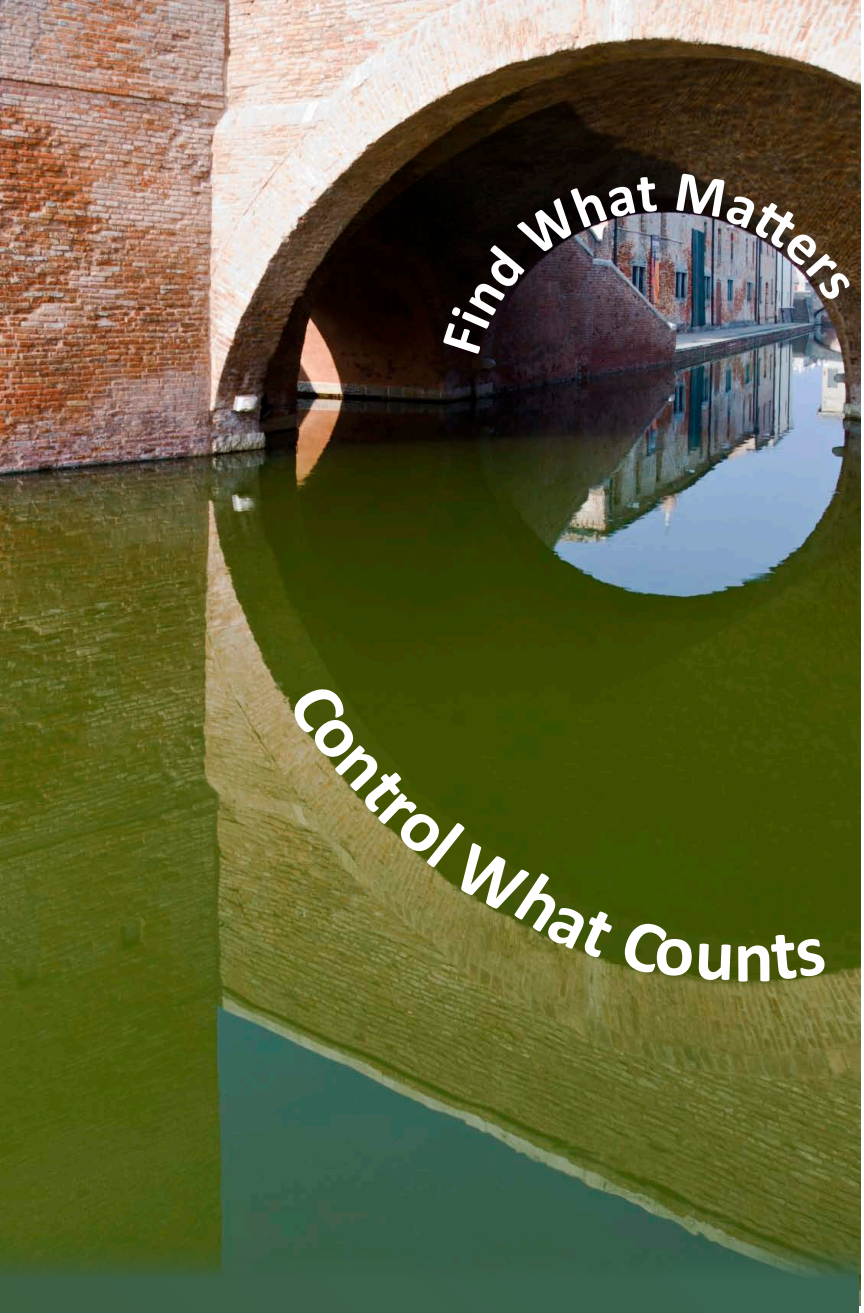


How does a leader create an affordable, sustainable, resilient and dynamic risk management program with the ability to reliably detect threats and morph rapidly to defeat them?

Find What Matters . . .
Control What Counts

IT Risk Management

Developing an information technology risk management (ITRM) program is on the minds of chief executive officers, chief risk officers, IT chief risk officers, and chief information security officers, who are asking: How do I build my ITRM program and office? What are its responsibilities? How do I ensure its effectiveness and success?

An ITRM program is designed to execute, manage, measure, control and report on risk matters within IT. It is essential to an organization's overall risk management capability and effectiveness. If successful, an ITRM program provides the board of directors, senior management, regulators and other external stakeholders with confidence that IT can deliver business value efficiently and securely, while providing high quality assurance around data integrity, availability, and confidentiality.

