

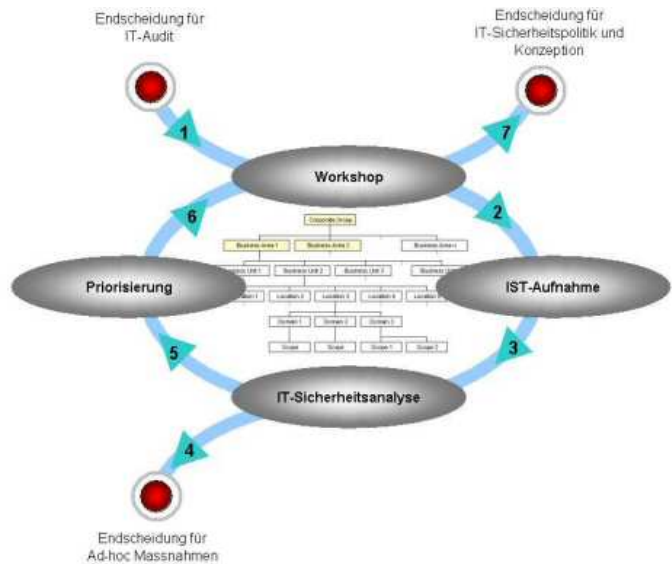
Organisatorische IT-Sicherheitsüberprüfungen (IT-Audits)

EISA-Projekt: IT-Risiken bewerten, Massnahmen priorisieren, entscheiden und umsetzen

EINLEITUNG

EISA-Projekt ist eine Sicherheitsüberprüfung (Audit) gegen Standards im organisatorischen und technischen Umfeld. Bewährte Beratungstechniken werden mit regelbasiertem Expertenwissen in Form von Datenbanken kombiniert. Die Teilprojekte erfolgen nach dem Phasenmodell in den vier Projektphasen:

1. Workshop
2. IST-Aufnahme mit Interviews und ggf. technischen Nachprüfungen
3. Sicherheitsanalyse mit Bericht
4. Priorisierung der empfohlenen Massnahmen



Ziele

Ziel eines Audits ist das Erkennen von Mängeln in der Organisation und von Fehlern in der technischen Umsetzung der Sicherheitskonzepte. In weiteren Schritten kann über geeignete Massnahmen bis hin zur Etablierung einer globalen Sicherheitspolitik entschieden werden.

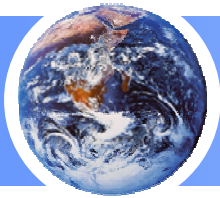
Standards

Der gewählte Standard bestimmt die Sicherheitsanforderungen, die erfüllt werden müssen. EISA-Projekt unterstützt den IT-Sicherheitsstandard ISO 27001 auf Basis IT-Grundschutz.

PHASE 1 – WORKSHOP

Im Workshop erfolgt die Aufnahme der Anforderungen des Kunden und die genaue Festlegung der Prüfbereiche. In einem speziellen Dokument, dem „Sicherheitsprofil“, werden die Entscheidungen zum erforderlichen Schutzbedarf der Daten und Informationen, die primären Schutzziele sowie des benötigten Sicherheitsniveaus festgehalten. Diese Informationen dienen später der Risikoanalyse. In Form eines Prüfplans wird festgelegt, welche IT-Bereiche und welche Themen abgeprüft werden müssen.



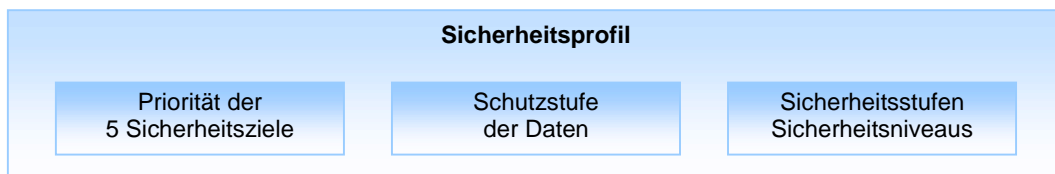


Organisatorische IT-Sicherheitsüberprüfungen (IT-Audits)

