

The Power of IT Investment Risk Quantification and Visualization

IT Portfolio Management

Is it worth the incremental effort to determine IT financial investment risk as part of the IT investment business case? Long, long ago (at least, in IT terms), an IT Portfolio Management Model was developed and introduced to corporate clients by a large IT company.¹ Developed in August 2003, the purpose of the model was to help clients make better decisions about investments in their IT portfolios in the context of both their burgeoning legacy IT costs and their need for IT innovation.

The IT Portfolio Management Model was based on the principles of financial portfolio management, specifically, the relationship between investment risk and investment return as per the so-called risk-return tradeoff. The tradeoff is that higher investment returns can be had only by taking on higher investment risk.²

The model also used a modified form of the Boston Consulting Group's (BCG) matrix concept of stars, cash cows, dogs and question marks to help identify the IT investments that would most likely make a sound financial contribution to the organization. The 40-year-old BCG tool is still in use today.³

This article explores that 15-year-old IT Portfolio Management Model and contrasts it with ISACA's IT-enabled investment portfolio management paradigm.⁴ Where the IT Portfolio Management Model explicitly considered IT financial investment risk and returns, ISACA's IT portfolio management paradigm explicitly considers IT returns and the IT investment mix, where "mix" represents the proportion of the IT portfolio that is invested in, for example, transactional, informational, transformational (strategic) and infrastructural information technology.⁵

Risk of Failure and the Expected Variability of Returns of an IT Investment

Assuming sound alignment between business and IT, knowing what the risk of failure and expected variability of financial returns of an IT investment

could feasibly cause stakeholders to rethink how it would be deployed, how it would be resourced, and the nature of process development required to ensure repeatability and consistency.

This is because commitments will have been made to the chief executive officer (CEO) and/or the board of directors (BoD) about the capabilities of the new investment to help realize the organization's strategic and financial objectives, with the chief information officer (CIO) noting that IT project failure would compromise those objectives, possibly with considerable reputational risk to the organization.

Monte Carlo simulation techniques help users visualize IT investment variability and the risk of failure. For example, **figure 1** shows a prospective IT investment with an assessed mean expected return of about US \$290,000, a standard deviation

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website (www.isaca.org/journal), find the article and click on the Comments link to share your thoughts.

<https://bit.ly/2slmGcl>



Guy Pearce, CGEIT

Has served on boards in banking, financial services, retail and not-for-profits over the last decade. He also served as chief executive officer of a multinational retail credit business, where he led the organization to profitability after the 2008 global financial crisis. He has published numerous articles on data and IT, and today consults on corporate governance, IT governance and data governance.

of about US \$200,000, and a ± 30 percent probability that the project will produce negative financial returns (financial failure). Metrics like these are useful because they help define the organization's IT investment risk appetite, which guides decisions about whether a new IT investment should be approved.

With some reporting that most IT projects fail,^{6,7} what probability of failure would an organization be willing to accept? Is it preferable to go into an IT deployment assuming it will be successful or should more up-front planning be mandatory? IT investment risk analysis helps provide a context for the answers to these questions.

