e|HealthCheck®

We x-ray your IT systems ...

b·prex
Business Process Excellence

bprex group ag
Stampfenbachstrasse 40 | 8006 Zurich | Tel +41 44 444 11 04 | Fax +41 44 444 11 02 | contact@bprex.ch
www.bprex.ch

... and provide you with assurance: efficient, competent, beneficial, and all from a single source.

The more a company depends on its computer systems and the higher the risk is that errors in the business processes can have their cause within the structure and handling of IT systems, the more important controls within IT will be.

What is the eHealthCheck?

Requirements from legislators, regulators and stakeholders on company management have increased dramatically over the recent years, partially due to amendments of the Swiss Law of Obligations (OR) relating to internal control systems (ICS) and the recent updating of the Data Protection Act. Furthermore, companies are under enormous cost pressure.

Do you know the risks of your company‘s computer systems?

- Have all the stipulated necessary security measures been implemented?
- Have all the statutory requirements with respect to data protection and information security been adequately addressed?
- Are the IT-internal processes robust enough to ensure that the impact of any negative incident (e.g. failure of critical business applications) remain at a manageable level?
- Does your IT adequately support the achievement of your business goals?
- Last but not least, do you know what costs IT will accumulate, both now and in the future?

If you did answer „no“ or „I don‘t know“ to one or more of the above questions, you will probably require an independent assessment of your IT that takes info consideration the specific characteristics and requirements of your industry. This kind of assessment will give you concrete information as to whether there is a need for improvement, or whether you are on the right track with your own efforts.

To highlight potentials for improvement or any weaknesses within IT in regard to operational and management processes – in comparison to applicable regulations and etablished best practices – we provide the eHealthCheck. An eHealthCheck is best described as a health check-up of your IT.

The eHealthCheck has been developed based on internationally recognised standards such as CobiT and ISO 27002, current legislation (e.g. the Data Protection Act, Patients‘ Law) and on countless years of practical experience in IT security and IT governance covering a wide range of customer projects.

Structure of the eHealthCheck

The eHealthCheck can be flexibly adjusted to any company and allows a structured evaluation of the entire IT environment. Special attention is given to the aspects of data protection and information security, as well as IT governance (management of the computer system). All IT-related areas are examined.

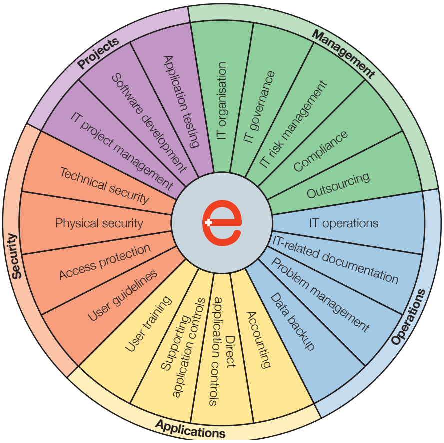


Figure 1: IT-related areas

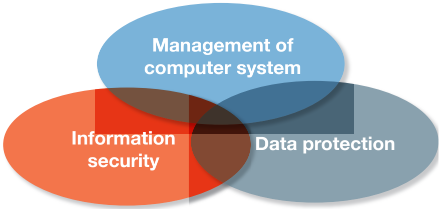


Figure 2: The three independent related issues for IT security

Data protection concerns the individual, the person, the customer, the employee, the patient - i.e. the stakeholders of a company, while information security essentially refers to the integrity of the information and its physical and logical security and availability. Although the two disciplines are closely interlinked, they have a distinct relevance and are weighted differently for different industries.

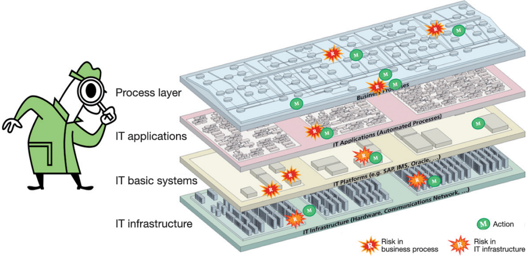

Process layer
IT applications
IT basic systems
IT infrastructure
Business Processes
IT Applications (Automated Processes)
IT Platforms (e.g. SAP, IMS, Oracle, ...)
IT Infrastructure (Hardware, Communications Network, ...)
R
M
M Action
R Risk in business process
R Risk in IT infrastructure

Figure 3: The four-layer model

The eHealthCheck examines each of the layers, which all represent a form of processes and resources:

- The top (blue) layer represents all the important (manual) business processes – normally broken down according to the responsible departments and into sub-processes and individual activities.
- The second (red) layer represents the automated parts of the business processes, the actual (IT) applications. With the exception of really small businesses, most companies process virtually all transactions using applications of this kind.
- The third (yellow) layer represents the basic IT system. This incorporates a wide range of possible platforms on which the second layer applications are running.

Examples include database management systems (e.g. SQL, Oracle), the basic components for integrated applications (e.g. SAP Basis) or more technical processing systems (e.g. Middleware).