EISA-Projekt: IT-Risiken bewerten, Massnahmen priorisieren, entscheiden und umsetzen

Ergebnis des Workshops: Das Sicherheitsprofil

In der Sicherheitsanalyse werden die vorhandenen Defizite mit Hilfe eines regelbasierten Verfahrens risikobewertet. Die Anpassung der Bewertung an die vorhandene bzw. gewünschte Sicherheitspolitik des Unternehmens erfolgt über das Sicherheitsprofil.



Das Sicherheitsprofil erfasst drei wichtige Eigenschaften der angewandten Sicherheitspolitik des Unternehmens für den untersuchten Bereich:

- Präferenzen** Priorität bzw. Gewichtung der 5 Sicherheitsziele Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität und Verbindlichkeit. Wenn z.B. Verfügbarkeit stärker als die anderen Sicherheitsziele gewichtet ist, dann werden später die empfohlenen Sicherheitsmaßnahmen zum Schutz der Verfügbarkeit höher priorisiert, wohingegen die Schutzmaßnahmen für die anderen Sicherheitsziele geringer priorisiert werden.
- Schutzstufe** Einschätzung der Sensibilität der Daten und Informationen bzw. investierten Werte im untersuchten Umfeld bzgl. Vertraulichkeit, Integrität und Verfügbarkeit (Datenklassifizierung).
- Sicherheitsstufen** Qualifizierungen des festgestellten Sicherheitsniveaus im Hinblick auf Sicherheit und Angemessenheit für den erforderlichen Aufwand für die Sicherheitsmaßnahmen.

Ergebnis des Workshops: Der Prüfplan

Der Prüfplan ist eine Vereinbarung, welche IT-Bereiche zum Prüfungsumfang gehören. Zu jedem IT-Bereich wird festgelegt, welche Prüfungsthemen geprüft werden sollen (z.B. Betriebssystem Windows, Datenbanken, Lotus Notes, Gebäudeschutz, Rechenzentrum, usw.).

Ziele des Workshops

Der Workshop bringt die Sichtweise des Managements der Kundenfirma mit dem Wissen der Sicherheitsspezialisten der Beratungsfirma zusammen. Ziel ist eine Konsensfindung als Basis für die Beurteilung der angemessenen Sicherheit und für die Ableitung geeigneter Massnahmen, wie diese Sicherheit zu erreichen ist.



Organisatorische IT-Sicherheitsüberprüfungen (IT-Audits)

EISA-Projekt: IT-Risiken bewerten, Massnahmen priorisieren, entscheiden und umsetzen

PHASE 2 - IST-AUFNAHME

Für das Thema org. Sicherheit (z.B: Sicherheitspolitik, Regelungen) werden Interviews auf Basis von Checklisten durchgeführt. Bei eher technischen Themen (z.B. Betriebssysteme) können zusätzlich Systemschecks erforderlich sein. Bei Infrastruktur-Sicherheit (z.B. Gebäudeschutz) werden generell zusätzliche Vorortbesichtigungen der Liegenschaft durchgeführt. Die Checklisten können auch in Eigenregie der Kundenfirma ausgefüllt werden. Zur Bestätigung einzelner kritischer Aussagen können zusätzliche Stichproben notwendig werden.

Checklisten werden eingesetzt, um alle signifikante Informationen vollständig, werturteilsfrei und schnell zu erfassen. Die Checklisten mit den Risikoindikatoren (Fragen) basieren auf dem gewählten Sicherheitsstandard (z.B. ISO 27001 auf Basis IT-Grundschutz).

PHASE 3 – SICHERHEITSANALYSE

Analysiert und bewertet wird die vorhandene Sicherheitspolitik und deren Umsetzung in Form von Konzepten und Regelungen.

Ein Vergleichskonzept definiert die minimalen Anforderungen an die Sicherheit für einen mittleren Schutzbedarf.

