Better Communications on IT Spending Risks

Robert D. Frum, DCS

Why are million-dollar information technology (IT) investment decisions based on single-point green, yellow, and red visual indicators, which are poorly defined and ineffective abstractions of the fundamental components of risk—probability and impact? Decisions are founded on a weak understanding of the risk without considering a range of possible outcomes for any choice of action.

IT professionals can significantly improve how they assess and communicate program risk to business investment decision makers, who must allocate funds among competing priorities. We can reform our communication of risk to

Frum, *a retired U.S. Army lieutenant colonel, is the Chief Information Officer in the Navy International Programs Office. He holds bachelor's degrees in Political Science and Computer Science, master's degrees in Business Administration and Management Information Systems, as well as a doctorate in Computer Science. He also is Level II certified in Information Technology under the Defense Acquisition Workforce Improvement Act and a certified Project Management Professional. The views expressed are the author's own and do not reflect those of the U.S. Navy or the Federal Government.*

business leaders so we provide a range of estimated outcome values, within a confidence interval that reflects the inherent uncertainties of large, complex decisions.

Monte Carlo simulation prepared with standard Microsoft Excel is a low-cost, yet effective, method for quantifiably modelling risk. Displaying the simulation results graphically as a familiar management histogram chart overlaid with a risk expectancy line enables uncertainty to be precisely articulated within a confidence interval for better-informed decision making. Risk variable values can also be changed on the fly to support dynamic what-if analysis. The model presented by the author was developed from material taught by Derek E. Brink, a Certified Information Systems Security Professional, in Harvard University's Division of Continuing Education course "How to Assess and Communicate Risk in Information Security."

The stakes are high. The federal IT dashboard indicates that government-wide IT spending for fiscal year (FY) 2017 totals about $81.6 billion. The site also specifies that for all major IT investments government-wide, 3.4 percent of the projects are considered to be high risk, and 23.2 percent are considered medium risk. The U.S. Government Accountability Office has issued several reports between 2011 and 2015 documenting failed major IT projects, including eight projects valued at more than $8.5 billion. Improved risk analysis and communication would return substantial value. For example, if the cost of failed programs was reduced by merely 1 percent, this would amount to more than $85 million saved on these eight projects alone.

The key or greatest facilitator of informed business decisions is communicating data uncertainty as a frequency and impact distribution, overlaid with an exceedance probability (EP) curve at the desired confidence level. The concept may seem complex, but the technique has been widely applied in financial, insurance, actuary, and catastrophe planning to estimate the probability that a certain level of loss will be exceeded over a given time.

I offer three assumptions regarding risk that show why I believe we must improve our assessment and communication of risk. These include:

- Risk is fundamentally determined by the likelihood of an undesirable event, and the impact of such an event.
- Risk in federal IT programs is mostly presented in qualitative terms of colors—red (high), yellow (medium) or green (low).
- Risk assessment and management are important activities for successful project management.

A More Detailed Look

Risk determination depends upon the type of threat, weakness or vulnerability. However, framing risk based only on potential dangers does very little to enable value-based investment judgments. In fact, using technical jargon to present risk supports poor value judgments because there is no assessment of the odds that something bad actually will happen. As a result, decision makers often are left with only a binary choice of whether to commit resources. For example, the IT professional might describe a cyber-security risk as an unauthorized access breach that could expose employee records to compromise if stronger access management controls are not put into place. In the best-case scenario, the business leader is somewhat better informed and at worst has misleading value information on which to base decisions. Properly framing risk in terms of the probability and associated consequence magnitude allows evaluation of the level of uncertainty. Communicating the same cyber risk as a 10 percent probability that unauthorized access could result in an annual business cost of $2 million enables the organization leaders to determine how much risk they are willing to mitigate at the corresponding cost.

Again, most risk in federal programs is presented as red, yellow or green. The color scheme is a risk representation convention described by the Department of Defense's *Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs*. The approach to relative risk levels attempts to assess risk based upon Likert scales ranging from "not likely" to "near certainty" and "minimal impact" to "critical impact." Likert scales are ordinal, meaning the data can be ranked but not accurately interpreted mathematically. In short, risk heat maps should be limited to the most basic risk prioritization. As a business investment decision support tool, the color-coded representation is ineffective for articulating quantified risk probability distributions for a range of possible outcomes for any meaningful choice of action.

