INFONEWS

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

www.goSecurity.ch
Mit Sicherheit an der richtigen Adresse.

Security Management nach ISO 27001

Schützen Sie ihre Unternehmensdaten mit einem Security Management auf Basis der ISO 2700x Standards. Dieser INFONEWS zeigt, was ISO 27001 ist und wie die Norm angewendet werden kann.

Inhaltsverzeichnis

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

1 Security Management auf Basis der ISO 2700x-Reihe

Informationssicherheit hat allgemein den Schutz von Informationen als Ziel. Dabei können Informationen sowohl auf Papier, in Rechnern oder auch in Köpfen gespeichert sein. Vordringliches Ziel der Informationssicherheit ist der Schutz elektronisch gespeicherter Informationen und deren Verarbeitung, wobei stets die Vertraulichkeit, Integrität und Verfügbarkeit der unternehmenskritischen Daten zu gewährleisten ist.

Aufgrund der Komplexität von Informationstechnik und der Nachfrage nach einer Zertifizierung sind in den letzten Jahren zahlreiche Anleitungen, Standards und nationale Normen zur IT-Sicherheit entstanden. Die internationale Norm ISO/IEC 27001:2005, "Information technology - Security techniques - Information security management systems - Requirements" ist der erste internationale Standard zum IT-Sicherheitsmanagement, der auch eine Zertifizierung ermöglicht. Diese spezifiziert die Anforderungen für Herstellung, Einführung, Betrieb, Überwachung, Wartung, und Verbesserung eines dokumentierten Informationssicherheits-Managementsystems unter Berücksichtigung der Risiken innerhalb der gesamten Organisation. Hierbei werden sämtliche Arten von Organisationen berücksichtigt.

1.1 Standards

Die ISO 2700x Reihe besteht aus verschiedenen Standards, die sich ergänzen:

Standard	Datum	Inhalt
ISO 27000	10.2005	Begriffsdefinitionen zum ISMS
ISO 27001	10.2005	Definition der Zertifizierungsanforderungen an ein ISMS Löst BS 7799-2 ab
ISO 27002	2007	Leitfaden zur Implementierung, Kontrollfragen Löst ISO 17799, BS 7799-1 ab
ISO 27003	in Arbeit	Einführungshilfe für ein ISMS
ISO 27004	2006	Definition von Kennzahlensystemen für ein ISMS
ISO 27005	06.2008	Risikomanagement zum ISMS Löst BS 7799-3 ab
ISO 27006	3.2007	Kriterien für Institutionen die das Audit und die Zertifizierung durchführen
ISO 27007	in Arbeit	Richtlinien für das Audit

1.2 Risikobeurteilung

Nachfolgend wollen wir uns zunächst mit dem ISO-Standard 27001 etwas genauer beschäftigen. Bevor Massnahmen umgesetzt werden können, muss zuerst das Risiko bekannt sein.

Für den Begriff „Risiko“ finden sich in der Literatur unterschiedliche Definitionen. Zwei gängige sind im Folgenden formuliert:

1. Ein Risiko ergibt sich für ein Schutz- bzw. Wertobjekt aus der potenziellen Schadenshöhe (Schadenspotential) multipliziert mit deren Eintrittswahrscheinlichkeit aufgrund einer latent vorhandenen Bedrohung. Das Schadenspotenzial bzw. das Ausmass eines potenziellen finanziellen Schadens kann zur Vergleichbarkeit und Anschau-

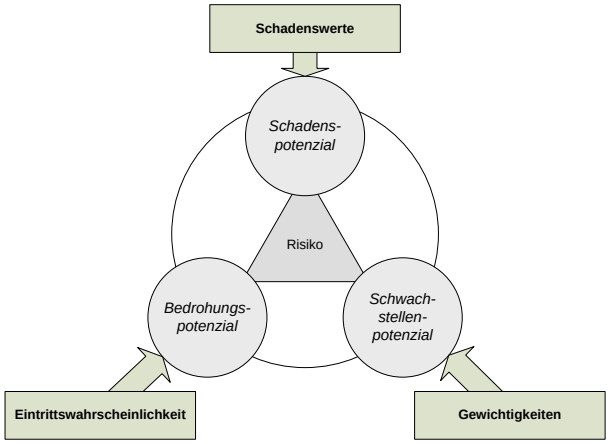
GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

lichkeit beispielsweise als prozentualer Anteil des Gewinns ausgedrückt werden.