Eine mögliche Risikoerhöhung wird unter Berücksichtigung der vorliegenden Informationen eingeschätzt und qualifiziert. Das Ergebnis ist u.a. der Sicherheitsstatus.

Organisatorische IT-Sicherheit
Mitgeteilte Informationen - IST-Aufnahme

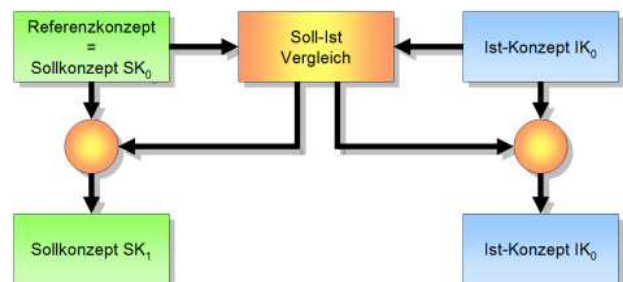
(07) - Berechtigungen - Organisation, Zutrittsrechte

(M2.006) - Vergabe von Zutrittsberechtigungen

Vor der Vergabe von Zutrittsberechtigungen für Personen sind die schutzbedürftigen Räume eines Gebäudes zu bestimmen, z. B. Büro, Datenträgerarchiv, Serverraum, Operating-Raum, Maschinsaal, Belegarchiv, Rechenzentrum. Der Schutzbedarf eines Raumes ist festzustellen anhand der im Raum befindlichen Informationstechnik sowie am Schutzbedarf der eingesetzten IT-Anwendungen und ihrer Informationen.

Bemerkungen:
- Keine -

		Ja	Teilweise	Nein	Nicht
01	Wird die Dokumentation schutzbedürftiger Räume und zugriffsberechtigter Personen aktualisiert? Bemerkung Informant: 70%, nicht zeitnah	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
02	Werden die Räume nach ihrer Schutzbedürftigkeit unterschieden?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
03	Der Schutzbedarf eines Raumes wird anhand der im Raum befindlichen IT und der eingesetzten IT-Anwendungen und ihrer Informationen festgesetzt. Ist die Vergabe von Zutrittsberechtigungen für Personen vom Schutzbedarf des Raumes abhängig?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
04	Liegt eine Dokumentation vor, die den Schutzbedarf von IT-Räumen ausweist?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
05	Durch Funktionstrennung wird festgelegt welche Funktionen nicht zusammen von einer Person ausgeübt werden dürfen. Wird die Funktionstrennung bei der Vergabe von Zutrittsrechten berücksichtigt?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>





Organisatorische IT-Sicherheitsüberprüfungen (IT-Audits)

EISA-Projekt: IT-Risiken bewerten, Massnahmen priorisieren, entscheiden und umsetzen

Berichtswesen

Der Bericht umfasst das Management-Summary, sowie die Einzelauswertungen mit kritischen Schwachstellen und Massnahmen.

In den Berichten wird der Sicherheitsstatus als Prozentwert ausgewiesen. Der Prozentwert bewertet den Erfüllungsgrad der geprüften Massnahmen gegenüber den Anforderungen aus dem gewählten Sicherheitsstandard. Die vorhandene Sicherheit wird durch das noch vorhandene Restrisiko für die Erfüllbarkeit der Sicherheitspolitik festgelegt. Zwischen dem Sicherheitsstatus in den Berichten und dem Restrisiko besteht folgender mathematischer Zusammenhang:

