SUBJECT

RISK ANALYSIS

SESSION 6 Technological Risk Assessment

RISK ANALYSIS

SESSION 6 Technological Risk Assessment

Technological Risk Assessment

A guide to managing the risk assessment process

Risk management assessments in IT take on many different forms -- from data risk to project risk. Learn more about managing the risk assessment processes in your IT organization.

The goal of a risk assessment process is to minimize the effects of any type of risk -- including data and project risk -- on an organization. IT plays a key role in the risk management process and assessment by using technology initiatives to eliminate any unplanned losses in financial, strategic and operational initiatives.

Our guide, a risk assessment primer for midmarket CIOs, addresses the various types of risks within the IT department and how they can be mitigated. Learn more about how CIOs can addressrisk within disaster recovery, data management and project management, using the tools and resources available here.

Be careful what you wish for. Now that security has the attention of business management and boards of directors, CIOs must learn how to translate aninformation security program into terms the business understands. The first rule of thumb? Focus on results, not details.

Gartner Inc. recommends five tips for linking security to corporate performance:

- Formalize a risk and security program.

- Map key risk indicators to key performance indicators.
- Don't use operational metrics in executive communications.
- Link risk initiatives to corporate goals.
- Communicate to executives what works and what doesn't.
- **Risk management strategy for an information technology solution provider**
  Looking to create an enterprise risk management strategy for an information technology solution provider? Security management expert David Mortman weighs in.

Quantifying and assessing risk

As many midmarket CIOs continue to face budget pressures, some are now slashing a mainstay of the IT budget: vendor maintenance contracts for software and hardware systems.

The economics of cloud computing

Hard-pressed to find more places to cut, CIOs are increasingly inclined to take the risks of going off vendor maintenance, or of moving to a cheaper third-party provider, interviews suggest. This is true even for mission-critical systems and even though it means forfeiting their rights to upgrade.

The surprising punch line? For CIOs who do not plan to upgrade a system soon, or carry more licenses than they now need because of layoffs, the gamble might be just the right thing to do.

- **How to quantify business risk exposure to malware**
  How safe is your enterprise from data-stealing malware? How can you know where your security program falls short? Find out how to gauge enterprise risk exposure to malware.

- **Risky business: How to assess risk during software purchases**
  Get advice from industry expert Andy Hayler on assessing risk during technology purchases. Will the product be retired or acquired? Learn how to spot the signs.

Mitigating risk with information security basics

The National Institute of Standards and Technology (NIST), a nonregulatory federal agency in the U.S. Department of Commerce, is putting final touches on a guide designed to help small businesses and organizations implement the fundamentals of an effective information security program. The NIST standards should also prove useful for the remote offices of larger companies, where IT staffs are often small or nonexistent and it's important that employees bear more responsibility for information security.

Last month, the U.S. Secret Service underscored the cyber danger to small and medium-sized businesses (SMBs), testifying before the Senate Homeland Security and Government Affairs Committee that cybercriminals are increasingly targeting small and medium-sized businesses that do not update their computer security, according to a story by the Associated Press.

Most of the attacks are waged by overseas criminal groups looking to steal sensitive financial and personal information, said Michael Merritt, assistant director of the Secret Service's office of investigation.

- **How to improve data quality on a tight budget -- a guide**
  Many organizations may be tempted to forgo data quality management during a recession, but it is important to assess the ROI for managing data quality, according to an industry expert.
- **How to mitigate operational, compliance risk of outsourcing services**
  Companies must have an approach to evaluating partner risk, the level

of risk of both the service and the provider, and the adequacy of the security practices of the provider.

- **Risk management must include physical-logical security convergence**
  There is a lot to be learned about using VMware Converter, configuring network connections and more when attempting to virtualize a disaster recovery site remotely.

Risk management strategies for disaster recovery, business continuity

His office is on the seventh floor of a building that's nowhere near a floodplain, so Robert Rosen had no particular fear of water damage to his IT equipment. But one weekend, in the office next door, the water filter in an office kitchen cracked, sending a stream of water onto the floor and under the wall into his facilities.

Although critical servers remained dry, the flood ruined equipment that was on the office floor, including 10 surge protectors, six uninterruptible power supplies, six power bricks and one PC. While things were drying out and a length of wallboard was replaced, Rosen implemented a disaster recovery plan that was crafted for an entirely different contingency.