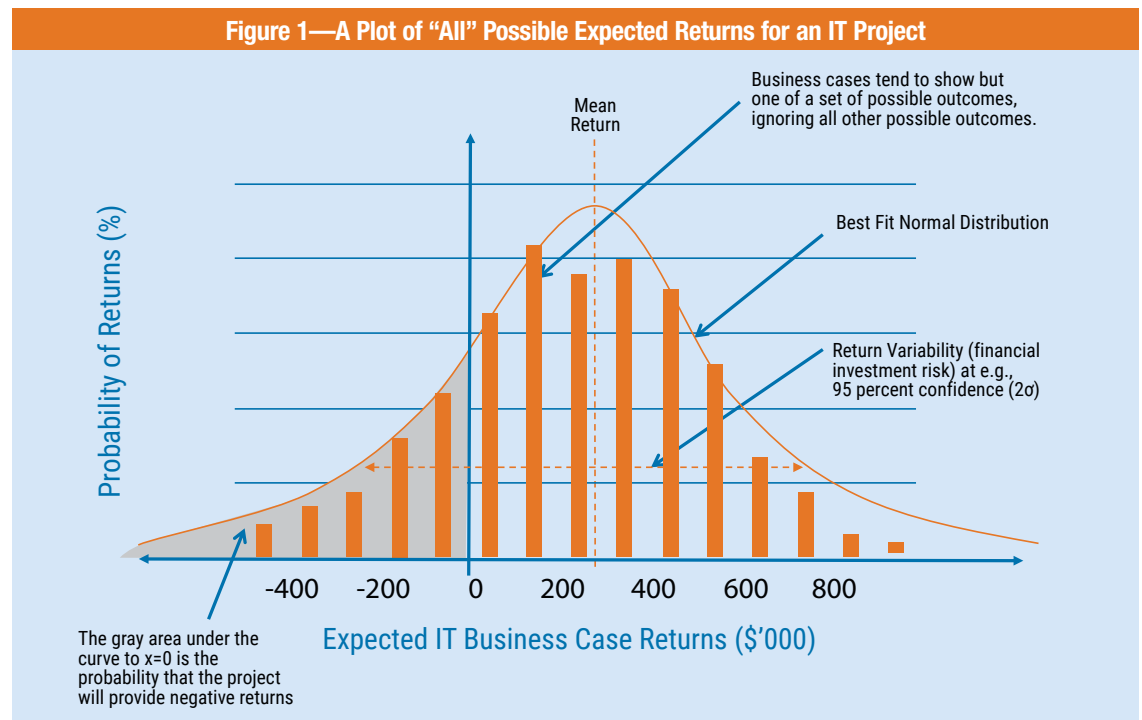
“THIS NEW MODEL, HOWEVER, TAKES THE BUSINESS CASE A STEP FURTHER, BY QUANTIFYING THE FINANCIAL RISKINESS OF THE INVESTMENT TO PROVIDE INTERESTING INSIGHTS INTO THE MAKE-UP OF THE IT PORTFOLIO.”

There Are Business Cases and There Are Business Cases

Good IT governance demands a rigorous business case⁸ and, in both portfolio models, the benefits of the IT investment are actually captured by the business case. Without an approved business case, the governance task of benefits tracking becomes nearly impossible.

This IT Portfolio Management Model, however, takes the business case a step further, by quantifying the financial riskiness of the investment to provide interesting insights into the make-up of the IT portfolio. In general, while business cases may be supported by a qualitative risk assessment, they generally are not supported by an assessment of the financial risk of the investment.

Figure 1 plots all expected returns from an IT project, showing a high probability of negative returns (the shaded area) and considerable variability of those returns (the width of the distribution).



The simplest way to determine investment risk is to use sensitivity analysis, which determines the percentage change in benefits as a result of a 1 percent change in an input variable, such as staffing costs. The impact of all key input variables is determined in this way and their impact on expected benefits is ranked to find the inputs that have the greatest impact on the business case, and for which risk responses may be needed. A downside of sensitivity analysis is that only one variable is considered at a time.

More sophisticated methods of determining investment risk—modeling the variability of all variables simultaneously—involve probabilistic methods, of which the most popular is Monte Carlo simulation.⁹ The technique is noted in the *CGEIT® Review Manual* in the Risk Optimization domain.

Essentially, Monte Carlo simulation substitutes variables in the business case with relevant probability distributions to model uncertainty. In a process involving many thousands of iterations, it selects a set of random values from each distribution for use in the business case, for each iteration, where the outcome of each iteration defines one possible business case outcome. On completion, all the outcomes are plotted in a distribution for analysis, as in **figure 1**.

Monte Carlo methods enable one to say, with a given degree of confidence, that the benefits of an IT investment are likely to fall within a certain range, rather than being expressed as a single value, as would be provided by a traditional business case; the chance of an IT investment returning the exact figure given by a traditional business case is remote, at best.

Plotting the IT Business Cases

In an organization that subscribes to the principles of good IT governance, business cases would exist for the most important IT projects in the portfolio and, in the case illustrated in **figure 1**, the riskiness of the expected returns would be determined too. When plotted, the plot may look similar to **figure 2**.

