ISO 27001 / ISO 27005
Vorgehen und Anwendung

Andreas Wisler
Dipl. Ing. FH, CISSP, ISO 27001 Lead Auditor
GO OUT Production GmbH
wisler@goout.ch

IT-Security Forum #8

Agenda

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

ISO 27001

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

  eines Informationssicherheits-Managementsystems (ISMS)

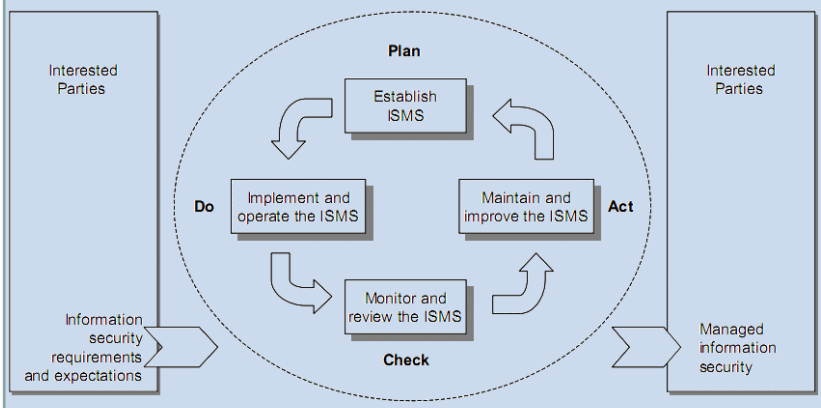
- Die Einführung eines ISMS sollte eine strategische Entscheidung sein.

28

GO OUT
entec
FORTINET
McAfee
wikima
IT-Security Forum #8
Computerworld.ch
Blickpunkt:KMU
maschinenbau

ISO 27001

- Informationssicherheits-Managementsystem (ISMS)



Quelle: ISO 27001

29

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

IT-Security Forum #8

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.

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 Coaching Business
IT-Security Forum #8
Computerworld.ch
Blickpunkt:KMU
maschinenbau

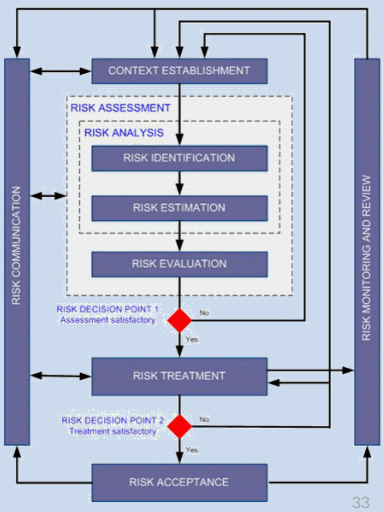
ISO 27005

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

  [Quelle Wikipedia]

- Wer nichts wagt, gewinnt nichts!

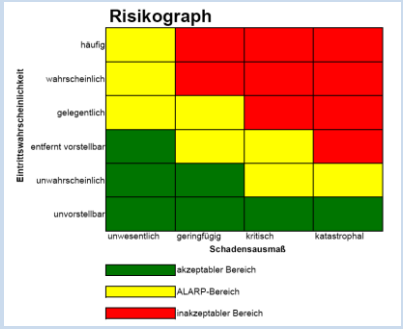
- Nichts geschieht ohne Risiko, aber ohne Risiko geschieht auch nichts.



33

Risikomanagementprozess

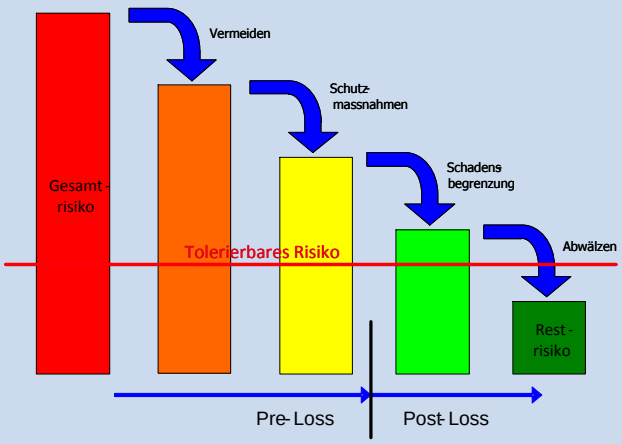
- Die wesentlichen Schritte eines Risikomanagementprozesses bestehen aus den Phasen:
  1. Risikoanalyse,
  2. Risikobewertung,
  3. Risikominimierung,
  4. Risikokontrolle,
  5. Risikoverfolgung.



