e|HealthCheck®

b·prex
Business Process Excellence

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

www.bprex.ch

**... und geben Ihnen Gewissheit:
rasch, kompetent, nutzbringend
und alles aus einer Hand.**

Kontrollen im Informatikbereich sind umso wichtiger, je stärker ein Unternehmen von Informatik-Systemen abhängig ist und je höher das Risiko ist, dass Fehler in den Geschäftsprozessen ihre Ursache im Aufbau von und Umgang mit Informatik-Systemen haben könnten.

Was ist der eHealthCheck?

Der Druck von Gesetzgeber, Regulatoren und Stakeholders auf die Unternehmensführung hat in den letzten Jahren deutlich zugenommen, so z.B. wegen der Anpassungen des Schweiz. Obligationenrechts (OR) in Bezug auf das Interne Kontrollsystem oder der kürzlich erfolgten Aktualisierung des Datenschutzgesetzes. Zudem stehen die Unternehmen unter einem enormen Kostendruck.

Kennen Sie die Risiken der Informatik Ihres Unternehmens?

- Wurden alle vorgeschriebenen oder notwendigen Sicherheitsmassnahmen implementiert?
- Sind die gesetzlichen Anforderungen hinsichtlich Datenschutz und Informationssicherheit ausreichend abgedeckt?
- Sind die Informatik-internen Prozesse ausreichend robust, so dass die negativen Auswirkungen bei Zwischenfällen (z.B. Ausfall kritischer Geschäftsanwendungen) in einem vernünftigen Rahmen bleiben?
- Unterstützt Ihre Informatik die Erreichung der Geschäftsziele angemessen?
- Und nicht zuletzt – wissen Sie, welche Kosten gegenwärtig und zukünftig in der Informatik anfallen werden?

Wenn Sie auf eine oder mehrere der obigen Fragen mit einem «nein» oder «ich weiss es nicht» antworten, besteht sehr wahrscheinlich ein Bedarf nach einer unabhängigen Einschätzung Ihrer Informatik, die auf die spezifischen Gegebenheiten und Bedürfnisse Ihrer Branche eingeht. Eine solche Beurteilung gibt Ihnen Gewissheit, ob Verbesserungsbedarf vorhanden ist oder dass Sie mit den eigenen Bestrebungen auf dem richtigen Weg sind.

Um das Verbesserungspotenzial oder allfällige Schwächen der implementierten Informatik (IT) auf Ebene der operativen Prozesse und der Führungsprozesse im Vergleich zu geltenden Regulatorien und bewährten Praktiken optimal ermitteln zu können, bieten wir den eHealthCheck an. eHealthCheck, ein eigentliches Wortspiel, wird mit «Check der Informatik-Gesundheit» am treffendsten beschrieben.

Der eHealthCheck ist auf der Basis von international anerkannten Standardwerken wie CobiT und ISO 27002, der aktuellen Gesetzgebung (z.B. Datenschutzgesetz, Patientinnen und Patientengesetz) sowie langjähriger Erfahrung im Umfeld von Informationssicherheit und IT-Governance in vielfältigen Kundenmandaten entstanden.

Aufbau des eHealthCheck

Der eHealthCheck kann flexibel auf eine Unternehmung skaliert werden und ermöglicht die strukturierte Einschätzung der gesamten Informatik-Umgebung.

Ein spezielles Augenmerk wird dabei auf die Bereiche Datenschutz und Informationssicherheit sowie die IT-Governance (Führung der Informatik) gelegt. Dabei werden alle Informatik-relevanten Sachgebiete untersucht.