Developing and managing the program is a multi-faceted task, requiring risk management capabilities, communication and negotiation skills, creativity, organization, time management, change management and education in the form of risk management awareness. The key success factors are similar to those for most strategic enterprise initiatives:

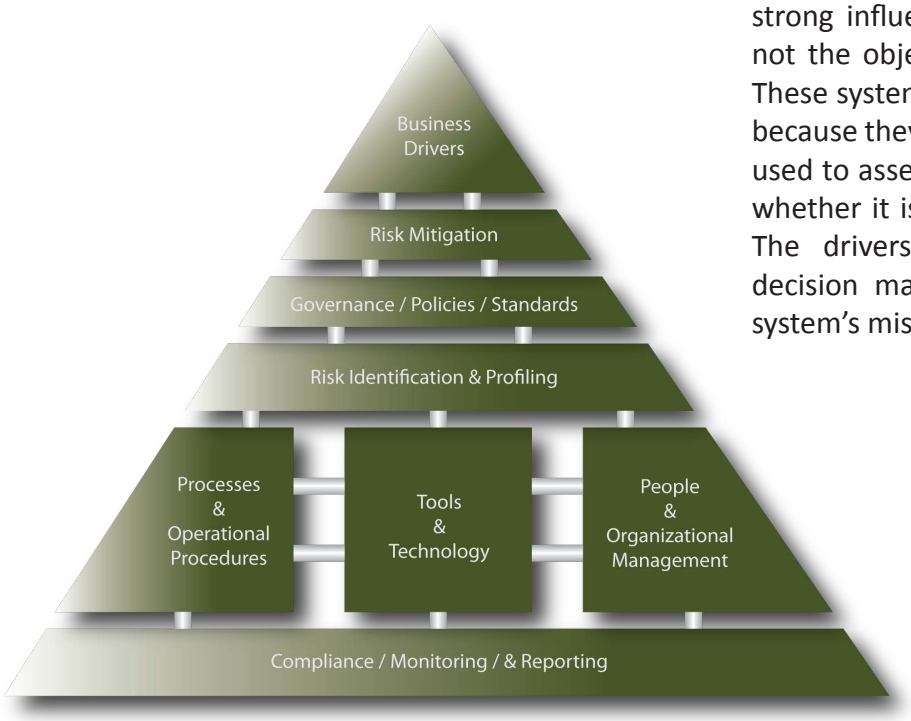
- Tone at the top and management support
- Management accountability and authority to effect change
- Close alignment with the corporate culture
- Consistent and standardized risk management processes
- Measurable results

Bridging the IT Security Gap

Carson

The CISA Review Manual 2006 provides the following definition of risk management: “Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization.” At Carson we understand the challenges of having a perpetual risk process that is adaptable to new threats while being efficiently implemented to respond to the importance of the information being protected. We provide risk management done right.

The Information Technology Risk Management Framework provides a comprehensive outline for establishing a successful program. At Carson, we have been building and tailoring these frameworks for a number of federal agencies in order to optimize implementation efficiencies and maximize results.



Successful implementation of a Framework starts with a mission risk analysis that provides a holistic view of the risk to an interactively complex, socio-technical system. The first step is to establish the objectives that must be achieved. The objectives define the desired outcome, or “picture of success,” for the system. Next, systemic factors that have a strong influence on the outcome (i.e., whether or not the objectives will be achieved) are identified. These systemic factors, called drivers, are important because they define a small set of factors that can be used to assess the system’s performance and gauge whether it is on track to achieve its key objectives. The drivers are then analyzed, which enables decision makers to gauge the overall risk to the system’s mission.

Once the mission risk analysis is completed, the foundation for implementation of all other layers of the Framework exists. While each layer poses certain challenges, with identification of the drivers and an understanding of their impact on objectives, there is a natural flow down to the effectiveness of the other Framework layers.

Building an ITRM program is a challenge. But an appropriately designed program helps align silos and cross-functional areas so that risk objectives are met in a highly coordinated, consistent fashion.

At heart, risk management is the process of making conscious decisions about appropriate levels of residual risk. Successful ITRM programs help better manage IT risk - and give their organizations important advantages in fulfilling their missions successfully. Other positives include: enhanced business value in the form of process, risk and control efficiencies; elimination of redundancies; expense reduction; effective resource management; and legal and regulatory compliance.

For additional information request our Risk Management White Paper or request a consultation with one of our cyber-security experts.

Carson Associates, 4720 Montgomery Lane, Suite 800, Bethesda, MD 20814
info@carsoninc.com 301.841.0094 www.carsoninc.com