GO OUT IT-SECURITY HOSTING
entec IT+COMMUNICATION
FORTINET
McAfee
wikima The Fine Art of Coaching Business
IT-Security Forum #8
Computerworld.ch
Blickpunkt:KMU
maschinenbau

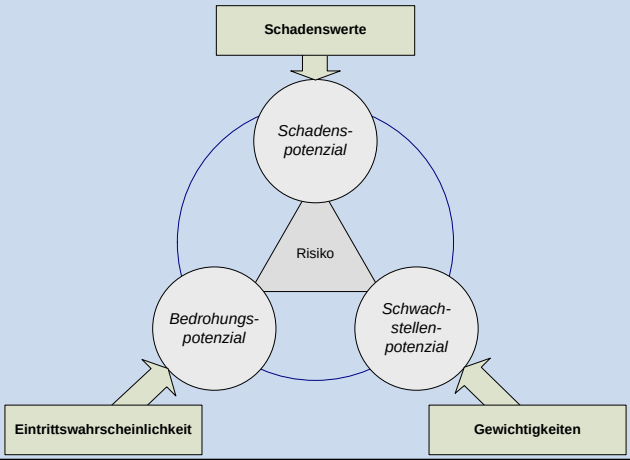
Risikoreduktion

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



Risikobetrachtung

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



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	

Beispiel

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

38

Beispiel

- BIA

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

39

GO OUT IT-SECURITY HOSTING
entec IT+COMMUNICATION
FORTINET
McAfee
wikima The Fine Art of Coaching Business
IT-Security Forum #8
Computerworld.ch
Blickpunkt:KMU
maschinenbau

Beispiel

- Risikobewertung

Prozess / Mittel	Kleinster Wert	alle Fo	Direktion, Bürokom	DBV-Plus (SAP)	Personal, Planung Bürokom																										
DC & Dienste	0.5	5	1	2	1.5	1.5	3	2		1	5				1	1	1	3	3	3				?	0.5	?					
Dateiserver, NAS	0.5	5	1		1.5		3			1	5	1			1	1	1	3	3	3					0.5	?					
LAN	0.5	5	1	2	1.5	1.5	3	2		1	5				1	1	1	3	3	3		1	1	?	0.5	?					
WAN	1	5	1	2	1.5		3	2		1	5				1		1	3	3	3		1	1	?	2	?					
Exchange	1	5	1		1.5		3			1	5						1	3	3	3											
WIDAS, AIX-Server	1	5	1		1.5		3			1	5					1	1	3	3	3		1	1	1		?					
BIT (FTP, Proxy)	1	5	1		1.5		3			1	5				1		1	3	3	3				?	?	?					
Internet	1	5	1		1.5		3			1	5						1	3	3	3		1	1		?	?					
Client	1	5	1	2	1.5	1.5	3	2		1	5				1	1	1	3	5	3		3	3	?	?	?					

