Rethinking Risk

A New Ethics of Enterprise IT

Not all that long ago, getting the enterprise to invest in IT required some convincing. According to conventional wisdom, IT was a back-office operation and no more. Today, the power and potential business benefit of IT are accepted facts—indeed, in many industries, IT virtually has the same scope and boundaries of the organization itself, and alignment of IT with business strategy and goals is a key recommendation of IT governance frameworks. Cybersecurity and information security threats increasingly force awareness of IT risk on boards of directors and senior management. Compliance requirements—and associated penalties—bring IT into board rooms and corner offices and necessitate investment in compliance risk management. Governance, security and compliance failures can be critical and deserve attention at the highest organizational levels; however, they do not represent the entire universe of IT risk. ISACA's Risk IT Framework asserts that "Risk IT is not limited to information security. It covers *all* IT-related risk,"[1] including:[2]

- Late project delivery
- Not achieving enough value from IT
- Compliance
- Misalignment
- Obsolete or inflexible IT architecture
- IT service delivery problems

So while cybersecurity failures can be catastrophic and often draw intense scrutiny, especially as they play out in public debates—for example, around elections and foreign influence—they are not the only IT system failures; in fact, the chance of failures unrelated to cybersecurity may be higher. Failure of IT systems can disrupt routines and daily life, e.g., while people shop or bank online, travel, or use social media. The failure of an airline scheduling system or unexpected downtime on a retail shopping website may barely make the local news; however, considering the scope of public dependency on these systems, the possibility of their failure demands more than a typical business impact analysis (BIA) exercise. The routine BIA may give moderately sophisticated organizations sufficient information, awareness, lead time and incentive to prepare and react. However, IT risk management and prevention should go deeper than the average BIA—into the mind-set of organizations, their employees and leaders, both in IT and the business. The scale of potential failure—running the gamut from public inconvenience to catastrophe—argues for the recognition of an ethics of IT as a risk domain in its own right. Ethics of enterprise IT (EEIT) could include organizational culture and individual employee values, all of which profoundly affect IT operations and delivery.

In the context of IT, ethics would address the risk to IT systems due to intentional or unintentional subversion of existing controls and established means, where intentional does not necessarily mean malicious or criminal. Rather, intent would be construed to encompass personal motives, like convenience or expediency in the service of self-promotion; ideals, like an orientation toward service; and collective dynamics, including politics or

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/2YUiipm

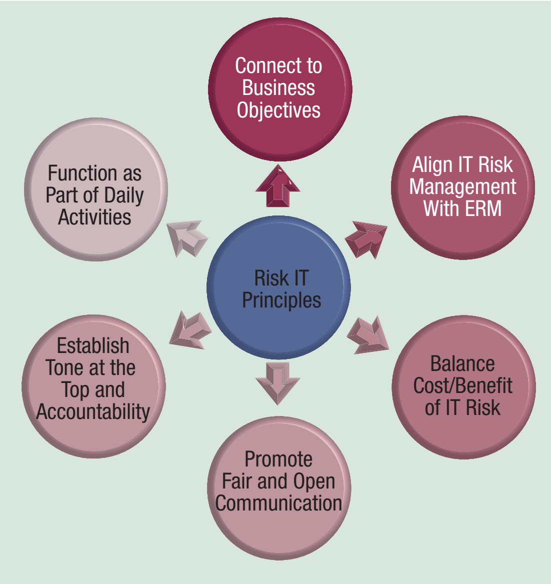
Rajesh Srivastava, CISA, CGEIT, ISO 20000, ITIL Expert, PMP
Is a 35-year veteran of the IT industry, with expertise in—and a passion for—IT process improvement, strategy and architecture, and overall cultural change. He currently leads infrastructure managed services in the United Arab Emirates for a global healthcare IT service provider.

competition, whether between or among whole departments or local teams. Risk IT that accounts for these factors, standards and norms comes closer to an ideal coverage of "all IT-related risk."

Taking Stock of Traditional Risk IT

Most relatively mature IT organizations have some degree of IT governance and risk management—and may have implemented a governance, risk management and compliance (GRC) framework—to mitigate conventionally recognized risk. However, in the current IT ecosystem—often characterized by multiple vendors, implementing diverse solutions, sharing information, or transferring and processing data across national boundaries—not all partners will likely have the same level of maturity when it comes to risk management and may diverge even more with respect to the culture and values. Traditional risk IT may prove insufficient to cover the complexity and variety of the ecosystem (**figure 1**).