- The bottom (green) layer represents the IT infrastructure. Essentially, this means the actual hardware (e.g. servers) and the associated network components and technical monitoring systems.

Our standardised approach allows an investigation into the „state of health" of the entire IT similarly to getting a medical check-up from a doctor. This is then compared to a target ICS profile (see Figure 4) drawn up in cooperation with the customer. The results are recorded in a standardised report.

Workflow for the eHealthCheck

The analysis and assessment consists of two phases with interviews with the persons in charge from senior management, the IT department and other business departments, and the evaluation of the existing internal documentation, with additional in-depth review steps if required.

Phase I: The company and industry-specific minimum target ICS profile is determined during a one-hour meeting (Figure 4).

Phase II: Performance of the actual cross IT audit based on the size and complexity of the company. The current profile is determined and compared to the jointly developed target ICS profile.

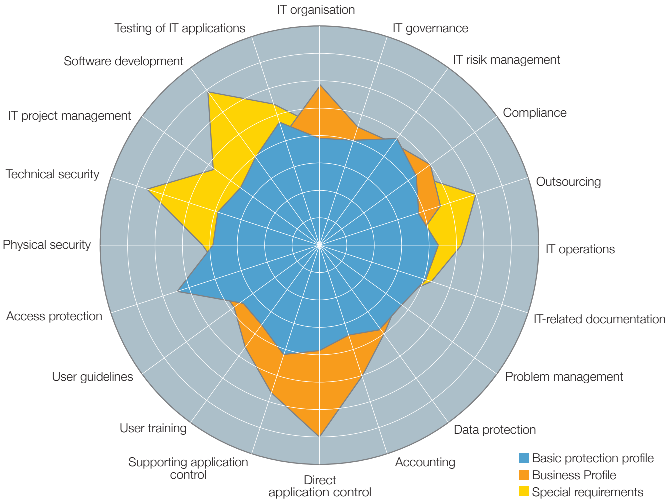


Figure 4: Target ICS profile based on a profile for baseline protection, one for business processes and one for special company-specific requirements

Phase I: Simulation of the company-specific target ICS profile within IT

When comparing the actual state with a set target state, the question arises as to whether the discrepancies highlighted are because the set goal is too ambitious or the current situation is actually unsatisfactory. It is, therefore, all the more important that not only the current situation is professionally determined, but that the „yardstick", the target state, is based on objective criteria.

It is, therefore, crucial to understand how a target ICS profile should look like for a specific company in a specific industry using specific business processes.

The eHealthCheck simulation model involves an initial interview with the department management being examined, which allows a company and industry-specific minimum target profile to be defined within a short space of time. This considerably improves acceptance of the subsequent audit procedures and possibly unsatisfactory results.

Simultaneously, the ICS simulation during the initial meeting with the customer allows the determination of further in-depth investigations required (Figure 5).

Phase II: The cross IT audit

The actual cross IT audit is carried out based upon the grid already utilized for the IT risk assessment with its 91 IT controls condensed into 20 general topics. Depending on the size of the company and the level of assurance required, the overall time required will be between 5 and 25 person days, including the compilation of a written report.

More in-depth checks

The cross IT audit or allready the earlier determination of the target ICS profile should reveal as to whether further in-depth checks are required and should be scheduled.

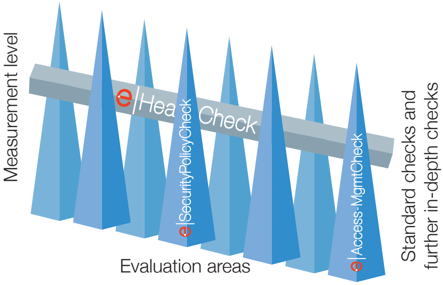


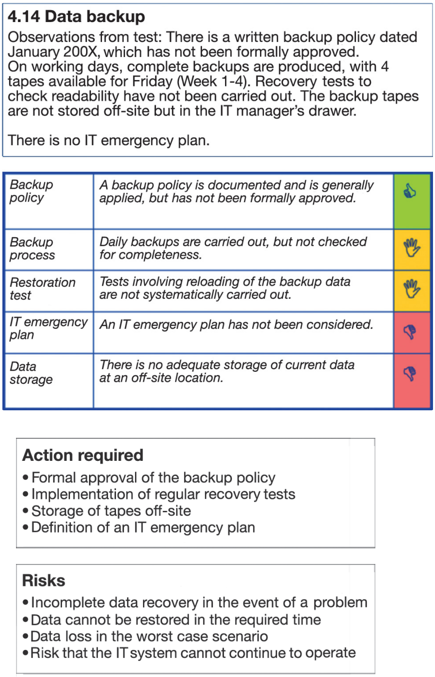
Figure 5: Positioning of the eHealthCheck, evaluation areas and measurement level

The target ICS profile defined is a key factor in the above decision: Depending upon which lines on the spider diagram necessitate high levels of maturity, more in-depth checks may be required. Relatively often, these are the „traditional" issues concerning access protection, software change management, IT operations, etc. – but sometimes there are also other issues which would barely have been considered or analysed in more detail without a simulation of the IT ICS.