Risk management seeks to define uncertainty as the probability of an event—and the business effect, positive or negative, of such an event. In terms of program and project management, risk is most often expressed for individual cost, schedule and performance variables in relationship to delivering the end product. Different disciplines such as research, engineering development, and logistics may each have its own perspective on project risk. But managing activity risk must not be confused with investment decisions that aggregate the effect of all variables to permit best-value business case investment analysis.

The subject-matter expert (SME) plays an essential role in determining risk. SMEs typically are more knowledgeable than others regarding uncertainty measures within their areas. Using the unauthorized access breach example, the cybersecurity SME might estimate the likelihood that the

Figure 1. Risk Simulation Model

Business impact risk = what is the risk that a longer project length will increase cost?

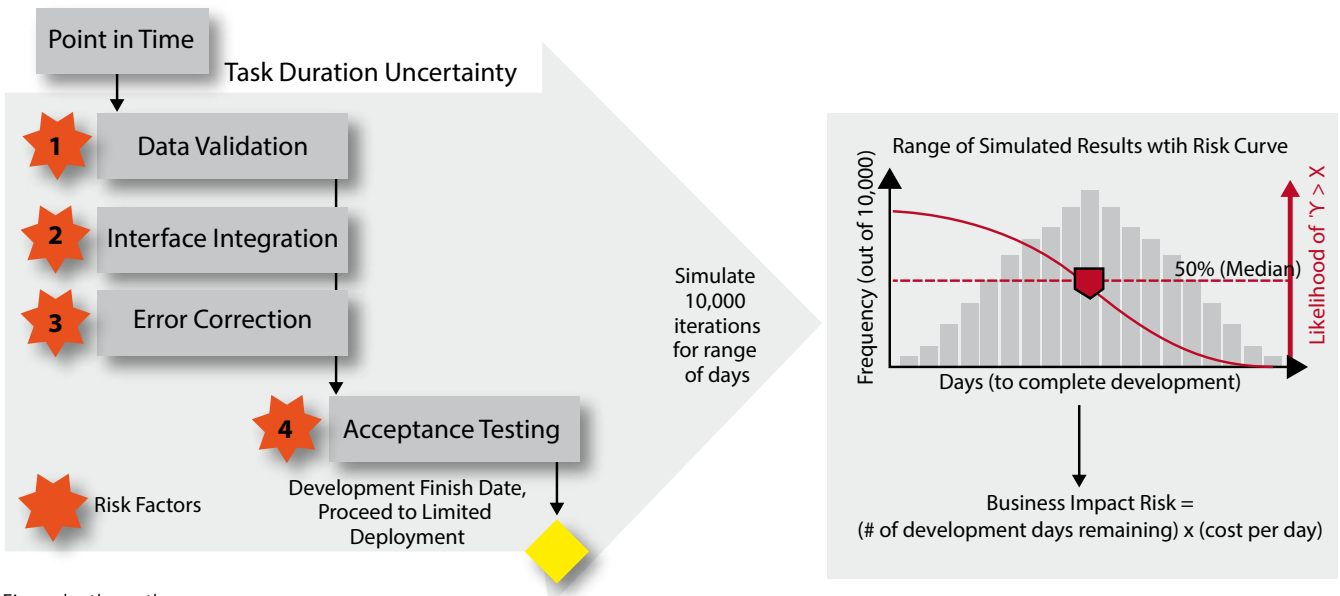

Figure by the author.