Based on the risk-reward tradeoff, one would expect an upward sloping trend line with sufficient data points, as indicated in **figure 2**. The closer the IT

investments are to the trend line, the more they perform as expected. The farther the IT investments are from this line (the investments highlighted by a darker plot), the more likely the risk-return profiles could be corrected involuntarily (by the market in the case of area B) or voluntarily (by risk response or a focus on realizing benefits).

The vertical axis plots the expected return from the IT investment, while the horizontal axis plots the riskiness of those returns, measured by the standard deviation of returns divided by the mean return (information from the simulation output in **figure 1**). The organization's IT investment risk appetite is shown, being the acceptable variability of returns.

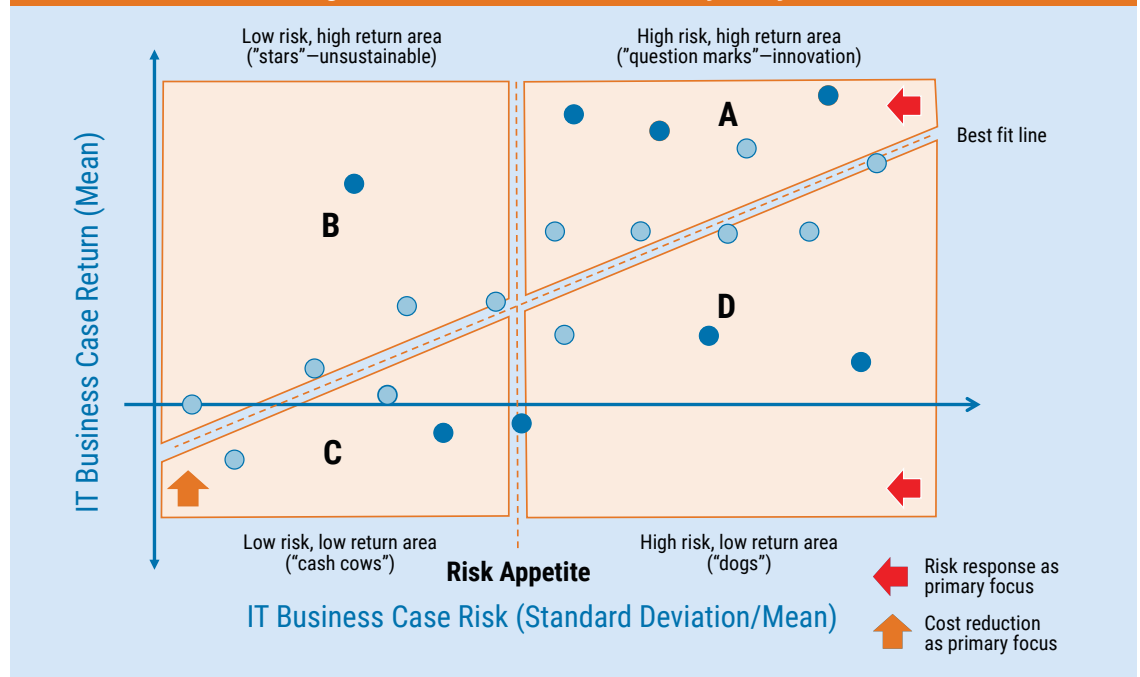
“ESSENTIALLY, MONTE CARLO SIMULATION SUBSTITUTES VARIABLES IN THE BUSINESS CASE WITH RELEVANT PROBABILITY DISTRIBUTIONS TO MODEL UNCERTAINTY.”