Datenverlust		5	3	2	1.5	1.5	3	2	3	1	5	3	3	3	1	3	1	3	5	3		1	1	1	1	2					
Finanzen									3													2	2								
Verstösse																															
Image		10	2	4	5	4	10	4		1	10	3	10	10	3	3	1	10	10	10		2	2	10	1	10					

40

GO OUT IT-SECURITY HOSTING
entec IT+COMMUNICATION
FORTINET
McAfee
wikima The Fine Art of Coaching Business
IT-Security Forum #8
Computerworld.ch
Blickpunkt:KMU
maschinenbau

Beispiel

- Risikobewertung

Prozess / Mittel	Max. Ausfall	IST	Bewertung	Vertrag / Bemerkung
DC & Dienste	0.5	5 x (8-17h)	Ungenügend	SLA
Dateiserver, NAS	0.5	7 x 24h (4 h)	Ungenügend	Wartungsvertrag
LAN	0.5	7 x 24h	Genügend	SLA Typ Silber, Service Level S24, 99.5%
Mess-PC / -Laptop	0.5	Ausweich-Gerät	Genügend	
SQL / Oracle	0.5	5 x (8-17h)	Ungenügend	Vertrag
WAN	1	7 x 24h	Genügend	SLA BIT
Exchange	1	5 x (7-18h)	Genügend	SLA
WIDAS, Lizenz, AIX	1	5 x (8-15h)		Vertrag Interventionszeiten: 4 h per Telekommunikation, 1 Tag vor Ort
BIT (FTP, Proxy)	1	7 x 24h	Genügend	SLA
Internet (Bsp.: CertiPro)	1	7 x 24h	Genügend	SLA
Client	1	Ausweich-Gerät	Genügend	

41

GO OUT IT-SECURITY HOSTING
entec IT+COMMUNICATION
FORTINET
McAfee
wikima The Fine Art of Coaching Business
IT-Security Forum #8
Computerworld.ch
Blickpunkt:KMU
maschinenbau

ISMS-Tool : Verinice

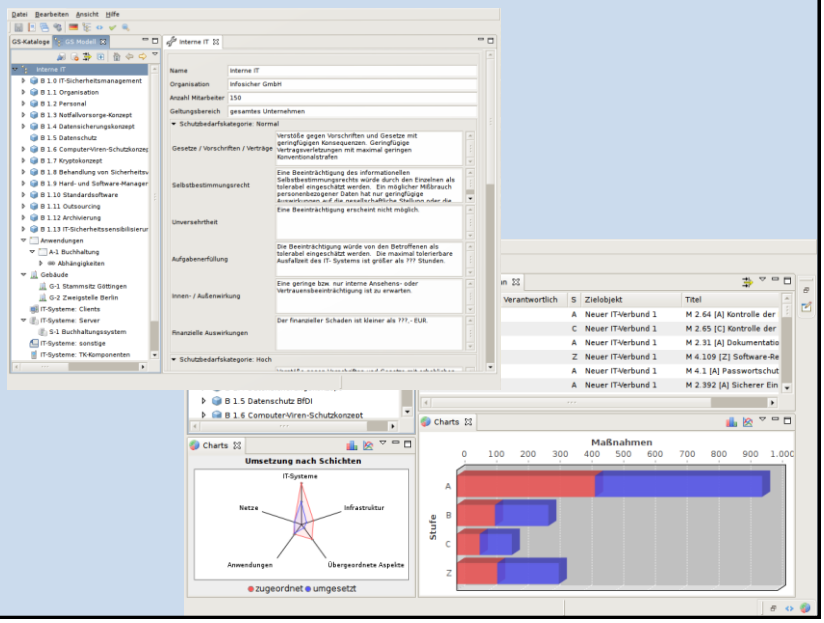
- Verinice ist ein Java-basiertes ISMS-Tool für das Management von Informationssicherheit.
- Die Software wird unter der Lizenz GPLv3 zum freien Download als Open-Source-Software kostenfrei bereitgestellt.
- Das Programm Verinice unterstützt die Betriebssysteme Microsoft Windows, Linux und Mac OS und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

verinice.

