

IT-Security Forum #8



## ISO 27001 / ISO 27005 Vorgehen und Anwendung

Andreas Wisler  
Dipl. Ing. FH, CISSP, ISO 27001 Lead Auditor  
**GO OUT Production GmbH**  
[wisler@gout.ch](mailto:wisler@gout.ch)



IT-Security Forum #8

## Agenda

- Normenübersicht
  - ISO 27001
  - ISO 27002
  - ISO 27005
- Risikomanagementprozess
- Risiko Betrachtung und Reduktion
- Eintrittswahrscheinlichkeit
- Beispiel
- Hilfsmittel
  - Verinice
  - QSEC



GO OUT  
IT-SECURITY  
HOSTING

entec  
IT-COMMUNICATION

FORTINET

McAfee

wikima  
THE FREE ART OF COOKING BUSINESS

IT-Security Forum #8


Computerworld.ch  
Blickpunkt KMU  
maschinenbau

## ISO 27001

- Modell für
  - Einrichtung
  - Umsetzung
  - Durchführung
  - Überwachung
  - Überprüfung
  - Instandhaltung
  - Verbesserung

eines Informationssicherheits-Managementsystems (ISMS)

- Die Einführung eines ISMS sollte eine strategische Entscheidung sein.



28

GO OUT  
IT-SECURITY  
HOSTING

entec  
IT-COMMUNICATION

FORTINET

McAfee

wikima  
THE FREE ART OF COOKING BUSINESS

IT-Security Forum #8

Computerworld.ch  
Blickpunkt KMU  
maschinenbau

## ISO 27001

- Informationssicherheits-Managementsystem (ISMS)

**Plan**

Establish ISMS

**Do** Implement and operate the ISMS

**Check** Monitor and review the ISMS

**Act** Maintain and improve the ISMS

Interested Parties

Interested Parties

Information security requirements and expectations

Managed information security

Quelle: ISO 27001

29

GO OUT  
IT-SECURITY  
HOSTING

entec  
IT-COMMUNICATION

FORTINET.

McAfee

wikima  
THE ART OF CREATING BUSINESS

IT-Security Forum #8

Computerworld.ch  
Blickpunkt KMU  
maschinenbau

## ISO 27001

- Vorgehen / Inhalt
  - Definition des Anwendungsbereichs + Grenzen des ISMS
  - Definition der ISMS-Leitlinie
  - Identifizierung der Risiken \*
  - Analyse und Bewertung der Risiken \*
  - Bewertung der Optionen für die Risikobehandlung \*
  - Auswahl der Massnahmenziele
  - Zustimmung und Genehmigung des Managements
  
  - Umsetzung
  
  - Überwachung und Überprüfung
  
  - Bereitstellung von Ressourcen
  - Schulungen, Bewusstsein und Kompetenzen

30

GO OUT  
IT-SECURITY  
HOSTING

entec  
IT-COMMUNICATION

FORTINET.

McAfee


wikima  
THE ART OF CREATING BUSINESS

IT-Security Forum #8

Computerworld.ch  
Blickpunkt KMU  
maschinenbau

## ISO 27001

- Interne ISMS-Audits
  - Die Organisation muss in geplanten Abständen interne ISMS-Audits durchführen, um zu ermitteln, ob die Massnahmenziele, Massnahmen, Prozesse und Verfahren ihres ISMS:
    - die Anforderungen dieser Internationalen Norm und die relevanten gesetzlichen und amtlichen Vorschriften erfüllen;
    - die identifizierten Anforderungen an Informationssicherheit erfüllen;
    - wirksam umgesetzt und instand gehalten werden und
    - den Erwartungen entsprechend ausgeführt werden.



31

GO OUT  
IT-SECURITY  
HOSTING

entec  
IT-COMMUNICATION

FORTINET

McAfee

wikima  
THE FINE ART OF COOKING BUSINESS

IT-Security Forum #8

Computerworld.ch  
Blickpunkt KMU  
maschinenbau

## ISO 27002

- ISO 27002 enthält diverse Kontrollmechanismen:
  - 11 Überwachungsbereiche
  - 39 Kontrollziele
  - 133 Sicherheitsmassnahmen
- Bereiche:
  - Weisungen und Richtlinien zur Informationssicherheit
  - Org. Sicherheitsmassnahmen und Managementprozess
  - Verantwortung und Klassifizierung von Informationswerten
  - Personelle Sicherheit
  - Physische Sicherheit und öffentliche Versorgungsdienste
  - Netzwerk- und Betriebssicherheit (Daten und Telefonie)
  - Zugriffskontrolle
  - Systementwicklung und Wartung
  - Umgang mit Sicherheitsvorfällen
  - Business Continuity Management
  - Einhaltung rechtlicher Vorgaben, Überprüfungen durch Audits