Floods, fires, power failures and pandemic flu can happen. Every IT professional must envision the impact of such disasters on company operations and devise tactics to deal with them. But first, take a step back and start with a comprehensive assessment of all the risks your business faces, of which IT vulnerabilities are an important part.

*Learn more about disaster recovery and risk management in "**Applying risk assessment to your disaster recovery plan**." Also:*

- **Comparing how-to guides for business continuity standards**
  What needs to be done to comply with business continuity standards?

First, perform a risk assessment, then define your business continuity strategy.

Risk management strategies for disaster recovery, business continuity

Using formal risk management tools, companies can more accurately calculate "worst-case scenarios" in IT and the effect their potential loss or corruption will have on the business. So how should you begin your risk management assessment process?

To get you started, we've tracked down some free risk management tools, templates, instructions, calculators and informational guides from across the Web. These free resources offer tools for assessing disaster recovery, risk management and even data loss, including:

- Risk management guidelines and procedures.
- Risk management tools.
- Disaster recovery and risk management assessment

Risk analysis (engineering)

.

Risk analysis is the science of risks and their probability and evaluation.

Probabilistic risk assessment is one analysis strategy usually employed in science and engineering.

Contents

Risk analysis and the risk workshop

Risk analysis should be performed as part of the risk management process for each project. The data of which would be based on risk discussion workshops to identify potential issues and risks ahead of time before these were to pose cost and/ or schedule negative impacts (see the article on Cost contingency for a discussion of the estimation of cost impacts).

The risk workshops should be chaired by a large group ideally between 6 to 10 individuals from the various departmental functions (e.g. project manager, construction manager, site superintendent, and representatives from operations, procurement, [project] controls, etc.) so as to cover every risk element from different perspectives.

The outcome of the risk analysis would be the creation or review of the risk register to identify and quantify risk elements to the project and their potential impact.

Given that risk management is a continuous and iterative process, the risk workshop members would regroup on at regular intervals and project milestones to review the risk register mitigation plans, make changes to it as appropriate and following those changes re-run the risk model. By constantly monitoring risks these can be successfully mitigated resulting in a cost and schedule savings with a positive impact on the project.

Risk analysis and Information security

Main article: IT risk

The risk evaluation of the Information technology environment has been the subject of some methodologies; Information security is a science that based itself on the evaluation and management of security risk, regarding the information used by organization to pursue their business objectives. Standardization bodies like ISO, NIST, The Open Group, Information Security Forum had published different standards in this field. International organizations such ENISA, ISACA had published many papers about it.

Risk analysis (business)

Risk analysis is a technique used to identify and assess factors that may jeopardize the success of a project or achieving a goal.

This technique also helps to define preventive measures to reduce the probability of these factors from occurring and identify countermeasures to successfully deal with these constraints when they develop to avert possible negative effects on the competitiveness of the company.

One of the more popular methods to perform a risk analysis in the computer field is called facilitated risk analysis process (FRAP).

Contents

Facilitated risk analysis process

FRAP analyzes one system, application or segment of business processes at time.

FRAP assumes that additional efforts to develop precisely quantified risks are not cost effective because:

- such estimates are time consuming
- risk documentation becomes too voluminous for practical use
- specific loss estimates are generally not needed to determine if controls are needed.
- without assumptions there is little risk analysis

After identifying and categorizing risks, a team identifies the controls that could mitigate the risk. The decision for what controls are needed lies with the business manager. The team's conclusions as to what risks exists and what controls needed are documented along with a related action plan for control implementation.

Three of the most important risks a software company faces are: unexpected changes in revenue, unexpected changes in costs from those budgeted and the amount of specialization of the software planned. Risks that affect revenues can be: unanticipated competition, privacy, intellectual property right problems, and unit sales that are less than forecast. Unexpected development costs also create risk that can be in the form of more rework than anticipated, security holes, and privacy invasions. [1]

Narrow specialization of software with a large amount of research and development expenditures can lead to both business and technological risks since specialization does not necessarily lead to lower unit costs of software.[2] Combined with the decrease in the potential customer base, specialization risk can be significant for a software firm. After probabilities of scenarios have been calculated with risk analysis, the process of risk management can be applied to help manage the risk.

Methods like applied information economics add to and improve on risk analysis methods by introducing procedures to adjust subjective probabilities, compute

the value of additional information and to use the results in part of a larger portfolio management problem.