Interpreting the Graph

The intersection between the trend line and the risk appetite line conceptually divides the graph in **figure 2** into four areas:

- 1. Area A, Question Marks**—Most investments classified as innovative would be found in this area. Innovative or transformational IT promises high returns, but the riskiness associated with it is seldom articulated, least of all by the technology vendors. The point is that half of these investments will fail,¹⁰ which makes them high-risk with a high probability of failure. The strategic focus should be on risk reduction.
- 2. Area B, Stars**—These are interesting investments because they provide higher returns than they should for the risk they bear. Assuming the assessment of risk and return is valid (e.g., all investment costs are appropriately accounted for, and statements of benefit are supported by an action plan that demonstrably drives the benefits claims), such cases can occur when a

Figure 2—A Plot of a Portfolio of IT Projects by Risk



competitive position is leveraged. The position is, however, not sustainable, because competitors will ultimately find ways to compete in this highly profitable area. A new business intelligence (BI) or customer relations management (CRM) (informational) system in an industry where BI or CRM is unfamiliar could result in this situation.

3. **Area C, Cash Cows**—Since these IT investments provide lesser returns than expected for the risk they bear, are they the dogs of the IT investment

portfolio? Not necessarily; transactional IT and infrastructural IT are the backbone of any business success and they illustrate cases where margins could be low (transactions) or where most of the benefits of an IT investment are difficult, if not impossible, to quantify (infrastructure).

The throughputs in these investments can be considerable, and variability in their performance is low due to considerations such as high-availability IT. Cost management is essential for managing this area, because any incremental reduction in costs increases the returns of those investments.

4. **Area D, Dogs**—This is probably the least desirable area on the graph, as the IT investments here provide low returns but bear high risk. Besides a risk focus, these investments should be reviewed through a strategic alignment lens and a cost-cutting lens.

“INNOVATIVE OR TRANSFORMATIONAL IT PROMISES HIGH RETURNS, BUT THE RISKINESS ASSOCIATED WITH IT IS SELDOM ARTICULATED, LEAST OF ALL BY THE TECHNOLOGY VENDORS.”

Limitations

The IT Portfolio Management Model has limitations; for example, its use demands a certain level of governance of enterprise IT (GEIT) maturity. Some other limitations are:

- Not all IT investments have benefits that are quantifiable. Innovative investments (area A) should be governed by an appropriate business case.
- Calculating investment risk could be complex for some.
- The model is but one abstraction of reality. There are others.
- The estimated risk-return frontier and the risk appetite are different for different companies, realizing that some IT investment business cases would be needed for the organization to make reasonable assessments of both.

It should be noted that the benefits and risk articulated in the business case are based on assumptions that should be qualified. Qualified assumptions provide a perspective of the conditions under which the business case will be a reasonable reflection of reality.

Without qualified assumptions, the benefits-tracking process could be embarrassing for the business case team, especially if the gap between reality and the business case is significant. Without socializing these assumptions, there is little leverage for when the time comes to explain why the technology did not deliver the claimed benefits.

Comparison With ISACA's IT Investment Portfolio Management Paradigm

One part of determining whether the incremental effort required to produce this IT Portfolio Management Model is worth it depends on how mature the GEIT practice is in the business case and benefits realization domains. Both models depend on credible business cases. **Figure 3** summarizes the differences between ISACA's IT investment portfolio management paradigm and the IT Portfolio Management Model.

Figure 3—Summary of the Key Differences Between the Two Approaches

	ISACA IT Investment Portfolio Management Paradigm	IT Portfolio Management Model
Relative time to build the portfolio	Less	More
Relative ease of calculation	Easier	More difficult
Relative data requirements	Less	More
Shows investment returns	Yes	Yes
Shows investment risk	No	Yes
Portfolio mix	Explicit	Implicit (strategic alignment assumption)
Provides investment strategy direction	By means of the mix criterion	By means of areas A, B, C and D in figure 2)
Defined investment risk appetite	Indirectly via the CGEIT risk domain	Yes

In Practice

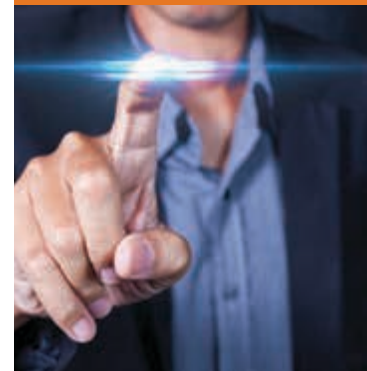
The Office of the Auditor General (OAG) of Canada refers to an artifact called an IT Portfolio Risk Profile, finding that:

(IT) Risk management is critical where high-priority portfolio components depend on each other, where the cost of portfolio component failure is significant, or when risks from one portfolio component raise the risks to another portfolio component.¹¹

The cost of portfolio component failure (rather than of portfolio failure) concerns the implications of an individual IT investment failing to deliver. Since the OAG report also speaks of IT playing "a key part in the Agency's ability to achieve its strategic

Enjoying this article?