GO OUT  
IT-SECURITY  
HOSTING

entec  
IT-COMMUNICATION

FORTINET

McAfee

wikima  
THE FINE ART OF COOKING BUSINESS

IT-Security Forum #8

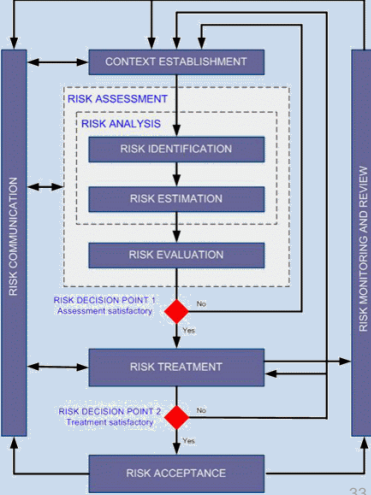
Computerworld.ch  
Blickpunkt KMU  
maschinenbau

## ISO 27005

- Risikomanagement ist die systematische Erfassung und Bewertung von Risiken sowie die Steuerung von Reaktionen auf festgestellte Risiken.

[Quelle Wikipedia]

- Wer nichts wagt, gewinnt nichts!
- Nichts geschieht ohne Risiko, aber ohne Risiko geschieht auch nichts.



33

GO OUT  
IT-SECURITY  
HOSTING

enttec  
IT-COMMUNICATION

F:RTINET

McAfee

wikima  
THE FINE ART OF COOKING BUSINESS

IT-Security Forum #8

Computerworld.ch

Blickpunkt KMU

maschinenbau

## Risikomanagementprozess

- Die wesentlichen Schritte eines Risikomanagementprozesses bestehen aus den Phasen:
  1. Risikoanalyse,
  2. Risikobewertung,
  3. Risikominimierung,
  4. Risikokontrolle,
  5. Risikoverfolgung.

### Risikograph

Eintrittswahrscheinlichkeit	häufig	unwesentlich	geringfügig	kritisch	katastrophal
	wahrscheinlich	unwesentlich	geringfügig	kritisch	katastrophal
	gelegentlich	unwesentlich	geringfügig	kritisch	katastrophal
	entfernt vorstellbar	unwesentlich	geringfügig	kritisch	katastrophal
	unwahrscheinlich	unwesentlich	geringfügig	kritisch	katastrophal
	unvorstellbar	unwesentlich	geringfügig	kritisch	katastrophal
		unwesentlich	geringfügig	kritisch	katastrophal

■ akzeptabler Bereich  
■ ALARP-Bereich  
■ inakzeptabler Bereich

34

GO OUT  
IT-SECURITY  
HOSTING

enttec  
IT-COMMUNICATION

F:RTINET

McAfee

wikima  
THE FINE ART OF COOKING BUSINESS

IT-Security Forum #8

Computerworld.ch

Blickpunkt KMU

maschinenbau

## Risikoreduktion

- Verhindern von realen und den daraus resultierenden wirtschaftlichen Schäden im Unternehmen durch **Risikoreduktion** des Gesamtrisikos bis zum **akzeptierbaren Restrisiko**.

Das Diagramm zeigt die Reduktion des Gesamtrisikos (rot) durch verschiedene Maßnahmen (Vermeiden, Schutzmassnahmen, Schadensbegrenzung, Abwälzen) bis zum Restrisiko (grün). Eine horizontale rote Linie markiert das 'Tolerierbare Risiko'. Die x-Achse ist in 'Pre-Loss' und 'Post-Loss' unterteilt.

35

GO OUT  
IT-SECURITY  
WORKSHOP

entec  
IT-COMMUNICATION

FORTINET

McAfee

wikima  
THE FIRST ART OF COOKING BUSINESS

IT-Security Forum #8

Computerworld.ch  
Blickpunkt KMU  
maschinenbau

## Risikobetrachtung

- Ein Risiko ergibt sich für ein Schutz- bzw. Wertobjekt aus der **potenziellen Schadenshöhe** (Schadenspotential) multipliziert mit deren **Eintrittswahrscheinlichkeit** aufgrund einer latent vorhandenen **Bedrohung**.