Diese Betrachtung des Risikos gewichtet die Auswirkungen eines Schadenereignisses. Sie wird als Brutto-Risiko bezeichnet, weil sie die Wirkung getroffener Sicherheitsmassnahmen nicht berücksichtigt. Somit ermöglicht das Brutto-Risiko die kosten-nutzen-orientierte Priorisierung der zu treffenden Schutzmassnahmen.

Hinweis: Eine Bedrohung mit einer geringen Eintrittswahrscheinlichkeit kann dennoch sehr kurzfristig auftreten!

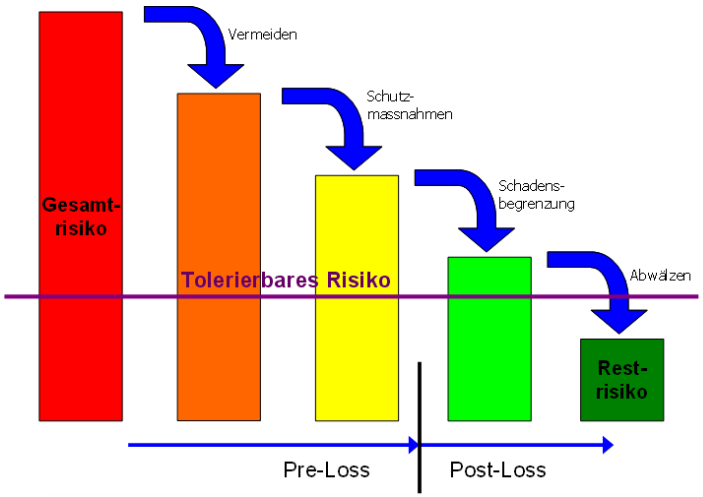


2. Die zweite Definition, die Netto-Risiko-Betrachtung, lautet: Ein Risiko ergibt sich aus der potenziellen Möglichkeit, dass eine Bedrohung die Schwachstelle(n) eines oder mehrerer schutzbedürftiger Wertobjekte (Assets) bzw. Schutzobjekte ausnutzt, sodass ein materieller oder immaterieller Schaden entsteht.

   Der Wert des Netto-Risikos ergibt sich als Brutto-Risiko, d.h. der potenziellen Schadenshöhe multipliziert mit der Eintrittswahrscheinlichkeit einer latent vorhandenen Bedrohung, multipliziert mit dem Schwachstellenpotenzial.

Als Risiko wird nach ISO 73 eine Kombination aus der (Eintritts-) Wahrscheinlichkeit eines (unerwünschten, unerwarteten, schädlichen) Ereignisses und dessen Konsequenzen definiert.

Das Ziel des IT-Sicherheitsmanagements ist es nun, die Risikoreduktion des Gesamtrisikos bis zum akzeptierbaren bzw. tragbaren Restrisiko:



GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

- **Risikovermeidung**: Dabei werden Risiken, denen ausgewichen werden kann, vermieden. Dies kann beispielsweise die Wahl eines geeigneten Raums oder der geeignete Aufstellungsort eines Servers sein.
- **Risikoverminderung** durch Schutzmassnahmen: Entgegen der Vermeidung, werden hier Risiken teilweise akzeptiert. Durch geeignete Schutzmassnahmen werden diese Risiken vermindert. Dies kann beispielsweise das Patchen von Systemen geschehen.
- **Schadensbegrenzung**: Durch geeignete Massnahmen wird bei Eintreten eines Risikos der Schaden begrenzt. Dies können beispielsweise Feuerlöschsysteme in einem Raum sein.
- **Risikoüberwälzung**: Bei der Risikoüberwälzung wird das Risiko durch faktische oder vertragliche, teilweise oder vollständig an Dritte übertragen. Dies kann beispielsweise durch Versicherungen der Fall sein oder die Abwälzung auf Vertragspartner.
- **Risikoakzeptanz**: Die Vermeidung, Verminderung und Überwälzung von Risiken kann die Risiken nicht vollständig ausschliessen. Das verbleibende Restrisiko muss das Unternehmen akzeptieren bzw. selber tragen.

