off the list and added to the project work. Others will be added as they either are identified, or their probability increases due to their relation to the project status or for other reasons.

The types of risks that are identified vary by ICSM phase. Table 12-1 provides examples of risks and pitfalls drawn from the discussion of ICSM phases in Part II.

<table>
<thead>
<tr>
<th>Table 12-1. Risks and Pitfalls by Phase</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

12.4.2 Lean Risk Management Plans

The word “Plan” often conjures up a heavyweight document full of boilerplate and hard-to-remember sections. Risk management plans should be particularly lean and risk-driven as illustrated in the outline presented in Figure 12-3.

1. Objectives (the “Why”)
2. Deliverables and Milestones (the “What” and “When”)
3. Responsibilities (the “Who” and “Where”)
4. Approach (the “How”)
5. Resources (the “How Much”)

Figure 12-3. Lean Risk Management Plan Outline.

Figure 12-4 (Boehm, 1991) provides an example of how the outline might be used to develop a risk management plan to conduct fault tolerance prototyping to mitigate identified risks that the fault tolerance features might seriously compromise performance aspects such as throughput, real-time deadline satisfaction, and power consumption. It also shows the examples of the types of information to be provided for responsibilities, the risk
management approach, and the needed funding resources. Note that much of this risk plan information can be provided in a resource-loaded network tool.

1. Objectives
Determine, reduce level of risk of the fault tolerance features causing unacceptable performance (e.g., throughput, response time, power consumption). Create a description of and a development plan for a set of low-risk fault tolerance features.

2. Deliverables and Milestones
By week 3: Evaluation of fault tolerance option, assessment of reusable components, draft workload characterization, evaluation plan for prototype exercise, and description of prototype.
By week 7: Operational prototype with key fault tolerance features; workload simulation; instrumentation and data reduction capabilities; and draft description, plan for fault tolerance features.
By week 10: Evaluation and iteration of prototype; revised description, plan for fault tolerance features.

3. Responsibilities
- System Engineer: G. Smith—Tasks 1, 3, 4, 9, 11, support of tasks 5, 10
- Lead Programmer: C. Lee—Tasks 5, 6, 7, 10 support of tasks 1, 3
- Programmer: J. Wilson—Tasks 2, 8, support of tasks 5, 6, 7, 10

4. Approach
Design-to-Schedule prototyping effort; driven by hypotheses about fault tolerance-performance effects; using multicore processor, real-time OS, add prototype fault tolerance features. Evaluate performance with respect to representative workload. Refine Prototype based on results observed.

5. Resources
$60K Full-time system engineer, lead programmer, programmer (10 weeks)*(3 staff)*($2K/staff-week)
$0K 3 Dedicated workstations (from project pool)
$0K 2 Target processors (from project pool)
$0K 1 Test co-processor (from project pool)
$10K Contingencies
$70K Total

Figure 12-4. Sample Lean Risk Management Plan

12.4.3 Electronic Process Guide (EPG)
The EPG provides templates for top ten lists, lean risk management plans and includes risk in the anchor point milestone descriptions and documentation.

12.4.4 Suggested Feasibility Risk Evaluation Criteria
In order to evaluate the findings of a feasibility assessment and determine the appropriate next steps, criteria are needed to help determine the associated risk for each finding. The following risk probability-impact framework provided in the book's web site (Boehm et al, 2009) can be used to assign a risk level to the various findings and guide the outcome of the associated Commitment Review:

Risk impact or Size (Loss) ratings vary from a critical impact of shortfalls in performing the SE task in question through significant impact and moderate impact to little-no impact, as illustrated in Table 12-2. These relative impact ratings enable projects to tailor the evaluation to the project's specific situation. The rating scale for the impact level is based on the user's chosen combination of effects on the project's likely cost overrun, schedule
overrun, and missing percent of promised over actual delivered capability (considering there are various tradeoffs among these quantities).