Abb.1: Die Informatik-relevanten Sachgebiete

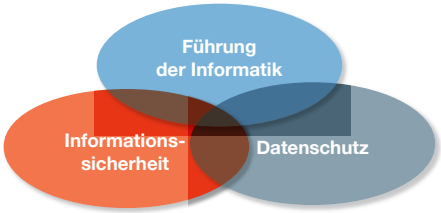

Abb. 2: Die drei voneinander abhängigen Fragestellungen zur Informatik-Sicherheit

Im Vordergrund des Datenschutzes steht das Individuum, die Person, der Kunde, der Mitarbeiter, der Patient – die Stakeholders eines Unternehmens eben, während sich die Informationssicherheit in erster Linie um die Integrität der Information, um deren physische und logische Sicherheit und Verfügbarkeit kümmert. Obwohl diese Disziplinen stark miteinander verzahnt sind, haben sie doch unterschiedliche Bedeutung und werden je nach Branche verschieden stark gewichtet.

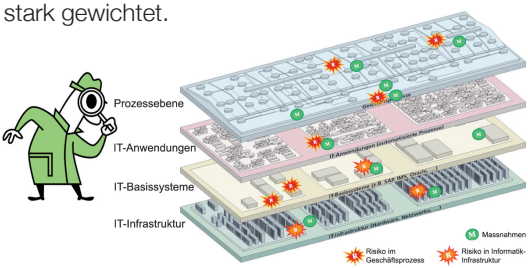

Abb. 3: Das vierstufige Schichtenmodell

Der eHealthCheck durchleuchtet das umfassende vierstufige Schichtenmodell, wobei jede der Schichten für eine Art von Prozessen und Ressourcen steht:

- In der obersten (blauen) Schicht finden wir alle wesentlichen (manuellen) Geschäftsprozesse – typischerweise aufgeteilt nach verantwortlichen Fachbereichen und in Sub-Prozesse und einzelne Aktivitäten.
- In der zweiten (roten) Schicht finden wir die automatisierten Teile der Geschäftsprozesse, die eigentlichen (IT) Anwendungen. Mit Ausnahme der wirklich kleinen KMUs wird bei praktisch allen Unternehmen der grösste Teil der Geschäftsfälle mit Hilfe solcher Anwendungen verarbeitet.
- In der dritten (gelben) Schicht finden wir die IT-Basissysteme. Dieser Begriff umfasst eine grosse Vielfalt möglicher Plattformen, auf denen die eigentlichen

Anwendungen der zweiten Schicht laufen. Beispiele sind Datenbank-Verwaltungssysteme (z.B. SQL, Oracle), die Basiskomponenten integrierter Anwendungen (z.B. SAP-Basis) oder auch eher technische Verarbeitungssysteme (z.B. Middleware).

- In der untersten (grünen) Schicht finden wir die Informatik-Infrastruktur. Im Wesentlichen umfasst diese die eigentliche Hardware (z.B. Server) wie auch die zugehörigen Netzwerk-Komponenten und technischen Überwachungssysteme.

Mit diesem standardisierten Vorgehen wird eine Untersuchung des «Gesundheitszustands» der gesamten Informatik analog einer generellen Untersuchung beim Hausarzt durchgeführt, einem gemeinsam erarbeiteten Soll-IKS-Profil (siehe Abb. 4) gegenüber gestellt und die Erkenntnisse in einem standardisierten Bericht festgehalten.

Ablauf des eHealthCheck

Die Analyse und Beurteilung erfolgt in zwei Phasen in der Form von Interviews mit den verantwortlichen Personen aus der Geschäftsleitung, der Informatik und den Zuständigen der Fachabteilungen sowie auf der Basis der vorhandenen Unternehmensdokumentation, fallweise ergänzt durch vertiefte, stichprobenmässige Erhebungen.

Phase I: In einem einstündigen Gespräch wird das unternehmen- und branchenspezifische, minimale Soll-IKS-Profil ermittelt (Abb. 4).

Phase II: In der zeitlichen Dimension abhängig von der Grösse und Komplexität eines Unternehmens erfolgt die eigentliche Querschnittsprüfung, die Erhebung des Ist-Zustandes und der Vergleich zum gemeinsam entwickelten Soll-IKS-Profil.