Die Vermeidung und Schutzmassnahmen gehören zu den Pre-Loss Tätigkeiten, d.h. diese Tätigkeiten finden vor dem Eintritt eines Ereignisses bzw. Risikos ein. Die Schadensbegrenzung und das Abwälzen folgen erst, wenn ein Ereignis bzw. Risiko eingetreten ist (Post-Loss). Jedoch müssen entsprechende Verträge und Versicherungen vor dem Eintreten definiert sein, da sie ansonsten nicht mehr umgesetzt werden können! Damit ein Schaden nicht grösser wird, lohnt es sich zudem, Notfallpläne zu erstellen und die Vorgehensweisen auch regelmässig zu üben.

Es stellen sich daher mit der Risikobewertung zwei Fragen: Welche Ereignisse gilt es zu untersuchen? Welche Konsequenzen können daraus entstehen?

Eine weitere Quelle sind Anforderungen, die sich aus Gesetzen, Politik, Regelungen und Verträgen ergeben und die von einer Organisation und ihren Handelspartnern, Vertragspartnern, und Dienstleistern erfüllt werden müssen sowie die soziokulturelle Umgebung.

Weiter sind die spezifischen Prinzipien, Ziele und geschäftlichen Anforderungen an die Informationsverarbeitung, die eine Organisation entwickelt hat, um ihren Geschäftsbetrieb zu unterstützen.

Die neue Norm ISO/IEC 27005 hilft dabei, die Risiken zu erkennen und zu behandeln. Eine kurze Einführung in diese Norm ist weiter unten beschrieben.

Nach ISO 27001 soll nun ein Informationssicherheits-Managementsystem (ISMS) aufgebaut werden, welches die Grundlage zur Identifikation und Beherrschung der

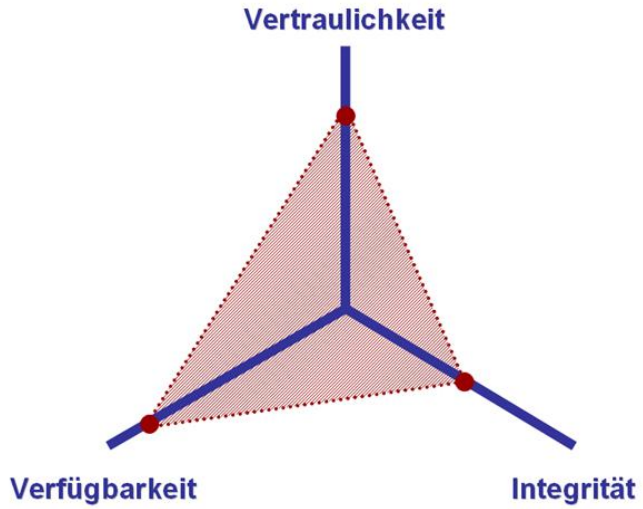
GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

Informationssicherheitsrisiken sowie zur Sicherstellung der Zuverlässigkeit von Systemen bietet.

Mögliche Ereignisse, die auf eine Organisation einwirken können, sind z.B. gezielte Angriffe von Personen auf technische oder organisatorische Schwachstellen; Elementarereignisse wie Erdbeben, Feuer, Wassereinbruch, Blitzschlag; Fahrlässige Handlungen oder Fehlbedienung von Systemen; Verstösse gegen Gesetze oder Verträge; sowie potentielle Schädigung von Personen (Ansehen, Gesundheit, Leben).

Die Konsequenzen können je nach Ereignis unmittelbaren monetären Schaden verursachen, aber auch Imageverlust, Verlust der Kreditwürdigkeit oder Entzug von Genehmigungen mit sich bringen.



Der ISO Standard verlangt für jeden erkannten Informationswert die Risiken bezüglich der Verfügbarkeit, Vertraulichkeit und Integrität und ggf. weiterer Ziele zu identifizieren und abzuschätzen. Dabei gehen die Bedrohungen, Schwachstellen sowie die Einschätzung von Ausmass und Häufigkeit der Schäden ein.

