

IMPORTANCE OF RISK DEFINITION FOR IT RISK CONTROL

M.A. Goman

Control of technological and security risks remains an actual problem in business. Problems in risk management include identification of the object of analysis, methods of analysis, incompleteness of information and lack of resources. Therefore, the methods should facilitate risk prioritization issue.

Concept of risk is not uniformly understood in practice and research. Available control frameworks understand the term “risk” differently. Principles of system approach were used to evaluate concepts of risk that we had found in literature. This made it possible to incorporate technological risk management as a subsystem into a wider system of business risk management. IT risk control is meaningful only as a part of overall business risk management. We revealed that the concept of risk is always related to a person (a decision-maker) or group of people who are interested in certain successful solution of their problem. The two key criteria of risk existence are “exposure” and “uncertainty”. Ability to recognize existence of risk saves resources. A strong risk concept enables justification of cases where quantitative analysis is a must. Evidently, the term “risk” means a bad event (outcome), not a positive one as some sources agree. Risk metrics should reduce uncertainty and refine probabilities and impacts of events that affect outcomes of the decomposed problem.

IT or security risks exist only in a certain environment and make sense there for a set of human actors during some time interval. Risks are also connected to a problem with at least two alternative solutions, including possible negative outcomes. Risk can only emerge if there is a possibility that the problem will not be solved adequately according to perception of the decision-maker. If we fail to formulate what risk in our context is, the problem can not be addressed effectively.

We propose a new look at the problem of risk control. First, define IT risk for a given situation. Then, identify an owner of the risk, his problem and decision. Risk control should support the risk owner in his decision. Then, determine metrics that show that the level of risk is changing. Such methods and criteria should be found that one could efficiently apply available resources to risk analysis, prioritize risk treatment actions and finally verify the effect of the actions.

To sum up, risk is connected to a business situation and is a multidimensional entity. Standards need update in order to reflect the nature of risk and suggest methods accordingly. This work is the basis for the further work on IT risk analysis methods for business control models.

IMPLEMENTATION OF THE VULNERABILITY MANAGEMENT PROGRAM USING PROJECT APPROACH

S. Joe-Madu, A.M. Prudnik

A vulnerability is defined in the standard as “A weakness of an asset or group of assets that can be exploited by one or more threats” [1]. IT security regulations increasingly are the norm demonstrating a standard of care in protecting sensitive data. To serve this standard, several regulatory bodies have mandated the creation of vulnerability management programs. Examples include: the Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), and Federal Energy Regulation Committee (FERC)

Vulnerability management is comprised of the following activities [3]: identifying / tracking assets (build asset inventory); categorizing assets into groups; scanning assets for known vulnerabilities; ranking risks; patch management; test patches; apply patches; follow-up remediation scan – confirms vulnerability addressed.

The planning phase of the vulnerability management program involves gathering company and regulatory vulnerability assessment requirements, detecting vulnerabilities, and rating and ranking their risk.

The doing phase of the vulnerability management program requires to implement the risk treatment plan. Risks are mitigated to the company’s acceptable levels. The plan may include patching systems to acceptable levels, decommissioning systems (removing them from the environment), or applying compensating controls.

The checking phase of the vulnerability management program requires to monitor systems regularly to ensure vulnerability compliance requirements are met. Companies may choose to run the