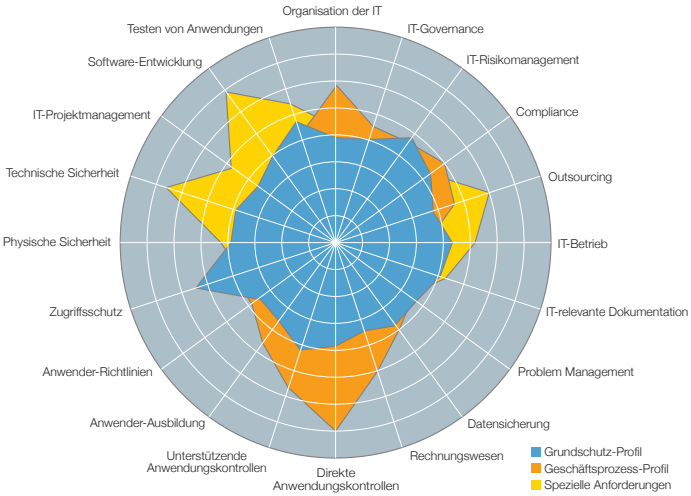

Abb. 4: Soll-IKS-Profil basierend auf einem Grundschutz- und Geschäftsprozess-Profil sowie auf speziellen unternehmensspezifischen Anforderungen

Phase I: Simulation des unternehmensspezifischen Soll-IKS-Profil in der IT

Bei Vergleichen zwischen Ist und Soll stellt sich schnell einmal die Frage, ob die aufgezeigten Abweichungen aufgrund überhöhter Ansprüche an das Soll oder auf tatsächlich ungenügenden Ist-Zuständen fusst. Deshalb ist es umso wichtiger, dass nicht nur der Ist-Zustand professionell erhoben wird sondern bereits die «Messlatte», das Soll, auf objektiven Kriterien basiert.

Daraus entstand die für den vorliegenden Prüfansatz absolut entscheidende Frage, wie denn für ein bestimmtes Unternehmen in einer bestimmten Branche und mit bestimmten Geschäftsprozessen ein Soll-IKS-Profil aussehen müsste.

Mit dem Simulationsmodell des eHealth-Check wird im Rahmen des Eröffnungsinterviews mit der Leitung des geprüften Bereichs innert kürzester Zeit ein unternehmen- und branchenspezifisches, minimales Soll-Profil bestimmt. Dies führt zu einer deutlichen Zunahme der Akzeptanz der nachfolgenden Prüfungshandlungen und allfälliger ungenügender Ist-Situationen.

Darüber hinaus bestimmen wir mit der IKS-Simulation bereits im ersten Gespräch mit dem Auftraggeber allenfalls notwendige Vertiefungsprüfungen (Abb. 5).

Phase II: Die eigentliche Querschnittsprüfung

Basierend auf dem bereits für die IT-Risikobeurteilung verwendeten Raster mit den 91, zu 20 generellen Themen verdichteten IT-Kontrollen, wird eine eigentliche IT-Querschnittsprüfung durchgeführt. Je nach Unternehmensgrösse und gewünschtem Grad der Assurance beläuft sich der notwendige Gesamtaufwand auf 5 bis 25 Personentage, inkl. der Erstellung eines schriftlichen Berichtes.

Vertiefungsprüfungen

Aus der Querschnittsprüfung oder aber bereits aus der IKS-Soll-Profil Bestimmung geht hervor, ob Vertiefungsprüfungen angezeigt sind und eingeplant werden sollten.

