



## Einführung

---

Durch das IT-Security Audit wird die gesamte Firma im Bereich der IT überprüft, das heisst, alle Prozesse, welche die IT berühren, werden einer detaillierten Untersuchung unterzogen. Dabei sind sämtliche Organisationsstufen betroffen: Geschäftsführung – IT-Leitung– IT-Verantwortliche –Mitarbeiter.

Jeder Zielgruppe werden konkrete Fragen gestellt, die sich ergänzen oder eine gegenseitige Kontrolle ermöglichen (z.B. Kompetenzen) und schliesslich zu einem Gesamtbild, einer Gesamtbeurteilung führen.

Bei der technischen Überprüfung werden das Netzwerk, die Server sowie die Clients kontrolliert. Diesbezüglich stellen wir Fragen technischer Art (z.B. Backupprozess: Wann?, Verantwortlichkeiten?, Lagerung?, etc.). Zusätzlich werden bei der technischen Überprüfung Verbindungen von/nach aussen kontrolliert (Partner, Heimarbeitsplätze, Aussenstellen, Internetzugang etc.).

## Inhalte

---

Auditieren der technischen und organisatorischen Gegebenheiten mittels Fragenkatalog und einer Inspektion der technischen Infrastruktur.

### Analyse der Ergebnisse

Konzepte, Reglemente, Technik und Umsetzungsstand untersuchen.

### Auswertung

Beurteilung der Risiken vornehmen. Einstufung der geschäftskritischen Gefahren sowie Massnahmenkatalog erarbeiten.

### Präsentation und Besprechung

Besprechung der wichtigsten Schwachstellen und Massnahmen.

## Nutzen

---

- :: **Wissen, wie es um die IT-Sicherheit steht**  
Wie sieht es allgemein um die Sicherheit aus? Was gilt es zu tun, um die Sicherheit zu erhöhen oder konstant zu halten?
- :: **Schwachstellen kennen**  
Welche Schwachstellen sind vorhanden? Welche Risiken sind damit verbunden? Mit welchen Auswirkungen muss gerechnet werden?
- :: **Massnahmen kennen**  
Was kann gegen die vorhandenen Schwachstellen unternommen werden? Welche Schritte sind als Erstes notwendig?
- :: **Planungsinstrument**  
Wann sollen Massnahmen umgesetzt werden? Mit welchen Kosten ist dies verbunden?
- :: **Vorbereitung auf einen möglichen Notfall**  
Massnahmen kennen und vorbereitende Schritte vor einem Notfall treffen.
- :: **Organisatorische / techn. Unterstützung**  
Mit den von uns erstellten Unterlagen ist es möglich, die weiteren Schritte selber oder mit einem IT-Partner umzusetzen. Sollten im Vorfeld detaillierte Fragen anstehen, können wir auf Basis des IT-Security Audits entsprechende Konzepte erarbeiten.
- :: **Sensibilisierung**  
Die Mitarbeiter sind oft das schwächste Glied in einer Sicherheits-Kette. Daher werden die Mitarbeiter in das IT-Security Audit integriert, damit sie zu einem grösseren Sicherheitsdenken angehalten werden können.
- :: **Verständnis der GL für IT wecken**  
Unser Anliegen ist es, auch nicht im IT-Bereich spezialisierte Mitglieder der Geschäftsleitung für nötige Massnahmen und deren Nutzen zu sensibilisieren. Dabei wird auch auf die Gefahren, die bei einer Nicht-Umsetzung drohen, hingewiesen.

## ***Vorgehen***

---

- :: Bedürfnisaufnahme**  
Mit Ihnen zusammen wird der Fokus und die Tiefe der einzelnen Themen, festgelegt. Dies ist abhängig vom Stand der IT.
- :: Vorbereitung**  
Die uns zur Verfügung gestellten Unterlagen werden sorgfältig studiert und bilden die Grundlage für das Audit.
- :: Audit**  
Vor Ort, ca. zwei bis vier Tage (Fragenkatalog, technische Überprüfung, Rundgang).
- :: Auswertung**  
Erstellen des Gefahrenkataloges und der entsprechenden Massnahmen.
- :: Präsentation**  
Präsentation und Besprechung der Resultate mit den IT-Verantwortlichen und der Geschäftsleitung.
- :: Nachbesprechung**  
Viele Fragen tauchen erst nach der Präsentation auf. Diese werden an einer Nachbesprechung beantwortet.

## ***Resultate***

---

- :: Zusammenfassung für die Geschäftsleitung**
- :: Risiko-Map (Übersicht) mit den behandelten Bausteinen und deren Einstufung in der Gesamtübersicht**
- :: Gefahrenpotentialliste in der Übersicht und pro Baustein**
- :: Gewichtete Massnahmen pro Baustein inkl. den Zuständigkeiten**
- :: Excel Tabelle mit allen Massnahmen (inkl. der Risikoverteilung) und den Zuständigkeiten**
- :: Alle Ergebnisse übersichtlich auf einer CD hinterlegt**
- :: CD ergänzt mit zusätzlichen Dokumenten und Informationen**

## ***Zielgruppe des IT-Security Audits***

---

Das IT-Security Audit richtet sich an mittlere bis grössere Firmen mit mindestens dreissig IT-Arbeitsplätzen und drei Servern. Das Verständnis für die IT sowie Grundbedürfnisse der Sicherheit müssen bekannt sein.

## ***Kosten***

---

Audit (durch Kunden begleitet): 2-4 Tage  
Bericht: 3-5 Tage

Der Aufwand ist abhängig von der Grösse und der Komplexität der Firma. (Anzahl Server, Netzwerkaufbau, Standorte, etc.)

Die Kosten bewegen sich in der Grössenordnung von Fr. 9'500.- (5 ½ Tage).

## ***Referenzen***

---

Amt für Militär und Zivilschutz, Zürich  
CARBOGEN AMCIS AG, Aarau  
Gemeinde Obersiggenthal  
Gemeinde Neuenhof  
Graf + Cie AG, Rapperswil  
Hauseigentümerverband, Zürich  
Orell Füssli Holding AG, Zürich  
Pfisterer SEFAG AG, Malters  
PMA AG, Uster  
Sanacare, Winterthur  
Symotech, Kleindöttingen  
Vorstadt Treuhand AG, Wynau  
WMH, Walter Meier Holding, Stäfa

## ***Kundenaussagen***

---

Die Art und Weise des Vorgehens hat uns überzeugt. Wir wurden von Anfang an in alle Punkte des Konzeptes mit einbezogen, was uns ein Gefühl der Sicherheit gab. Wir können die Firma GO OUT Production GmbH nur weiterempfehlen, denn Ihre Art und Weise einer Sicherheitsüberprüfung hat Hand und Fuss. (Hans-Ueli Studer, Pfisterer SEFAG AG)

Die Firma hat uns mit Know-how und Dokumentation überzeugt. Die wesentlichen Schwachstellen und Korrekturmassnahmen wurden aufgezeigt. Es wurde auf Fragen eingegangen und kompetente Erläuterungen abgegeben. (Marc Bühler, Amt für Militär und Zivilschutz)

## ***Kontakt***

---

GO OUT Production GmbH  
Schulstrasse 11  
8542 Wiesendangen  
Tel: 052 320 91 20  
Fax: 052 320 91 21  
info@goout.ch  
www.goSecurity.ch