The wrong end of the stick: rules vs. principles

LinkedIn, 30-09-2014

ICT regulators and controllers tend to follow a rule-based approach. Although – if asked – they soon enough admit that they actually don’t believe it is the right approach. They would love to see their target audience being so well organized that they can stand up to any test. They know that a rule-based approach starts at the wrong end of the stick. But still – they always start at that end. Makes you wonder why....

Healthcare

Healthcare institutions are increasingly facing tough demands in the field of information security. In practice this is often expressed in terms of ISO27001 controls. Dutch healthcare regulators use a local standard, NEN7510, which is almost identical to ISO27001. In 2010, the regulators decreed that all healthcare institutions had to meet a subset of 33 controls, out of the full set of 125 controls in NEN7510. This NEN standard was recently updated to follow ISO27001:2013, but the set of controls used for healthcare institutions is still largely the same.

In their audits, the regulators didn’t demand hard scores, instead they emphasized that the organization should rather be able to show that they were systematically working towards a better score on the selected controls. In fact, the regulators stimulated the institutions to improve their quality in a methodical way, so that they would improve their assessment score in the next audit. In practice however, they are still auditing against the same set of controls. This approach is now stimulated even further, because the full set of NEN7510 requirements was recently promoted to law for any healthcare organization using the unique citizen registration number in their systems.

Finance

This approach is very similar to what is currently happening in the financial world: in the Netherlands, that sector is also sampled by means of a (self) assessment. The supervisor in this case is the Dutch national bank (De Nederlandsche Bank, DNB), and the controls they use are derived from COBIT, enriched with guidance from ISO27002. But the situation is essentially the same: a control-based approach (*rule-based*) does not lead to the desired result. Instead, banks, pension funds and insurance companies should turn to a quality management approach that produces the desired information security assurance inside-out.

In the mean time, healthcare institutions have learned to achieve at least maturity level 3 (CMMI), with a methodical approach based on the ISM Method, within a year, and level 4 is within reach shortly after. Not by following a rule-based approach, but by means of gradual improvement. "*Old wine in new bottles, PDCA, been there, done that....*". The standard response. But when you look at the daily practice of our most elusive experts, with all the certificates you can think of on their wall, they always start on the rules end of the stick, using *best practice* guidance from sources like ITIL, COBIT, ASL, BiSL, and other frameworks. Hey, and why not? Nobody ever got fired for hiring an ITIL consultant, or a COBIT consultant, or ....

Dot on the horizon

The essence is that the road to information security is not walked by trying to start at the controls end of the stick – whether there are 33 or 125, they still represent tricks. And the real trick is that you should turn it around: if you manage to teach the organization an integrated and systematic way of managing their work, you are leading them to a dot on the horizon.

"If you want to build a ship, don't drum up people to collect wood and don't assign them tasks and work, but rather teach them to long for the endless immensity of the sea."

This is 'ancient wisdom', words spoken by Antoine de Saint Exupéry. Each seriously educated expert must have heard that line before. Nevertheless, consultants are taught to apply *best practices* to their clients, and they honestly believe it's the best they can do for them. But *best practices* are the **result** of (hopefully) a systematical approach that can (hopefully) be replicated in the environment of their clients. And you cannot *start with results* when improving the structure of an organization: *you cannot start at the wrong end of the stick*. They should focus on finding the approach that *delivered* these practices, and then replicating these practices by *using* that approach – or at least by teaching the organization to work with the approach.

Dots on the horizon will be changing all the time, but walking the road to the horizon will largely stay the same.

The method

The method Dutch organizations have learned to use is the ESM Method – Enterprise Service Management, developed in 2005. ESM is a method to get in control of any type of service organization, or any combination of service sections in an organization. The information management domain has proven to be a very grateful domain for ESM, because organizations had to gain ultimate control over their IT services, as a result of the ever growing dependency on IT. The IT specific application of the generic ESM Method was called the ISM Method: Integrated Service Management. In practice, ESM was applied to various other service domains, including the "business information management" domain (where it is labeled FSM - Functional Service Management), and to combinations of IT and other service sections (e.g. medical technology, education), where the term ISM or ESM was used.

In IT organizations, the ISM Method focuses on the management system (the engine), and on the turnaround the management and staff need to make to adopt a systematic approach to their work. In a standard ISM introduction project it takes 13 weeks to get all (existing) instruments in place in a fully standardized project, and then 6-9 months are spent teaching the organization to apply the method and to get used to a systematic step-by-step improvement approach. External consultants can coach the organization through this project, but a do-it-yourself approach is also often used, based on the book The ISM Method.

The results of the ISM Method are attracting lots of attention: organizations can achieve improvement goals (like ISO27001 or COBIT controls) in shorter times and at lower cost then before – and the results are lasting. Tool providers, consulting organizations, game developers, and trainers in the Netherlands are now adopting the method to create a new market; one with a much better cost/benefit ratio for their customers.

The big turnaround

The major advantage of starting at the other end of the stick is that you invest in an efficient and effective systematic approach, that can be applied again and again in a cyclic improvement strategy – as Shewhart and Deming taught us half a century ago. The new IT world is full of that approach, but only as long as it concerns technology: SCRUM, LEAN, DEVOPS.... It’s about time the management consultants join the bandwagon and pick up what Eliyahu Goldratt wrote down on the Theory of Constraints.

And following a rule-based approach is not what Goldratt, Deming and Shewhart meant.

In the Netherlands, the first finance organizations now work on their management system from a systematic inside-out approach, starting at the other end of the stick – even though their regulators confront them with rules to be followed and controls to be achieved - preferably by the letter, if you believe your auditor. Within a year they grow 2 levels on a 5-level maturity scale. Their road is the same, even though their dot on the horizon will differ.

Banks, insurance companies, pension funds, hospitals, nursing homes, care clinics, most of them still need to make the big turnaround to a systematically assured quality management. Luckily, they all aim for the same (improvement) and they all can use the same trail to their dot on the horizon following a standardized methodical approach that saves time, money, and worries. But the biggest advantage lies in the simplicity that it buys you. If your 'inside' is put together well enough, it doesn’t matter much what stick they use to measure you.

Jan van Bon

Inform-IT, Knowledge Center for Service Management