Real-life Risk Theory

Mette Brottmann is a senior risk analyst and controller in a bank.

Klaus Agnoletti is a senior security specialist at an outsourcing vendor.

Morten Als Pedersen is responsible for IT security at a university.

Ronnie Lykke Madsen is chief information security officer at an audit company.

Michael Rosendal Krumbak is an IT security specialist at a pharmaceuticals company.

Thor Ahrends, CISA, CISM, CRISC, is an IT security consultant, IT auditor and senior manager at an audit company. He has worked as an IT security consultant and IT auditor at several recognised companies.

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article and choose the Comments tab to share your thoughts.

Go directly to the article:

Most IT professionals know the theory and importance of addressing and mitigating risk. Daily resource limitations and task prioritisation, however, do not always allow for best practice approaches to be taken.

ERFA (erfaringsudveksling) is a Danish concept that means "knowledge sharing." A group of Danish security experts meets four times annually to discuss new threats, technologies and issues experienced. The group members include IT security experts working in, for example, big and medium-sized banks, consulting firms, manufacturing companies and universities. All discussions are treated confidentially. The authors of this article are some of the members of this group. The participants have discussed day-to-day issues and lessons learned have been collected in this article.

The basic idea behind the approach outlined herein is to define some basic tasks that can be used as eye-openers to drive the business case for further risk work. This article outlines real-life approaches to risk work used by members of the ISACA® Denmark Chapter's RiskERFA group (the group).

Working with risk is needed to balance IT security controls. How is it possible to determine the protection level of IT assets if these are not categorised and associated with a financial value? Risk-based controls are growing in importance, and no one can disagree that the business side must be involved and stakeholders must commit.

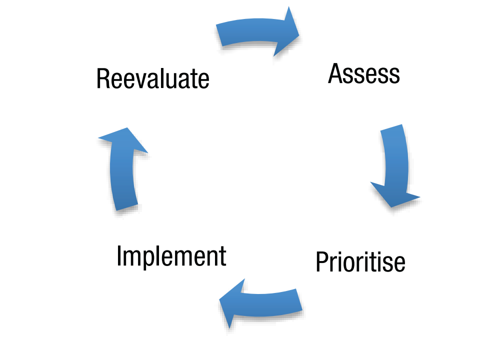
During discussions, the group realised that the COBIT® 4.1 Capability Maturity Model level 5 sometimes is out of reach in daily tasks and procedures. Complex procedures and strict requirements for documentation may collide with requirements for lean business operation.

Topics of discussion that contributed to this realisation included:

- At a large, 40-year-old Danish company with a tradition of *ad hoc* procedures, limited documentation and an unstructured risk management process made it difficult for the IT department to identify critical processes. Instead, the IT security department, supported by IT operations personnel, identified the 21 most important IT services that are now the basis for developing general information security management system (ISMS) processes.
- Using different cases, the group also discussed how the risk of IT projects can be assessed informally simply by asking the project owners, 'What is the worst thing that could happen with this new service'? Through these discussions, the risk is clarified on a common basis and risk/impact may informally be classified.
- Risk regarding personal data and privacy are always on the agenda. The coming European Union Data Protection Regulation will only emphasize privacy risk. To quantify not only direct risk, but also indirect risk (e.g., reputational risk), it might be relevant to reach out to departments (e.g., communications, human resources).

Rather than aiming only at a high maturity level, it is possible to significantly improve the basis for decision making by performing some simple initial steps. This also stimulates the process of increasing the maturity level by asking relevant questions to the relevant actors participating in the risk work, thereby raising awareness and attracting management support for implementing a more formalised ISMS.[1] The process is a continual improvement circle, as illustrated in **figure 1**.