- Learn more about, discuss and collaborate on information security management in the Knowledge Center. www.isaca.org/information-security-management



“THE COST OF PORTFOLIO COMPONENT FAILURE (RATHER THAN OF PORTFOLIO FAILURE) CONCERNS THE IMPLICATIONS OF AN INDIVIDUAL IT INVESTMENT FAILING TO DELIVER.”

objectives,”¹² it indicates that strategic alignment is an important construct for the agency and failure of high-priority components will have negative implications for performance.

Conclusion

Financial risk is an important part of portfolio management at the level of individual IT investments. This article proposes a means to increase the visibility of individual IT component financial risk in the interests of mitigating the negative implications of IT failure on strategic performance.

Potentially augmenting ISACA's IT investment portfolio management paradigm, the visualization of financial risk and understanding what kinds of responses are required to increase success of IT in the different areas, as in **figure 2**, are useful in the context of helping to ensure that the strategic objectives of the organization are achieved.

Strategically, determining financial IT investment risk provides invaluable visual insights in the context of IT portfolio management, even though it may take a little more effort to produce.

Endnotes

- 1 As a management consultant for this large IT company at the time, the author developed the model in question. A recent study of ISACA's *CGEIT® Review Manual* gave the author reason to revisit his 15-year-old IT Portfolio Management Model and even to contrast it with ISACA's IT investment portfolio management paradigm.

- 2 Nasdaq, "Risk-Return Tradeoff," definition, www.nasdaq.com/investing/glossary/r/risk-return-trade-off
- 3 Reeves, M.; S. Moose; T. Venema; "BCG Classics Revisited: The Growth Share Matrix," Boston Consulting Group, 4 June 2014, www.bcg.com/publications/2014/growth-share-matrix-bcg-classics-revisited.aspx
- 4 ISACA, *CGEIT® Review Manual*, 7th Edition, USA, 2015, p. 95, https://www.isaca.org/bookstore/Pages/Product-Detail.aspx?Product_code=CGM7ED
- 5 Massachusetts Institute of Technology (MIT) Center for Information Systems Research, IT Portfolio Management, MIT Sloan School of Management, Cambridge, USA, <https://c isr.mit.edu/research/research-overview/classic-topics/it-portfolio-management/>
- 6 Krigsmann, M.; "Study: 68 Percent of IT Projects Fail," *ZDNet*, 14 January 2009, www.zdnet.com/article/study-68-percent-of-it-projects-fail/
- 7 Ezer, J.; "Why Do So Many I.T. Projects Fail?" *Huffpost*, 10 September 2010, https://www.huffingtonpost.com/jonathan-ezer/why-do-so-many-it-project_b_712060.html
- 8 *Op cit* ISACA
- 9 Sharcnet, "1.5 Probabilistic Design Techniques," University of Waterloo, Ontario, Canada, https://www.sharcnet.ca/Software/Ansys/16.2.3/en-us/help/ans_adv/Hlp_G_ADV PDS5.html
- 10 Massachusetts Institute of Technology (MIT) Center for Information Systems Research, Risk-Return Profiles in the IT Portfolio, MIT Sloan School of Management, Cambridge, USA, 2009, https://c isr.mit.edu/files/2009/12/Topic-Portf_Slide4_Ig.PNG
- 11 Office of the Auditor General of Canada, "Report 5—Information Technology Investments—Canada Border Services Agency," 2015, www.oag-bvg.gc.ca/internet/English/parl_oag_201504_05_e_40351.html#p17
- 12 *Ibid.*