42

GO OUT IT-SECURITY HOSTING
entec IT+COMMUNICATION
FORTINET
McAfee
wikima The Fine Art of Coaching Business
IT-Security Forum #8
Computerworld.ch
Blickpunkt:KMU
maschinenbau

Verinice : Screenshots



GO OUT IT-SECURITY HOSTING
entec IT+COMMUNICATION
FORTINET
McAfee
wikima The Fine Art of Coaching Business
IT-Security Forum #8
Computerworld.ch
Blickpunkt:KMU
maschinenbau

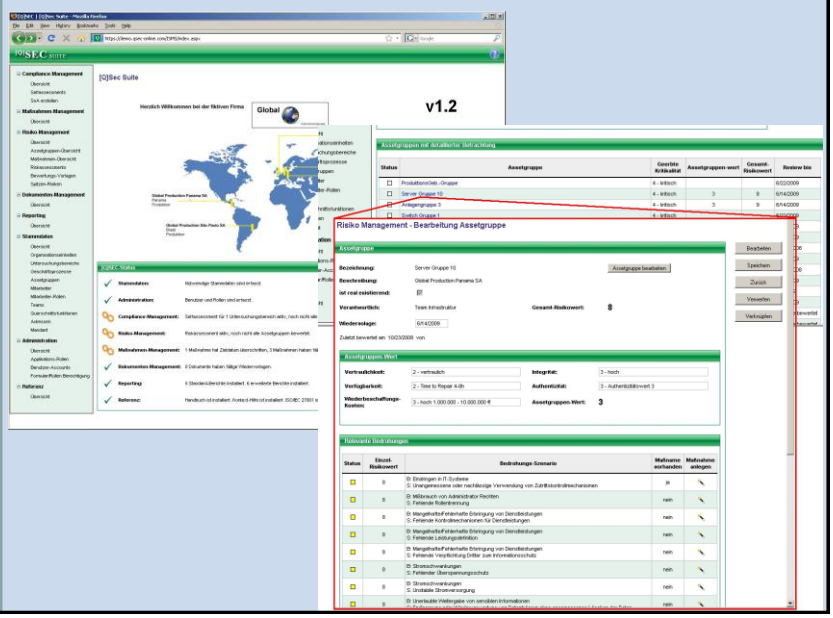
ISMS-Tool : QSEC

- 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.

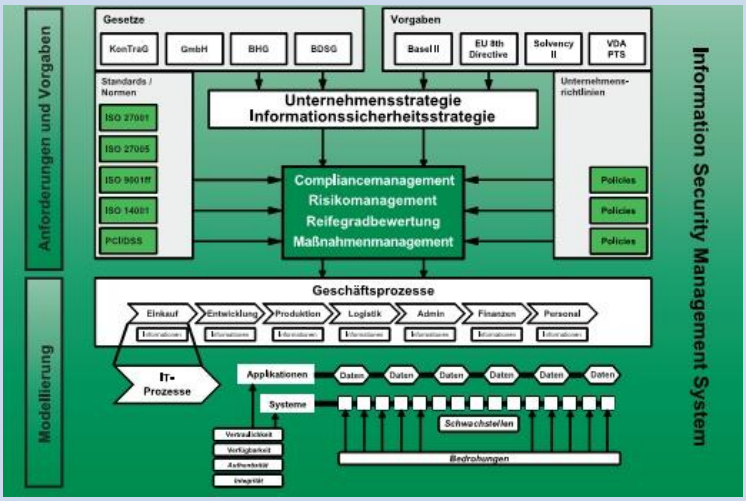
IQ SEC
WMC Wüpper Management Consulting
44

GO OUT IT-SECURITY HOSTING
entec IT+COMMUNICATION
FORTINET
McAfee
wikima The Fine Art of Coaching Business
IT-Security Forum #8
Computerworld.ch
Blickpunkt:KMU
maschinenbau

QSEC : Screenshots



QSEC : Live-Demo



GO OUT IT-SECURITY HOSTING
entec IT+COMMUNICATION
FORTINET
McAfee
wikima The Fine Art of Coaching 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
- Grundschutzkataloge des BSI helfen bei den Massnahmen
- ISO 27002 bietet 133 Massnahmen

Wichtig für die Benutzer

- Werden mit einbezogen
- Regelmässige Schulung notwendig

GO OUT

entec

FORTINET

McAfee

wikima

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