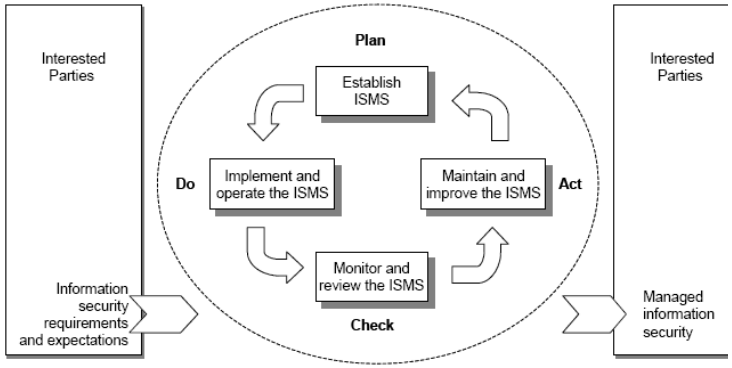
goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

2 Vorgehen

Wie bereits aus anderen Bereichen bekannt, verwendet auch ISO 27001 das PDCA-Modell von William Edwards Deming („Plan-Do-Check-Act“ - „Planen, Durchführen, Prüfen, Handeln“):



- **Planen** (Festlegen des ISMS)
  Festlegen der ISMS-Leitlinie, -Ziele, -Prozesse und -Verfahren, die für das Risikomanagement und die Verbesserung der Informationssicherheit notwendig sind, um Ergebnisse im Rahmen aller Grundsätze und Ziele einer Organisation zu erreichen.

- **Durchführen** (Umsetzen und Durchführen des ISMS)
  Umsetzen und Durchführen der ISMS-Leitlinie, Massnahmen, Prozesse und Verfahren.

- **Prüfen** (Überwachen und Überprüfen des ISMS)
  Einschätzen und ggf. Messen der Prozessleistung an der ISMS-Leitlinie, den ISMS-Zielen und praktischen Erfahrungen, und Berichten der Ergebnisse an das Management zwecks Überprüfung.

- **Handeln** (Instandhalten und Verbessern des ISMS)
  Ergreifen von Korrekturmassnahmen und Vorbeugungsmassnahmen, basierend auf den Ergebnissen von internen ISMS-Audits und Überprüfungen des Managements und anderen wesentlichen Informationen, zur ständigen Verbesserung des ISMS.

Die ISO-Norm 27001 beschreibt dabei das Informationssicherheits-Managementsystem im folgenden Satz: „Die Organisation muss ein dokumentiertes ISMS im Kontext ihrer allgemeinen Geschäftsaktivitäten und der Risiken, der sie sich gegenübersieht, festlegen, umsetzen, durchführen, überwachen, überprüfen, instandhalten und verbessern.“

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

3 ISO/IEC 27001

Die ISO-Norm 27001 ist in verschiedene Kapitel unterteilt:

- **Einleitung**
  Beschreibt den prozessorientierten Ansatz sowie die Verträglichkeit mit anderen Managementsystemen

- **Anwendungsbereich**
  Zeigt, wie die Norm angewendet werden soll.

- **Begriffe**
  Alle in der Norm verwendeten Begriffe werden in kurzen Sätzen beschrieben

- **Informationssicherheits-Managementsystem**
  Der erste Teil der Norm beschreibt die allgemeinen Anforderungen an ein ISMS. Ein wichtiger Aspekt gilt dem Festlegen (Definition des Anwendungsbereichs und der Grenzen; Identifizierung der Risiken inkl. Analyse und Bewertung; Optionen für die Risikobehandlung mit anschliessender Auswahl der Massnahmen zur Risikobehandlung) und dem anschliessenden Umsetzen und Durchführen. Die Norm verlangt hier unter anderem klar, dass ein Programm zur Schulung und Bewusstseinsbildung umgesetzt wird.

  Weiter gehören auch das Überwachen und Überprüfen in regelmässigen Abständen dazu. Die Norm verlangt, dass in regelmässigen Abständen, jedoch mindestens einmal pro Jahr, interne bzw. eigene Audits erfolgen müssen. Diese „internen“ Audits dürfen an externe, spezialisierten Firmen in Auftrag gegeben werden. Dies kann sich sicherlich lohnen, kommt doch eine unabhängige Drittmeinung dazu. Alle drei Jahre ist die Zertifizierung zu wiederholen. Sollten in den internen und externen Audits Mängel festgestellt werden, sind diese Instand zu stellen und zu verbessern.

  Ein weiteres Kapitel im ersten Teil beschreibt die Dokumentationsanforderungen. Die Dokumentationen müssen Aufzeichnungen von Managemententscheidungen enthalten, sicherstellen, dass sich Aktivitäten auf Managemententscheidungen und Grundsätze zurückverfolgen lassen und zusätzlich sicherstellen, dass die aufgezeichneten Ergebnisse reproduzierbar sind. Es ist wichtig, dass es möglich ist, die Beziehung von den ausgewählten Massnahmen zurück zu den Resultaten des Risikoeinschätzungs- und Risikobehandlungsprozesses nachzuweisen und weiter zurück zu der ISMS-Leitlinie und den –Zielen verfolgbar ist.