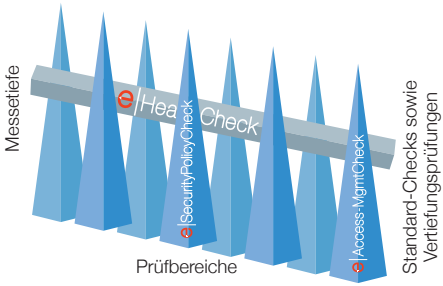

Abb. 5: Positionierung des eHealthCheck, Prüfbereiche und Messtiefen

Eine wesentliche Grundlage für diesen Entscheid ist das erhobene IKS-Soll-Profil: je nachdem, welche Strahlen im Spinnendiagramm eine zwingend hohe Maturität erfordern, drängt sich die eine oder andere Vertiefungsprüfung auf. Relativ häufig sind dies «klassische» Themen wie Zugriffsschutz, Softwareänderungsmanagement, IT-Betrieb usw. – manchmal sind es auch Themen, an die man ohne eine Simulation des (IT-) IKS kaum gedacht und damit auch kaum genauer geprüft hätte.

Ergebnisse des eHealthCheck

Beschreibung des Ist-Zustandes, der Risiken und des Handlungsbedarfs

Die Ergebnisse des eHealthCheck werden in einem schriftlichen Bericht zusammengefasst, der neben dem ermittelten Ist-Zustand die erkennbaren Risiken sowie entsprechende Empfehlungen aufzeigt. Dies ermöglicht eine gezielte Auswahl der wichtigsten Themen für gezielte Verbesserungsmassnahmen und/oder weitergehende Untersuchungen.

4.14 Datensicherung

Feststellungen als Text: Es besteht ein schriftliches Sicherungskonzept, datiert vom Januar 200x; dieses wurde nicht formell genehmigt. An Werktagen werden vollständige Sicherungen erstellt, wobei für den Freitag 4 Tapes vorhanden sind (Woche 1-4). Wiederherstellungstests zur Überprüfung der Lesbarkeit werden keine durchgeführt. Die Backup-Bänder werden nicht ausser Haus gelagert, sondern in einer Schublade des zuständigen IT-Verantwortlichen.

Ein IT-Notfallplan existiert nicht.

Sicherungs-konzept	*Ein Datensicherungskonzept ist dokumentiert und wird in der Regel angewendet; es wurde aber nie formell verabschiedet.*	
Sicherungs-prozess	*Es werden tägliche Sicherungen durchgeführt, aber nicht auf Vollständigkeit überprüft.*	
Wiederher-stellungstest	*Es werden keine systematischen Tests zum Zurückladen der Sicherungen durchgeführt.*	
IT-Notfallplan	*Es wurden kaum Überlegungen zum Thema IT-Notfallplan angestellt.*	
Datenaus-lagerung	*Es werden keine ausreichend aktuellen Daten-sicherungen an einem Standort ausserhalb des Unternehmens aufbewahrt.*	

Handlungsbedarf
- formelle Verabschiedung des Backup-Konzeptes
- Durchführung regelmässiger Wiederherstellungs-tests
- Auslagerung der Bänder ausser Haus
- Definition eines IT-Notfallplans

Risiken
- Unvollständige Datenwiederherstellung im Schadenfall
- Datenwiederherstellung nicht in der geforderten Zeit
- Datenverlust im Katastrophenfall
- Gefährdete Fortsetzung des IT-Betriebes

Abb. 6: Auszug aus einem Beispielbericht

Zusammenfassung der Ergebnisse des eHealthCheck

Abb. 7: Gegenüberstellung des Soll-IKS-Profils zum Ist-IKS-Profil im Spinnendiagramm

Die systematische Erhebung der Fakten mit über 90 Fragen, ihre Bewertung in einem vierstufigen Maturitätsmodell mit für jede der Fragen individuell spezifizierten Anforderungen sowie die Verdichtung zu den 20 oben aufgeführten Themen durch unsere ausgewiesenen Spezialisten ergibt einen hochwertigen Einblick in alle relevanten Schlüsselindikatoren und damit der inhärenten Risiken in den wichtigsten Bereichen der Informatik.

Der schriftliche Bericht zeigt neben dem ermittelten Ist-Zustand und der Gesamtübersicht der Maturität die erkennbaren Risiken sowie entsprechende Empfehlungen auf. Dies ermöglicht eine priorisierte Auswahl der wichtigsten Themen für gezielte Verbesserungsmassnahmen und/oder weitergehende Untersuchungen.