Deliverables of the eHealthCheck

Description of current state, risks and actions required

The results of the eHealthCheck are summarised in a written report, which sets out both the current situation as well as the recognisable risks and corresponding recommendations. This allows the specific selection of the most important issues for targeted improvements and/or more in-depth analysis.



4.14 Data backup

Observations from test: There is a written backup policy dated January 200X, which has not been formally approved.
On working days, complete backups are produced, with 4 tapes available for Friday (Week 1-4). Recovery tests to check readability have not been carried out. The backup tapes are not stored off-site but in the IT manager's drawer.

There is no IT emergency plan.

Backup policy	*A backup policy is documented and is generally applied, but has not been formally approved.*	👍
Backup process	*Daily backups are carried out, but not checked for completeness.*	✋
Restoration test	*Tests involving reloading of the backup data are not systematically carried out.*	✋
IT emergency plan	*An IT emergency plan has not been considered.*	👎
Data storage	*There is no adequate storage of current data at an off-site location.*	👎

Action required

- Formal approval of the backup policy
- Implementation of regular recovery tests
- Storage of tapes off-site
- Definition of an IT emergency plan

Risks

- Incomplete data recovery in the event of a problem
- Data cannot be restored in the required time
- Data loss in the worst case scenario
- Risk that the IT system cannot continue to operate

Figure 6: Extract from an example report

Summary of the results of the eHealthCheck

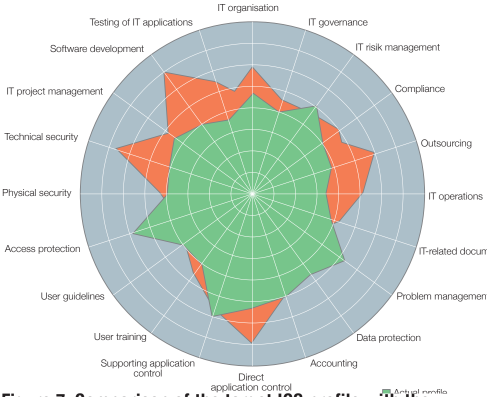


Figure 7: Comparison of the target ICS profile with the actual ICS profile in a spider diagram

A systematic survey of the facts with more than 90 questions which are evaluated based upon a four-level maturity model with individually specified requirements for each question and their compression into 20 subject areas detailed above by our trained specialists will give you valuable insight into all the relevant key indicators and therefore the inherent risks in the most important areas of IT.

Besides a descripton of the current situation and an overview, the written report also highlights the recognisable risks and provides recommendations accordingly. This allows prioritised selection of the most important issues for targeted improvements and/or more in-depth analysis.

The report also features a management summary, which recapitulates the most important findings in regard to information security, data protection and IT governance (management of IT).

Organisation and costs

The timing and the costs for an eHealth-Check depend on the scope of the audit defined and the size of the company.

Cost estimate and ceiling

The cost of the evaluation provided depends on numerous factors, which need to be determined before the review. Without further in-depth checks, the total expenditure typically lies between 5 and 25 peron days, and can be broken down as follows:

- Detailed planning
- Collection and analysis of the existing documentation
- Interviews
- Defining the target ICS profile
- Cross IT audit, establishing process maturity
- Creation of final report
- Final presentation

Suggested optional extras, selected in-depth checks

Access-MgmtCheck
DataCenter-SecurityCheck
Risk-MgmtCheck
SecurityPolicyCheck
Service-MgmtCheck
ProjectSecurityCheck
ISO27001-ReadinessCheck
ISO27002-MaturityCheck
ISO20000-ReadinessCheck
SAPCheck

Value added by an eHealthCheck

The results of the cross IT audit (eHealthCheck) provide valuable information and findings for personnel in various positions throughout the company.

An eHealth-Check gives the Board and Senior Management concrete information concerning:

- as to whether the IT meets all the statutory and regulatory requirements with respect to data protection, data security and data integrity;
- where the IT already represents a solid basis for the current and future support for the company strategy and where improvements are required;
- that the risks in the IT environment are recognised and addressed accordingly.

The eHealthCheck shows the Head of IT and the Risk Management:

- how good the IT processes (really) are;
- as to whether the risks inherent to IT are recognised and managed;
- where there is a gap between the target requirements and the actual situation (and how wide that gap is);
- where there might be further potential for standardisation and outsourcing.

For Internal and External Auditors, the eHealthCheck is:

- an ideal approach to assessing ICS in the IT environment,
- a systematic, standardised and independent audit covering the entire IT,
- a suitable means for the determination of strengths and weaknesses within IT and the potential risks;
- an aid in determining which prior or subsequent additional in-depth IT checks should be carried out to allow for selective improvement of IT controls.

The positions above appreciate the eHealthCheck as a unique opportunity for determining the **company-specific maturity of the IT ICS** as a function of the industry, the business and other requirements.

This provides an objective comparison of the actual situation with the target state. The information and findings concerning the eHealthCheck will be accepted by all parties involved and utilized as the basis for any optimisation measures.