36

GO OUT  
IT-SECURITY  
WORKSHOP

entec  
IT-COMMUNICATION

FORTINET

McAfee

wikima  
THE FIRST ART OF COOKING BUSINESS

IT-Security Forum #8

Computerworld.ch  
Blickpunkt KMU  
maschinenbau

## Eintrittswahrscheinlichkeit

- Es empfiehlt sich, die Plausibilität der Schätzungen zu hinterfragen: besser ungefähr richtig, als präzise falsch.
- Bsp.: Häufigkeit eines Schadens 1/100 Jahre
- Wie viele vergleichbare Betriebe in der Schweiz?
- Bei 10'000 solcher Betriebe müssten jährlich durchschnittlich 100 einen solchen Schaden erleiden.

Bezeichnung	Definition	Quantifizierung
Sehr häufig	Kann oft erwartet werden	> 1/1 Jahr
Häufig	Kann mehrmals vorkommen	Ca. 1/10 Jahre
Gelegentlich	Solche Fälle sind bekannt	Ca. 1/50 Jahre
Selten	Oft keine Fälle aus eigenem Unternehmen bekannt, aber vorstellbar	

37

GO OUT  
IT-SECURITY  
HOSTING

entec  
IT-COMMUNICATION

FORTINET

McAfee

wikima  
THE FINE ART OF CREATING BUSINESS

IT-Security Forum #8

Computerworld.ch  
Blickpunkt.KMU  
maschinenbau

## Beispiel

- Vorgehen
  - Untersuchung der org. und techn. Umgebung
  - Definition der Prozesse
  - Verfügbarkeiten festhalten
  - Risikobewertung
  - Massnahmenausarbeitung

38

GO OUT  
IT-SECURITY  
HOSTING

entec  
IT-COMMUNICATION

FORTINET

McAfee

wikima  
THE FINE ART OF CREATING BUSINESS

IT-Security Forum #8

Computerworld.ch  
Blickpunkt.KMU  
maschinenbau

## Beispiel

- BIA

BIA Datenerhebung Geschäftsprozesse				
Bereich:				
Prozess:				
Prozessbeschreibung:				
Prozessverantwortliche:				
Kritikalitäten:	Sehr gering	Gering	Hoch	Sehr hoch
*Finanziell:				
*Aufgabenstellung:				
*Verstösse:				
*Imageschaden:				
<small>*Eingabe in Felder = Bewertungszeit für welche die Kritikalität zutrifft.</small>				
Maximale Ausfallszeit:				
Maximaler Datenverlust:				
Priorisierung:				
Dienste und Ressourcen:				
Vertraulichkeit der Daten:				
Mindestanforderungen:				
Abhängigkeiten:				
Bemerkungen:				
	Datum	Name	Visum	
Prozessverantwortlicher				
Bereichsleiter				
Notfallverantwortlicher				

39







## ISMS-Tool : Verinice

- Verinice ist ein Java-basiertes ISMS-Tool für das Management von Informationssicherheit.
- Die Software wird unter der Lizenz GPLv3 zum freien Download als Open-Source-Software kostenfrei bereitgestellt.
- Das Programm Verinice unterstützt die Betriebssysteme Microsoft Windows, Linux und Mac OS und hat die IT-Grundschutz-Kataloge des BSI lizenziert.



## Verinice : Screenshots

The screenshots show the Verinice software interface. The top part displays a tree view of the 'IS-Kataloge' (IS Catalogs) with categories like 'B 1.0 IT-Sicherheitsmanagement', 'B 1.1 Organisation', 'B 1.2 Personal', 'B 1.3 Notfallvorsorge-Konzept', 'B 1.4 Datensicherheitskonzept', 'B 1.5 Datenschutz', 'B 1.6 Computer-Viren-Schutzkonzept', 'B 1.7 Krisenkonzept', 'B 1.8 Behandlung von Sicherheitsvorfällen', 'B 1.9 Hard- und Software-Manager', 'B 1.10 Standardsoftware', 'B 1.11 Sicherung', 'B 1.12 Archivierung', 'B 1.13 IT-Sicherheitsereignisbilanz', 'Anwendungen', 'Abhängigkeiten', 'Gebäude', 'Stammstz Göttingen', 'Zweigstelle Berlin', 'IT-Systeme: Clients', 'IT-Systeme: Server', 'IT-Systeme: Backup', 'IT-Systeme: sonstige', and 'IT-Systeme: TK-Komponenten'.