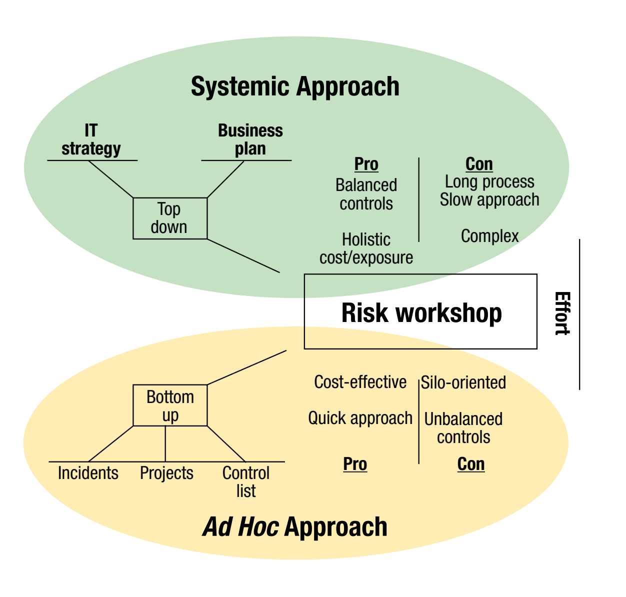
Figure 1—ISO Plan-do-check-act Approach



Source: The Danish RiskERFA (Brottmann, Agnoletti, Pedersen, Madsen, Krumbak and Ahrends). Reprinted with permission.

Figure 2 was agreed upon by all group members. The risk approach can be top down or bottom up. Sometimes both approaches are used at the same time within the company. Different projects and organisational units may benefit from using different approaches. This is also a way of risk orienting the risk approach. The work is best organised in a structured risk workshop with participation from both the line of business and IT security professionals.

Figure 2—Risk Workshop Model



Source: The Danish RiskERFA (Brottmann, Agnoletti, Pedersen, Madsen, Krumbak and Ahrends). Reprinted with permission.

Determining the methodology to use should be a conscious decision based on the following points:

- Business requirements, legislative compliance and contractual requirements
- Urgency of timely clarification
- Complexity of the area in question
- Internal process flow complexity and conflicting interests
- System implementation and technology legacy

Some industries (e.g., pharmaceuticals, banking) have strict compliance requirements covering risk mitigation and risk reporting. Compliance requires a formalised approach, but the bottom-up method can also be used in these cases as long as the outcome is communicated in a formalised risk report, issues are identified and continuous improvements are initiated if needed.

Any risk activity must be anchored with a business owner (system or project owner). Anchoring should be determined by who will suffer the most if something breaks (both in the short and medium term).

Alignment with business policies and strategic initiatives must be ensured by the IT facilitator as part of the risk workshop.

The bottom-up approach for specific projects and/or compliance-driven adjustments is most often the reality. Anchoring is, therefore, essential; otherwise, the initiatives lose value. The bottom-up approach requires coordinating multiple diverse risk activities.

In contrast, the top-down approach requires a complete overview of assets, which is hard to establish in a large organisation. Complex challenges must be addressed, and a top-down approach requires some form of formalised role managing of the risk work. The outcome is highly dependent on the required organisational muscles and implemented governance framework. There is no right or wrong approach. The proper approach is most often a combination of the two approaches.

The following pragmatic suggestions are based on actual findings within the group:

- **Workshop**—Input must be gathered from both subject matter experts (SMEs) and groups with more generic knowledge (line of business). Only by combining the two can the decision makers acquire the necessary information. From a risk-view maturity level, three out of five is, in many cases, sufficient (using the COBIT® Capability Maturity Model scale).
- **Simplification**—A fast-track approach could be to ask business areas to identify the top-five pain points/risk factors for each business area and start the risk work within this scope. This may be done by interviewing the individual responsible for the relevant business areas. Another way of rating could be to prioritise high-revenue areas or high-damage areas.
- **Mapping**—The IT facilitator then needs to identify the infrastructure/systems required to support the areas identified by business.
- **Scoring**—The focus should be on simple and tangible deliveries, with simple scoring on a scale of one to five. Use a simple chart illustration to show deviations from the defined baseline.

- **Enforcement**—Recommendations or requirements are not effective without necessary anchoring. The risk owner must have both the power to make decisions and resources to enforce implementation processes, projects and systems.
- **Learnings**—Actual incidents should be evaluated, the realised cost should be compared to the expected cost and the model should gradually be improved. The outcome of this work will be a prioritised improvement list and potentially a business case with embedded cost calculations.
- **Continuous**—With constant measuring, mitigation and response, the risk assessment can accommodate changes in use and threat exposure. This result can be trusted as a decision tool. The assessment should be followed by implementation of prioritised risk controls.

Currently the method described is being further developed in real-world cases among the members of the RiskERFA. Future lessons learned will be shared in a subsequent article.

AUTHOR'S NOTE

The article is a product of contributions from all RiskERFA group members, including, but not limited to those listed on authors of this article.

ENDNOTES

[1] International Organizations for Standardization, ISO 27001, *www.iso.org/iso/home/standards/management-standards/iso27001.htm,* or ISO 27002, *www.iso.org/iso/catalogue_detail?csnumber=54533*