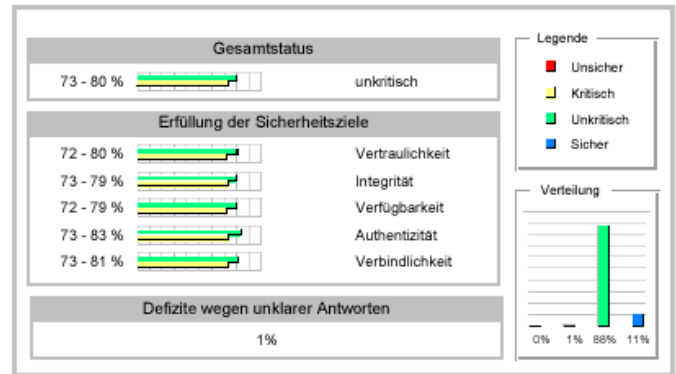
$$\text{Sicherheitsstatus} = (1 - \text{Restrisiko}) \times 100\%$$

(Restrisiko = 0,00 – 1,00)

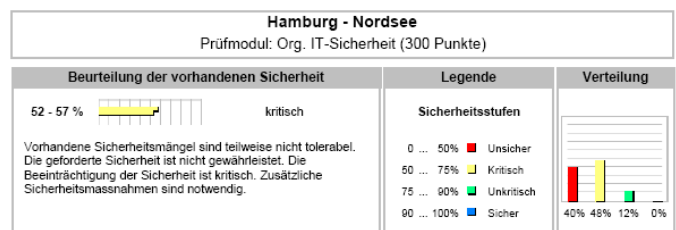
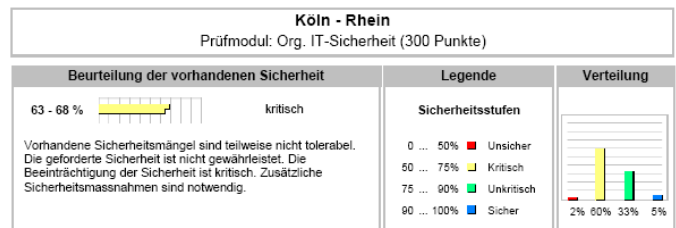
Wenn alle angemessenen Sicherheitsmassnahmen wirksam sind, ist das verbleibende Restrisiko zwar nicht völlig Null, aber in einem Bereich, welcher vom Unternehmen akzeptierbar ist. Die Sicherheit ist dann per Definition zu 100 % gegeben.

100%-ige Sicherheit ist meist nur mit sehr großem Aufwand erreichbar, welcher oft die Möglichkeiten eines unter wirtschaftlichen Bedingungen tätigen Unternehmens übersteigt.

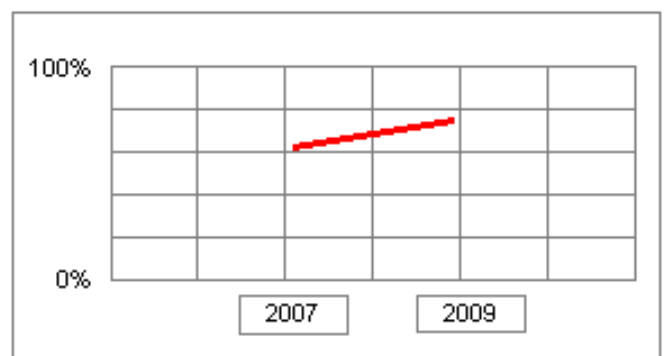
Möglich ist ein Vergleich zwischen Standorten, IT-Bereichen, Themen und Perioden. Zum Beispiel lässt sich feststellen, ob das Unternehmen bei der technischen Sicherheit besser dasteht als bei der org. Sicherheit oder im Gebäudeschutz. Im Periodenvergleich lässt sich der Erfolg oder Misserfolg des Ressourceneinsatzes an Zeit und Geld ablesen. Zum Periodenvergleich ist ein Wiederholungsaudit unter gleichen Bedingungen erforderlich.



Status der Sicherheitsziele und insgesamt



Bsp.: Vergleich der org. IT-Sicherheit zweier Standorte



Entwicklung der Sicherheit zwischen zwei Audits



Organisatorische IT-Sicherheitsüberprüfungen (IT-Audits)

EISA-Projekt: IT-Risiken bewerten, Massnahmen priorisieren, entscheiden und umsetzen

Schwachstellen-Report

Als „Schwachstellen“ werden Defizite mit hohen Risiken bezeichnet (Schadenshöhe, Eintrittswahrscheinlichkeit). Besonders kritische Schwachstellen sind hohe Defizite, bei denen der Sicherheitsstatus weniger als 50% beträgt. Hier besteht sofortiger Handlungsbedarf.