Figure 2. Project Risk Simulation

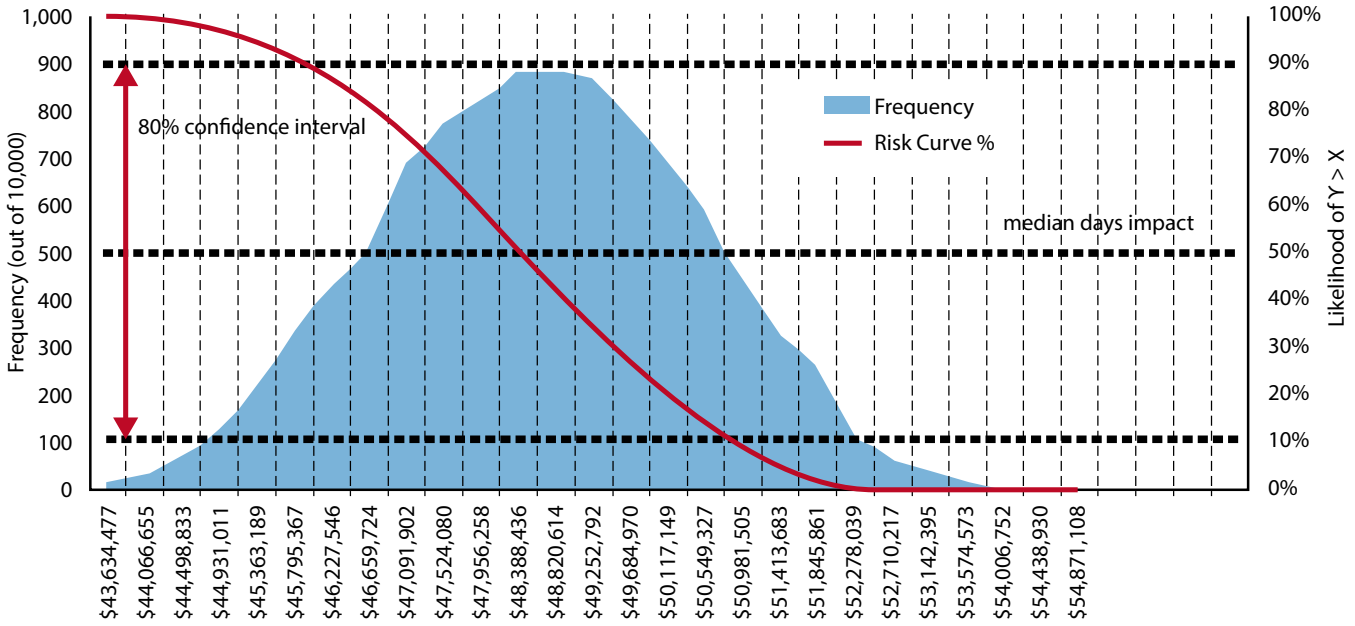

Figure by the author.

organization could experience between one and three unauthorized access breaches within the next 12 months, in line with the 2016 Ponemon Institute data breach study reporting about a 26 percent likelihood of a company having one or more data breaches involving at least 10,000 records in the following 24 months. The SME knowledge, supplemented with historical and industry data, provides a reasonable measurement of the factors of risk, while incorporating the inherent uncertainty. Typical—though insufficient—risk representation would then simply apply an annualized loss expectancy (ALE) calculation such as *annual loss = (likelihood of at least one breach) x (estimated number of breaches per year) x (estimated cost per breach)*. Given a breach cost estimated at $100,000, an ALE statement would quantify the annual potential risk as an average of $200,000. Based on this rudimentary cost analysis, risk then would be conventionally presented as red, yellow or green ordinal choices for the business leader to determine if the potential loss would be worth the financial investment needed to mitigate the risk.

Monte Carlo simulation is an excellent quantitative method for determining the likelihood of a potential loss within any of several designated intervals, over a range of values. Standard Microsoft Excel is more than adequate for creating simulation models and displaying possible scenario impact outcomes graphically as familiar charts. In the simulation model, the SMEs provide their estimates for the risk factors; specifically, providing the values for the upper and lower bounds, with a 90 percent certainty.

For example, consider a hypothetical software development project for which the business leader wants to assess the risk of the project's $40 million budget and submits the Business Impact Question: What is the risk that a longer development time will increase the overall project cost? Figure 1 illustrates the project simulation risk model, with four key risk variables that fundamentally determine the overall project duration. The model simulates the number of days to complete each factor. Factors 1, 2 and 3 are accomplished in parallel and must be completed before Factor 4 can begin; Factor 4 is then added to the highest of the three values. Daily cost is then applied to the resulting number of days.

Figure 3. Risk Simulation Chart

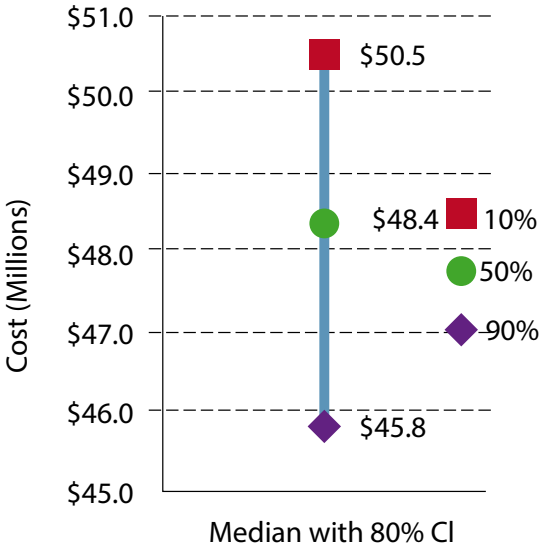

Figure by the author.