In einem Management-Summary werden darüber hinaus die wichtigsten Erkenntnisse aus Optik Informationssicherheit, Datenschutz und IT-Governance (Führung der Informatik)zusammengefasst.

Organisation und Kosten

Die zeitliche Planung sowie die Kosten eines eHealthCheck sind vom definierten Prüfumfang und der Grösse eines Unternehmens abhängig.

Aufwandschätzung und Kostendach

Der Aufwand für die aufgeführten Analyse-Dienstleistungen hängt von zahlreichen zu Beginn einer Untersuchung zu eruierenden Faktoren ab, die sich unter anderem auch aus der nach der Auftragserteilung erarbeiteten Vorgehensweise und Detailplanung ergeben können.

Der Gesamtaufwand, ohne allfällige Vertiefungsprüfungen, beläuft sich typischerweise auf 5 bis 25 Tage und lässt sich wie folgt gliedern:

- Detailplanung
- Sammlung und Studium der vorhandenen Dokumentation
- Durchführung der Interviews
- Erhebung des Soll-IKS-Profil
- Querschnittsprüfung; Erhebungen der Prozess-Maturität
- Erstellung des Abschlussberichtes
- Schlusspräsentation

Sinnvolle Ergänzungen
Ausgewählte Vertiefungsprüfungen

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

Wertschöpfung durch einen eHealthCheck

Das Resultat aus dem vorgestellten Prüfmodell (eHealthCheck) liefert wertvolle Informationen und Erkenntnisse für die unterschiedlichsten Funktionsträger eines Unternehmens.

Dem Verwaltungsrat und der Geschäftsleitung bringt ein eHealthCheck Gewissheit darüber:

- ob die Informatik die gesetzlichen und regulatorischen Anforderungen hinsichtlich Datenschutz, Datensicherheit und Datenintegrität erfüllt;
- wo die IT bereits eine solide Grundlage für die aktuelle und künftige Unterstützung der Unternehmensstrategie darstellt und wo Verbesserungen notwendig sind;
- dass die Risiken im IT-Umfeld erkannt und entsprechend adressiert sind.

Dem Informatikleiter und dem Risiko-Management zeigt der eHealthCheck auf:

- wie gut die Informatikprozesse (wirklich) sind;
- ob die inhärenten Risiken der Informatik bekannt sind und gemanagt werden;
- wo Soll-Anforderungen und Ist-Zustand auseinanderklaffen (und wie weit);
- wo sich Standardisierungs- und Outsourcing-Potential ergeben.

Für die interne oder externe Prüfstelle ist der eHealthCheck:

- die ideale Vorgehensweise für die Beurteilung des IKS im IT-Umfeld;
- die systematische, standardisierte und unabhängige Querschnittsprüfung der gesamten IT;
- das geeignete Mittel für die Ermittlung der Stärken und Schwächen der Informatik sowie des Risikopotentials;
- eine Unterstützung bei der Bestimmung der vor- oder nachgelagerten IT-Vertiefungsprüfungen zur selektiven Verbesserung von IT-Kontrollen.

Die oben erwähnten Funktionsträger schätzen die einzigartige Möglichkeit des eHealthCheck, den **unternehmensspezifischen notwendigen Reifegrad des IT-IKS** in Abhängigkeit von Branche, Geschäftstätigkeit und Zusatzanforderungen bestimmen zu können.

Damit ist ein objektiver Soll-Ist Vergleich gegeben. Die Informationen und Erkenntnisse aus dem eHealthCheck werden von allen involvierten Seiten akzeptiert und als Basis für allfällige Optimierungsmassnahmen weiter verwendet.

b·prex
Business Process Excellence

b·prex group ag
Stampfenbachstr. 40 • 8006 Zürich • Tel +41 44 444 11 04 • Fax +41 44 444 11 02
contact@bprex.ch • www.bprex.ch