Figure 1—Traditional Risk IT Principles


Connect to Business Objectives
Function as Part of Daily Activities
Align IT Risk Management With ERM
Risk IT Principles
Establish Tone at the Top and Accountability
Balance Cost/Benefit of IT Risk
Promote Fair and Open Communication

Even if risk is not managed aggressively, most IT organizations have some level of service management maturity (addressed in Information Technology Infrastructure Library [ITIL] and International Organization for Standardization [ISO]/International Electrotechnical Commission [IEC] ISO/IEC 20000, among other standards).[3, 4] These enterprises generally accept the importance of change management or incident management; however, local adherence to principle usually depends first on the tone of senior management and, second, on the understanding and execution of individuals in IT, all of which can vary across contracting organizations and geographies. Enterprises and vendors alike may cite key performance indicators (KPIs), key risk indicators (KRIs), the balanced scorecard (BSC), management dashboards and so on to illustrate business alignment along with IT service, change, incident and/or risk management. However, the data and controls that inform and mediate these metrics can be sensitive to local dynamics of data capture and reporting—hence their susceptibility to "intentional or unintentional subversion." Principles promoting fair and open communication and accountability at any level (especially at the top) depend upon organizational culture and values in play wherever data for critical indicators are collected, interpreted, packaged and presented, whether internally or to business partners. A whole range of IT behaviors will condition the outcome(s) and call for an ethics of IT, not only to articulate ideals, but also to assess their realization.

Observations from industries as diverse as oil, banking and insurance help to illustrate the point. Despite heavy government oversight and regulation, events like the Enron scandal or the US subprime mortgage crisis leading to the 2008 US stock market crash happened. Similarly, insurance fraud is a reality that large organizations have been fighting for years. Despite a host of traditional controls, governance and formal risk management, IT remains exposed to failures that may be averted by ethical controls.

Traditional risk IT emphasizes the centrality of people, processes and technology.[5] People are influential most constructively in terms of innovation, creativity and spirit and least constructively, or even destructively, in terms of human error or bypassing defined controls and processes (whether accidentally or deliberately). An IT auditor with a view of the ethics of risk IT can look beyond the surface, past the available evidence, and detect the cultural assumptions, values and dynamics, individual motives, and biases or shortcomings working for or against the subversion of controls. Although metrics present a rosy picture, the organization may lack basic awareness of IT ethics and might take a casual attitude toward IT discipline. Intelligence and measures around ethical practices in IT could provide a new dimension of assurance on top of typical risk management.

Organizations such as ISACA® and the Project Management Institute (PMI) have clear guidelines on ethics. Perhaps the whole idea of COBIT®, ITIL or ISO and other frameworks—along with the organizations that maintain and publish them—sufficiently articulate IT ethics. However, there are many sizes and shapes of organizations out there—and many are not mature enough to adopt service management or governance principles. Such an organization can easily purchase a GRC application or help desk tool (and integrate the tools with existing service management processes); but appearances of compliance or assurance could be misleading.

Among relatively mature enterprises, the use of service management processes, controls, automation and sophisticated tools is a good defense against wrongdoing in IT; together, they make bypassing controls and other processes difficult, especially in the absence of deliberate intent. However, like any hacker skilled in finding and eventually exploiting weaknesses, an internal IT resource may subvert controls with criminal intent. Others can bypass established processes—nonetheless intentionally, but without malice, in an effort just to get the work done—without fully realizing the potential impact of control failures. However, as the ethics of IT is more integrated with IT, it improves consciousness and reduces the temptation to bypass established processes and controls.

Ethics of Enterprise IT in Practice

To implement ethics of enterprise IT, one might start by looking within the organization, determining how things actually get done in IT, and acknowledging the reality with honesty and transparency. For the most part, people do not have malicious intent. However, because timelines and delivery targets are often aggressive—and both internal teams and external vendors work in all too human contexts of shifting loyalties, internal competition, career aspirations, tight budgets and so on—corners are cut, and expedient development decisions go unacknowledged or are hidden from view, all of which, in turn, may compromise the broad, long-term goal of IT to support business growth and stability and to monitor and reduce risk.

> “AS THE ETHICS OF IT IS MORE INTEGRATED WITH IT, IT IMPROVES CONSCIOUSNESS AND REDUCES THE TEMPTATION TO BYPASS ESTABLISHED PROCESSES AND CONTROLS.”

Personal agendas, organizational politics, distorted communication, weak vendor management, department silos and sometimes even unrealistic service level agreements/timelines/targets can dilute the overall intention of IT: to serve business users and customers.

