bakertilly
SWITZERLAND

IT Health Check – identifying IT risks and taking advantage of the resulting opportunities

A stable, robust IT environment combined with an awareness of cyber risks and of limited IT resources enable management to provide reliable information and to succeed as an SME on the market. This article explains how an objective, external view can help management to protect itself against IT risks.

Philipp Schweizer
Senior Manager/
IT-Prüfer
Member of the
Management
Zurich

SMEs and their owners, CIOs, Heads of IT and other IT managers are confronted with many challenges in today's working environment. IT security and limited IT resources (IT budgets) are high on the agenda alongside digital transformation and growing complexity. What is more, the business risk is heightened by the recent increase in cyberattacks. In this context, it is important to be familiar with IT risks and to ensure that the core processes in day-to-day business are adapted accordingly.

Identifying IT risks
The need to harmonise the IT architecture and to digitise processes at the same time requires agility and a stable control environment. Often, many fundamental risks are not or not fully taken into account. An objective, external IT risk assessment, e.g. as part of an IT Health Check, can be useful and provide a fresh look at a company's internal projects and challenges. In principle, it is possible to identify three main levels with a number of further focus topics (see IT strategy and vision).

■ **Management and control**
Experience has shown that it is difficult for SMEs to precisely define responsibilities in the area of IT. This is often due to scarce human resources. Particularly when changing ERP systems, it is important to ensure

successful data migration. In many cases, fundamental questions are not adequately addressed in the course of this type of project. As well as ensuring complete and correct data migration, it is vital to involve specialist departments in good time, not to lose sight of project organisation and control bodies, preliminary data cleansing, error handling and acceptance, and to manage these aspects proactively. The following questions should be answered:
- Is the IT organisation in a position to provide adequate support for essential core processes and IT projects?
- Are projects completed on time, within the defined budget and to the desired quality standard?
- Is the IT strategy in line with the corporate strategy?

■ **IT operations / IT processes**
Within the framework of IT operations, it is necessary to define and

monitor aspects including access protection, segregation of duties, the authorisation concept and change management.
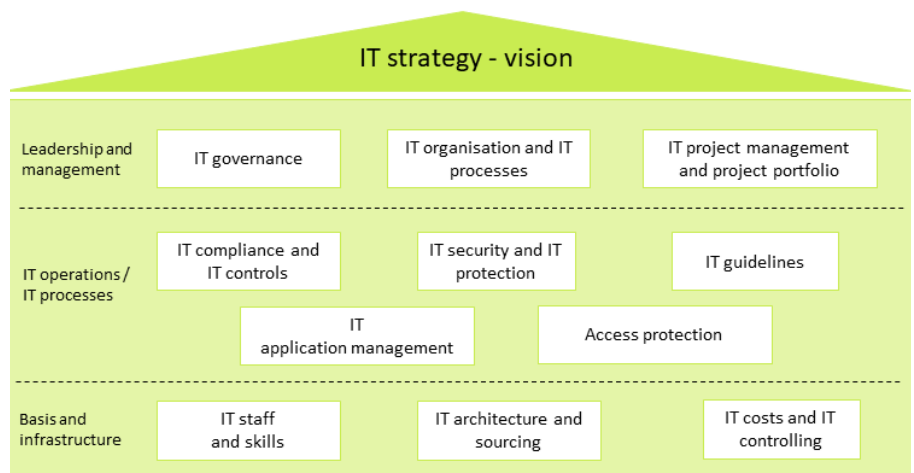■ Questions arise such as:
- Are all changes and accesses adequately defined, approved and controlled?
- Is there a general awareness of cyber risks and are such risks reviewed?
- Are employees made aware of the relevant issues and trained accordingly?

■ **Basis and infrastructure**
CIOs or Heads of IT are basically responsible for the company's day-to-day infrastructure, its performance and costs. The main issues to be addressed include:
- Do you use in- or outsourcing of data centres and services?
- Are all applications up to date and is performance sufficiently guaranteed?

IT strategy - vision			
Leadership and management	IT governance	IT organisation and IT processes	IT project management and project portfolio
IT operations / IT processes	IT compliance and IT controls	IT security and IT protection	IT guidelines
	IT application management	Access protection	
Basis and infrastructure	IT staff and skills	IT architecture and sourcing	IT costs and IT controlling

- Are my employees adequately trained and do they have the right skills?

(See IT strategy and vision)

OBT would be happy to draw up an initial assessment of your IT environment and, as part of an IT Health Check, provide you with pragmatic, solution-oriented recommendations on how to improve your IT processes and reduce IT risks by making just a few effective changes. We adopt a collaborative approach and hold discussions with you to explore good/best-practice solutions in a targeted manner based on our experience in optimising business and IT processes, as well as reducing IT risks.

Our transparent process begins with an initial interview and a self-assessment. During this stage, we survey the current conditions of the general IT environment in order to evaluate the three main levels.

Anomalies are openly discussed in order to examine and investigate them in more detail.

Assessment of core IT processes

A more in-depth IT audit to take stock of the situation helps many companies to identify their potential for improvement and to pinpoint any "blind spots". This audit can be based on an IT Health Check. The assessment of the IT environment offers several advantages.

Gaps with regard to access authorisations, change management, program development and IT operations can be detected and improved with relatively little effort thanks to surveys and spot checks after identifying the responsible parties together. In addition, anomalies can be objectively measured according to a maturity model and analysed in relation to companies of a similar size from a comparable sector.

CONCLUSION

The world is undergoing constant change. Given the challenges associated with digitalisation and questions related to IT security, there is always potential for improvement in order to counter IT risks in a timely and expedient manner. That is where an IT Health Check, an in-depth IT audit or a project-related audit can come in useful, e.g. when migrating data or evaluating the IT ICS maturity level. OBT offers various products to assist you, and will be happy to guide you through the process with pragmatic, straightforward solutions.

Level 5 – Optimised
Enhancement of the company's compliance management system, continuous development and

Level 4 – Controlled and monitored
Effective (measurable and implemented) IT processes; integrated strategy

Level 3 – Defined and established
Appropriately documented and applied IT processes for all process areas

Level 2 – Repeatable
Uniform basis for IT processes available; subject to severe fluctuations

Level 1 – Initial
Individual IT processes defined, depending on the commitment of individuals

Level 0 – Not available
Unsystematic; no common rules/framework conditions