Table 12-2. Risk impact ratings

<table>
<thead>
<tr>
<th>Rating: Size (Loss)</th>
<th>Cost/Schedule/Capability Shortfall</th>
</tr>
</thead>
<tbody>
<tr>
<td>Little-No impact</td>
<td>0-2% (1% average)</td>
</tr>
<tr>
<td>Moderate impact</td>
<td>2-20% (11% average)</td>
</tr>
<tr>
<td>Significant impact</td>
<td>20-40% (30% average)</td>
</tr>
<tr>
<td>Critical impact</td>
<td>40-100% (70% average)</td>
</tr>
</tbody>
</table>

Using the first question in the evidence checklist in Chapter 15 (Have the Key Performance Parameters (KPPs) been identified in clear, comprehensive, concise terms that are understandable to the users of the system?) as an example, if the project were a MedFRS post-crisis data analysis application with no mission-critical key performance parameters (KPPs), its impact rating would be Little-No impact. However, if the project were a MedFRS command decision support system with several mission-critical KPPs such as response time, decision options understandability, and decision effects understandability, its rating would be Critical impact.

The Evidence/Risk rating is the project’s degree of assurance that each SE evidence question is satisfactorily addressed, scored on a Prob (Loss) scale: the less evidence, the higher the probability of shortfalls. The evaluator chooses a rating based on the probability of an unsuccessful outcome in performing the SE task in question, as noted in Table 12-3-3.

Table 12-3. Risk probability/evidence shortfall ratings

<table>
<thead>
<tr>
<th>Prob (Loss) of Shortfall</th>
<th>Degree of evidence</th>
<th>Probability Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>High probability</td>
<td>Little-no evidence</td>
<td>P = 0.4 - 1.0; average 0.7</td>
</tr>
<tr>
<td>Medium probability</td>
<td>Weak evidence</td>
<td>P = 0.2 - 0.4; average 0.3</td>
</tr>
<tr>
<td>Low probability</td>
<td>Partial evidence</td>
<td>P = 0.02 – 0.2; average 0.11</td>
</tr>
<tr>
<td>Very Low probability</td>
<td>Strong and externally validated evidence</td>
<td>P = 0 – 0.02; average 0.01</td>
</tr>
</tbody>
</table>

Again, using the question above about Key Performance Parameters (KPPs) as an example with respect to a MedFRS command decision support system with several mission-critical KPPs, then a lack of evidence (from analysis of current-system shortfalls and/or the use of operational scenarios and prototypes) that its “KPPs had been identified in clear, comprehensive, concise terms that are understandable to the users of the system” would result in a High risk probability, while strong and externally validated evidence would result in a Very Low risk probability.

Using the average probability and impact values from Table 12-2 and 12-3, the relative Risk Exposure = Prob(Risk) * Size(Risk) implied by the ratings is presented in 12-4.
Table 12-4. Average risk exposure calculation

<table>
<thead>
<tr>
<th>Impact // Probability</th>
<th>Very Low</th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>0.7</td>
<td>7.7</td>
<td>21</td>
<td>49</td>
</tr>
<tr>
<td>Significant</td>
<td>0.3</td>
<td>3.3</td>
<td>9</td>
<td>21</td>
</tr>
<tr>
<td>Moderate</td>
<td>0.11</td>
<td>1.21</td>
<td>3.3</td>
<td>7.7</td>
</tr>
<tr>
<td>Little-No Impact</td>
<td>0.01</td>
<td>0.11</td>
<td>0.3</td>
<td>0.7</td>
</tr>
</tbody>
</table>

One can then cluster the risk exposure ranges into a familiar 5-level Risk Exposure scale as follows:

1. Very Low RE: 0.01 – 0.3
2. Low RE: 0.7 - 1.21
3. Medium RE: 3.3
4. High RE: 7.7 – 9

12.5 Using Risk to Determine How Much Evidence is Enough

As discussed at the end of Chapter 4, determining how much feasibility evidence is enough is one of the decisions covered by the ICSM Meta-Principle of Balance: Balancing the risk of doing too little and the risk of doing too much will generally find a middle course sweet spot that is about the best you can do.

---