The Risk IT principles “Promotes fair and open communication of IT risk” and “Establishes the right tone at the top and while defining and enforcing personal accountability” encompass a range of concrete activities where ethics of IT could set higher standards, track their achievement, report abuses and improve outcomes. The following is a sample list of common and day-to-day IT operations, where any gaps and deficiencies can compromise the overall intent of IT:

- **Metrics and dashboards**—Data are often gathered from multiple sources to assess and report on the health of IT systems for upper management and boards of directors. Tweaking these metrics to put the best foot forward, impress clients or meet service availability targets can be common and may hurt enterprise IT in the long run by obscuring opportunities for process improvement.

  Metrics and dashboards are usually a rollup from several underlying data points and sub-metrics.

While several of them can be automated, others could be subjective and, hence, exposed to misrepresentation. Even with automated data collection, the tie to actual user experience or service availability can be subjective. As an example, infrastructure uptime statistics do not necessarily mean optimal user experience and satisfaction. Therefore, resources responsible for interpreting the metrics and related data must see them from the ethical point of view, i.e., is the end goal being met?

> THE CULT OF THE IT HERO CAN ENCOURAGE COMPETITIVE HOARDING OF KNOWLEDGE VS. AUTHENTIC KNOWLEDGE SHARING AND TEAM LEARNING.

- **Change management**—To get the work done, nudge a project over the finish line a little early or satisfy an important stakeholder, routine changes may be pushed as an emergency, in violation of change management policy. Bypassing or overruling a change advisory board (CAB) or other governance function, senior management or executives may insist on an emergency change to secure a major contract or sale or ingratiate an important customer, regardless of the underlying risk. Unauthorized changes are one of the common underlying causes of IT failures.

Unauthorized changes are, by nature, an ethical issue. Also, unauthorized changes are more than unapproved changes. Change management is also about understanding the "seven R's," i.e., who raised the change, what is the reason for the change, what is the return required from the change, what are the risk factors involved in the change, what resources are required to deliver the change and what is the relationship between this change, and other changes,[6] which can be easily lost among day-to-day IT operational needs.

Considering change is a permanent reality of IT operations, this is the area where awareness and consciousness probably have the most direct impact. Hence, while the change management policies list the types of changes or criteria of a change, it is critical to embed and track the ethical behavior in this area.

- **Incident management**—Responses to IT incidents can be compromised by lack of transparency or failure to complete appropriate root cause analysis in order to protect individuals and/or teams. The goal of incident management is to return the system to its stable state in the shortest possible time and minimize user impact, especially for major incidents. However, for complex IT architecture or fragile legacy environments, a culture of the knight in shining armor or hero often flourishes. One individual knows all the shortcuts taken over time and, thus, becomes virtually indispensable to fix issues or apply the next temporary fix. The cult of the IT hero can encourage competitive hoarding of knowledge vs. authentic knowledge sharing and team learning. This has a direct bearing on the goal as mentioned previously; as an example, incident closure does not eliminate the dependency on individuals or their shortcuts. In an ethics-rich IT environment, these tendencies would be addressed by balance of knowledge and transparency.
- **Vendor management**—Favoritism in awarding contracts—regardless of what is best from an enterprise architecture perspective—can compromise long-term efficiency and quality. IT partners or vendors may oversell irrelevant data and/or solutions to senior management.

It is a normal practice to have best-of-breed technologies or pick technologies that align with the current ecosystem and enterprise architecture. However, pushy vendors offering heavy discounts to get their foot in or senior management bringing preconceived notions from elsewhere can break the ecosystem and impacts IT's ability to support these technologies. A recent ethics investigation at the Georgia Institute of Technology (USA) examined a claim that the university's chief information officer (CIO) had a personal relationship with a vendor's sales representative, resulting in the university paying too much for equipment from the vendor.[7] Unfortunately, many ethical violations go unreported and uninvestigated. Vendor selection should be driven by the vendor's ability to support the organization, the need for its services and meeting business requirements. Anything else could be a violation of IT ethical behavior.

- **Consulting**—Encouraging fluff consulting can sometimes elevate the perceived importance or criticality of teams or departments in the eyes of senior management, especially when consultants do not understand or command the necessary technical experience or detailed history of the enterprise's IT. Additionally, consultants can pad their billable hours and recommend more complex options than what is practical or necessary.

  External parties are expected to bring an unbiased and trusted advisor perspective. However, if not managed well, the aspects of supportability and true need can potentially be compromised with complex, unachievable and long-term goals that may not meet the organizational objectives. Therefore, to meet or exceed the billable hours is an ethical behavior risk that needs to be managed well.