Alle gefundenen Defizite werden im Schwachstellen-Report ausgewiesen. Auf Schwachstellen mit sofortigem Handlungsbedarf geht der Berater in der Management-Zusammenfassung nochmals gesondert ein.

Verfügbarkeit der Ergebnisse

Die Ergebnisse können unmittelbar im Anschluss an die erste Auswertung dem Management zur Verfügung gestellt werden. Dadurch sind sehr zeitnahe Entscheidungen möglich.

PHASE 5 PRIORISIERUNG

Die Sicherheitsanalyse liefert Massnahmen, die entsprechend der Sicherheit gewichtet sind. Mit Hilfe der Massnahmenpriorisierung können auch andere Faktoren wie Ressourcen, Umsetzbarkeit, Budget in die Rangfolge der Massnahmen einfließen.

Die Massnahmenpriorisierung erfolgt in einem Workshop mit Hilfe eines Tools. Ergebnis ist eine Massnahmendatenbank mit auswertbaren Informationen. Weitere Möglichkeiten sind anschliessend eine Kostenplanung und eine Schadensanalyse für den Fall, wenn Massnahmen nicht umgesetzt werden sollen. Somit sind alle Kontrollmechanismen beschrieben und können in einen laufenden Überwachungsprozess einbezogen werden.

(03) - Sicherheitsprozess

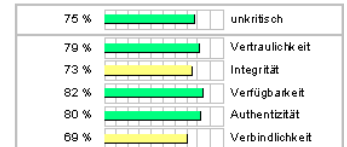
IT-Sicherheit ist ein laufender Geschäftsprozess. Zur Sicherstellung des Prozesses müssen Risiken abgeschätzt und bewertet sein.

Sicherheitsbewertung:

Risikoklasse: 1 (Hohes bis maximales Risiko)

Restrisiko: 0,25

Bewertung: Schwachstelle



Bemerkungen:

- Keine -

Nicht relevant, nicht geprüft oder nicht bekannt:

Indikatoren / Stärken / Schwächen	Risikoklasse	Teilweise	Ergänzende Bemerkungen
14 Findet regelmässig eine Überprüfung des Prozesses IT-Sicherheit statt? Bemerkung 'Relevanz': Kein Prozess definiert	-	<input type="checkbox"/>	

Positives:

Indikatoren / Stärken / Schwächen	Risikoklasse	Teilweise	Ergänzende Bemerkungen
03 Es werden Risikoanalysen zur näheren Betrachtung der Auswirkungen auf die Geschäftstätigkeit durchgeführt.	2	<input type="checkbox"/>	
04 Aufgetretene Risiken werden schriftlich festgehalten.	2	<input type="checkbox"/>	
05 Risiken werden durch Massnahmenauswahl und -umsetzung auf ein akzeptables Mass reduziert.	1	<input type="checkbox"/>	
06 Die verbliebenen Restrisiken sind schriftlich festgehalten.	2	<input type="checkbox"/>	

Schwachstellen: Auch Positives wird dokumentiert

The screenshot shows the TISA Tools interface with a table of measures and their status. Key elements include:

- Table:** Columns for ID, Risk, Assessment, Urgency, Effort, Severity, Priority, and Action. Measures include 'Detektorinstallationspunkt auf dem Gelände installieren' and 'Organisationsmassnahmen - Kontrollgänge durchführen lassen'.
- Right Panel:** 'Massnahmenpriorisierung und -umsetzung' section showing 'Erfüllungsgrad: 0%' and 'Schwierigkeit: Mittel'.
- Bottom:** 'Verantwortliche' field for each measure.

Die Massnahmenpriorisierung erfolgt mit Hilfe eines Tools