SECTION 3685, TITLE 39, U.S.C. SHOWING OWNERSHIP, MANAGEMENT, AND CIRCULATION

Defense AT&L is published bimonthly at the Defense Acquisition University, Fort Belvoir, Va. 22060-5565. The university publishes six issues annually. The director of the DAU Press is Randy Weekes; the managing editor of *Defense AT&L* is Benjamin Tyree; and the publisher is the Defense Acquisition University Press. All are colocated at the following address: Defense Acquisition University, Attn: DAU Press, 9820 Belvoir Rd., Ste. 3, Fort Belvoir, VA 22060-5565.

Average Number of Copies of Each Issue During the Preceding 12 Months

A. Total number of copies printed (net press run): 3353
B. Paid and/or requested circulation: 3227
1. Sales through dealers and carriers, street vendors, and counter sales: 0
2. Mail subscriptions paid and/or requested: 3227
C. Total paid and/or requested circulation: 3227
D. Free distribution by mail, carrier, or other means; samples, complimentary, and other free copies: 71
E. Total distribution: 3298
F. Copies not distributed: 55
G. Total: 3553

Actual Number of Copies of Single Issue Published Nearest to Filing Date

A. Total number of copies printed (net press run): 3305
B. Paid and/or requested circulation:
1. Sales through dealers and carriers, street vendors, and counter sales: 0
2. Mail subscriptions paid and/or requested: 3189
C. Total paid and/or requested circulation: 3189
D. Free distribution by mail, carrier, or other means; samples, complimentary, and other free copies: 46
E. Total distribution: 3235
F. Copies not distributed: 70
G. Total: 3305

The probability and impact simulation results for this hypothetical project are displayed in Figure 2, indicating that for 10,000 simulations there is a 90 percent likelihood that the annual cost will exceed about $46 million and a 10 percent probability that the annual cost will exceed about $50 million, with a median (50 percent likelihood) expected annual cost of about $48 million. The values between 90 percent and 10 percent represent an 80 percent confidence interval, but any level of risk can be determined simply by examining the exceedance probability curve.

When communicating with business leaders, the same information could be presented as in Figure 3. Because Excel calculates 10,000 simulations of this model in about 1 second, leaders could quickly receive answers to "what if" sensitivity analysis questions that change the risk simulation variable values such as labor and material costs, purchase versus lease, number of units produced or purchased, workforce size and payment schedules. Creating an initial risk simulation model from existing Monte Carlo modeling templates took about a week, but subsequently building the model used in this example took only about 1 hour. The simulation model is clearly a significant improvement over ALE and red-yellow-green risk communication. First, simulation considers thousands of possible outcomes, not just the average outcome. Second, simulation assesses the likelihood of each outcome. Third, risk analysis can then be communicated as quantified values rather than hunches or guesses.

Conclusions and Recommendations

Business leaders facing uncertainty for significant investments in complex and expensive IT projects require more than simple risk heat maps to inform their decisions. Accurate and meaningful communication of risk requires a quantitative measurement of business impact. Risk simulation provides an inexpensive yet effective method for reducing uncertainty, by quantifying probability and impact for a possible future event, within a specified time period, over a range of values, with a specified confidence level. Communicating risk as, "90 percent likelihood that the annual cost will exceed about $46 million with a median (50 percent likelihood) annual cost of about $48 million" is far more useful to making a better-informed business decision than simply stating that increased project cost is "Very Low, Low, Moderate, High, or Very High."

To begin transitioning from risk matrix to risk simulation for investment circumstances I recommend the following:

- Schedule FY 2018 and FY 2019 for discussion, publishing guidance and creating training opportunities. Then, beginning in FY 2020, provide that Monte Carlo risk simulation become mandatory for all IT investment decisions exceeding $1 million.
- Establish a library of basic simulation models and tutorials to facilitate rapid development for a variety of applications.

The author can be contacted at **robert.frum@navy.mil**.