The middle part shows a detailed view of a security measure for 'Interne IT'. The details include:
 

- Name:** Interne IT
- Organisation:** infuscher GmbH
- Anzahl Mitarbeiter:** 150
- Geltungsbereich:** gesamtes Unternehmen
- Schutzbedarfskategorie:** Normal
- Gesetze / Vorschriften / Verträge:** Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen, geringfügige Vertragsverletzungen mit maximal geringen Nebenbestrafungen
- Selbstbestimmungsrecht:** Eine Beeinträchtigung des informationellen Selbstbestimmungsrechts würde durch den Erwerb als Internet-Angebote entstehen. Ein möglicher Nebenrecht personenbezogener Daten hat nur geringfügige Auswirkungen auf die wesentlichen Schritte und/oder die
- Universierbarkeit:** Eine Beeinträchtigung erscheint nicht möglich.
- Aufgabenerfüllung:** Die Beeinträchtigung würde von den Betroffenen als Internet-Angebote entstehen. Die maximal tolerierbare Ausfallzeit des IT-Systems ist größer als ??? Stunden.
- Innen- / Außenwirkung:** Eine geringe bzw. nur interne Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
- Finanzielle Auswirkungen:** Der finanzieller Schaden ist kleiner als 100,- EUR.
- Schutzbedarfskategorie:** hoch

The bottom part shows a chart titled 'Maßnahmen' (Measures) with a horizontal bar chart showing the implementation progress for different levels (A, B, C, Z). The x-axis represents the number of measures (0 to 1000). The y-axis represents the levels (A, B, C, Z). The bars are color-coded: red for 'zugeordnet' (assigned) and blue for 'umgesetzt' (implemented). The chart shows that level A has the highest number of assigned measures, followed by level B, and then levels C and Z.



IT-Security Forum #8



## ISMS-Tool : QSEC

- Die QSEC-Suite hilft bei der Einführung und dem Betrieb eines ganzheitlichen Information Security Management Systems (ISMS) nach ISO 27001.
- Das komplette Information Security Risikomanagement nach ISO 27005 mit allen Inhalten ist in die Lösung integriert.
- Ebenso Bestandteil sind das Massnahmen- und Dokumentenmanagement und ein aussagekräftiges und flexibles Reporting.



IT-Security Forum #8



## QSEC : Screenshots

The screenshot displays the QSEC v1.2 web interface. On the left is a navigation menu with categories: Compliance Management, Maßnahmen Management, Risiko Management, Dokumenten Management, Reporting, Standards, and Policies. The main content area is divided into several sections:

- Global:** A world map showing regional data points.
- Risiko Management - Bearbeitung Assetgruppe:** A detailed view of an asset group with fields for 'Assetgruppe', 'Verantwortlich', 'Wiederholungszyklus', and 'Zuletzt bearbeitet am'. It includes a 'Gesamt Risikowert' of 8.
- Assetgruppe Werten:** A table with columns for 'Verwundbarkeit', 'Verfügbarkeit', 'Wiederbeschaffungskosten', 'Integrität', 'Aufwendbarkeit', and 'Assetgruppen Wert'.
- Risikowert-Trend-Übersicht:** A table with columns for 'Status', 'Risiko-Bewertung', 'Betroffene Elemente', and 'Maßnahmen erfordern'. It lists various system components and their risk levels.

GO OUT  
IT-SECURITY  
HOSTING

entec  
IT-COMMUNICATION

FORTINET

McAfee

wikima  
THE FIRST ART OF COOKING BUSINESS

IT-Security Forum #8

Computerworld.ch  
Blickpunkt KMU  
maschinenbau

## QSEC : Live-Demo

46

GO OUT  
IT-SECURITY  
HOSTING

entec  
IT-COMMUNICATION

FORTINET

McAfee

wikima  
THE FIRST ART OF COOKING BUSINESS

IT-Security Forum #8

Computerworld.ch  
Blickpunkt KMU  
maschinenbau

## Zusammenfassung

### Wichtig für die Geschäftsleitung

- Unterstützung zwingend notwendig
- Benötigt SEHR viel Zeit
- Risikoabschätzung wichtig

### Wichtig für die IT

- Umfasst eine saubere IST-Aufnahme
- Grundsatzkataloge des BSI helfen bei den Massnahmen
- ISO 27002 bietet 133 Massnahmen

### Wichtig für die Benutzer

- Werden mit einbezogen
- Regelmässige Schulung notwendig

47

**GO OUT**  
IT-SECURITY  
PROTECTING

**entec**  
IT-COMMUNICATION

**FORTINET**

**McAfee**

**wikima**  
THE FINE ART OF COOKING BUSINESS

IT-Security Forum #8

**Computerworld.ch**

**Blickpunkt.KMU**

**maschinenbau**

## GO OUT Production GmbH

### Wissen Sie, wie es um Ihre IT-Sicherheit steht?

GO OUT Production GmbH  
Security Audits, -analysen und -beratungen  
Schulstrasse 11  
8542 Wiesendangen  
+41 52 320 91 20  
<http://www.goSecurity.ch>