- **Service management**—Enterprise architecture and service management can favor certain tools over others that might be better fit for purpose or more cost-effective. Multiple platforms or duplicative applications may be tolerated or overlooked to please stakeholders in place of a common platform or shared tools that could be more easily maintained and documented.

  Service management plays a vital role when it comes to service quality and management. However, simplicity is key; complex processes may push the tendencies to bypass controls, hence posing potential behavior risk. A common example these days are the security controls that, though absolutely essential, lack agility, which could be seen as a hindrance to getting essential critical work completed and could pose a temptation to bypass the established controls.

- **Continuous improvement**—A culture of isolated, disparate and/or organizationally misaligned teams or individuals can encourage defensive behaviors and resistance to change.

  The terms "lessons learned," "root cause analysis" and "problem management" are talked about generously in most IT organizations, especially at senior management level. However, depending on organizational maturity and local political dynamics, the continuous-improvement mind-set may vary. Considering that continuous improvement is core to service quality (reference: plan-do-check-act [PDCA] model),[8] it needs to be embedded into the organization's IT ethics policy and tracked for mind-set risk and roadblocks.

- **Audit and assurance**—Strong controls may be avoided to increase agility. Conversely, controls may become so inflexible or autocratic in terms of security and change that barely anything gets done. Protection trumps innovation completely, and striking the right balance can require a highly developed judgment that considers business, technical and ethical dimensions at the same time.

  A complex control does not necessarily translate into its effectiveness; it may, in fact, fuel the tendency to bypass it to get the work done, hence a risk to ethical behavior. As mentioned previously, the right balance of control effectiveness with agility and flexibility can have a positive influence on ethical behavior. The previous are some examples, where the existing technical or organizational controls (however widely recognized and well conceived), common best practices, and qualitative measurements may not address the real underlying culture of IT. Organizations and auditors who begin to account for the behavioral aspects of IT can understand—and potentially address—the subtle tendencies for or against subversion of common controls. Hence, an ethics of IT becomes, if not yet a formal discipline, then a soft skill or attitude to foster at all levels, whether among boards of directors, executives, managers, teams or individuals.

Conclusion

An ethical perspective can help the enterprise assess behavioral aspects of IT and the human dynamics of organizational culture. Senior management and their values play an important role, as indicated by the key Risk IT principle "Establishes the right tone at the top and while defining and enforcing personal accountability." In organizations where transparency and accountability seem especially lacking, a trusted third party or unbiased partner should be established in IT. Along with conventional KPIs and KRIs, there should be an ethics indicator—not to police IT, but to ensure that a barometer of IT ethics remains an integral part of risk management. In addition, each IT employee (including senior managers) should receive mandatory IT ethics (part of an organization's risk management framework awareness) training every year, much like security or change management training—in fact, ethics training ideally should supersede and lead into all other training, whether technical, risk, compliance, etc. The goal is to raise awareness and foster an ethical culture, to treat the topic of IT ethics seriously, and establish ethics as a top metric when KPIs related to risk management are measured and reported.

If ethics of IT gains traction over time and garners more attention, comments and developments, perhaps a new type of GRC can become the norm—one that looks beyond standards, best practices and compliance. It would pay attention to the core values engrained into IT strategy and operations and bring ethics to bear not only on IT controls and processes, but also on the behaviors of those who interact with them.

Endnotes

1. ISACA®, *The Risk IT Framework*, USA, 2009, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/The-Risk-IT-Framework.aspx*
2. Fischer, U.; "Risk IT Based on COBIT®," ISACA, *www.isaca.org/Knowledge-Center/Standards/Documents/Risk-IT-Overview.ppt*
3. Axelos, "ITIL—IT Service Management," *https://www.axelos.com/best-practice-solutions/itil*
4. International Organization for Standardization, "ISO/IEC 20000-1:2018," September 2018, *https://www.iso.org/standard/70636.html*
5. ITIL News, "ITIL: Back to Basics (People, Process and Technology)," *https://www.itilnews.com/index.php?pagename=ITIL__Back_to_basics_People_Process_and_Technology*
6. Information Technology Infrastructure Library (ITIL), "ITIL V3 2011: Service Transition. Change Management," 2011
7. Horne, W.; M. Foxman; "Investigative Report: The Georgia Institute of Technology Ethics Line Report USGB-18-08-0018," 15 April 2019, *https://www.news.gatech.edu/sites/default/files/cio-final.pdf*
8. International Organization for Standardization, "ISO/IEC 20000-1:2011," *https://www.iso.org/standard/51986.html*