Enduring relevance is a category of research and commentary which was published more than 10 years ago, yet its ideas, arguments and facts are as relevant today as they were then.

Enduring Relevance

Understanding risk from ITIL perspective

The IT Infrastructure Library (ITIL) and its fundamental concern for quality IT service delivery and management provides a completely fresh way of identifying the full range of risks that organizations face in conceiving, funding, executing, and operating IT services that support business objectives. ITIL strategic and tactical objectives are as clear as the desert sky.

Because of this clarity, managers should find it easier to document the potential risks in failing to fulfill ITIL's prescriptions. And identification is the necessary first step to mitigation of those risks. Businesses looking to boost their cybersecurity management can use a simple mini-methodology based on ITIL mandates for the consistent, systematic identification of risks at every stage of the IT service lifecycle within the entire organization.

ITIL is anchored to a service orientation of quality. Some IT risks have business consequences that the IT organization will have a deepened appreciation for in a service-oriented context because (1) the service mandate confronts a much wider range of issues than merely technology; and (2) the IT organization is reminded of its accountability in these service contracts. For example, failure to meet a service goal of four nines application uptime (99.99% availability) means that an application, in general, is down more than a few hours a month. In particular, it might mean that payroll is not completed on time or that a supply chain disruption occurs because of a delay in raw materials procurement.

For anyone who has implemented ITIL as an IT management methodology, many of the risks documented in the report are well known in the literature. Managers schooled in ITIL are well aware that ITIL is not explicitly a risk analysis tool. In fact, although the subject of risk management as an explicit management discipline in ITIL, like demand management or applications management, is not mentioned until you reach the process guidance of availability management within the Service Design phase/volume, the concept of risk has its hands all over ITIL v3. Simply by virtue of understanding the intent behind both the

strategic approach to each phase/volume of the services lifecycle (e.g., Service Design and Service Operations) and the specific objectives of the process guidance within each of those phases (e.g., applications management and configuration management), the range of risks becomes clearer.

Clearly understood intent and objectives of the ITIL methodology cause risks to pop out at you, because unambiguous goals provide a better understanding of the tasks required to fulfill those objectives. And when tasks are clear, the risks in failing to carry them out are also clear.

Many of the risks made apparent from the business logic of ITIL are rooted in a failure to adequately fulfill some process requirement in a particular management domain. ITIL is chock full of process guidance and mandates for every corner of IT management. This idea of objectives, tasks, and how risks emerge will be obvious to anyone who has drilled down deeply into ITIL.