- **Verantwortung des Managements**
  Der zweite Teil nimmt das Management in die Pflicht. Es muss in acht Punkten nachweisen, dass es seine Verpflichtungen wahr nimmt. Dazu gehört auch das Ermitteln und Bereitstellen der erforderli-

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

chen Ressourcen. Weiter muss die Organisation sicherstellen, dass die Schulungen, das Bewusstsein und die Kompetenzen vorhanden sind.

- **Managementbewertung des ISMS**
  Wie bereits erwähnt, gilt es, das ISMS mindestens einmal pro Jahr zu überprüfen. Dieses Kapitel der Norm zeigt, was die Managementbewertung im Minimum enthalten muss. Die Ergebnisse der Managementbewertung müssen Entscheidungen und Aktivitäten zur Verbesserung und Wirksamkeit sowie die Aktualisierung des Risikoeinschätzungsplans enthalten.

- **Verbesserung des ISMS**
  Ein eigenes Kapitel erhält auch die Pflege und Verbesserung des ISMS. Wie der PDCA-Zirkel zeigt, bewegt sich das ISMS immer weiter. Ein Stillstand ist nicht möglich. Die Organisation muss Massnahmen zur Beseitigung der Ursachen von Nichtkonformitäten mit den ISMS-Anforderungen ergreifen, um deren erneutes Auftreten zu verhindern. Weiter gehören Vorbeugungsmassnahmen dazu, damit potenzielle Probleme erst gar nicht auftreten können.

- **Anhang A: Massnahmenziele und Massnahmen**
  Der Anhang umfasst die Kontrollfragen von ISO 27002 in einer kurzen Übersicht (siehe folgendes Kapitel)

- Der **Anhang B** enthält die OECD Grundsätze und das PDCA Modell. Zum Schluss zeigt der Anhang C die Übereinstimmungen zwischen ISO 9001:2000, ISO 14001:2004 und ISO 27001.

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

4 ISO/IEC 27002

Obwohl die ISO-Norm 27001 klare Anweisungen und Aufgaben enthält, ist es nicht immer einfach entsprechende Massnahmen abzuleiten.

Das Ziel von ISO 27002 "Information technology – Code of practice for information security management" definiert ein Rahmenwerk für das IT-Sicherheitsmanagement. Es befasst sich mit den erforderlichen Schritten, um ein funktionierendes IT-Sicherheitsmanagement aufzubauen und gliedert sich in elf Managementgebiete mit 39 Massnahmenzielen. Die Massnahmenziele enthalten insgesamt 133 Massnahmen (baseline controls), die zur Zielerreichung umgesetzt werden können. Die elf Managementgebiete umfassen dabei folgende Punkte:

- Sicherheitsleitlinie,
- Organisation der Informationssicherheit,
- Management von organisationseigenen Werten,
- Personalsicherheit,
- Physische und umgebungsbezogene Sicherheit,
- Betriebs- und Kommunikationsmanagement,
- Zugangskontrolle,
- Beschaffung, Entwicklung und Wartung von Informationssystemen,
- Umgang mit Informationssicherheitsvorfällen,
- Sicherstellung des Geschäftsbetriebs und
- Einhaltung von Vorgaben.

Jede der wesentlichen Sicherheitskategorien enthält:

a) ein Massnahmenziel, das angibt, was zu erreichen ist und
b) eine oder mehrere Massnahmen, die angewandt werden können, um dieses Massnahmenziel zu erreichen.

Die Beschreibung der Massnahmen ist wie folgt strukturiert:

- **Massnahme**
  Definiert die spezifische Aussage der Massnahme zur Erfüllung des Massnahmenziels.

- **Anleitung zur Umsetzung**
  Stellt weitere detaillierte Informationen bereit, um die Umsetzung der Massnahmen und das Erreichen des Massnahmenziels zu unterstützen. Manche der Anleitungen sind möglicherweise nicht in allen Fällen passend. Daher können andere Wege der Umsetzung der Massnahme geeigneter sein.

- **Weitere Informationen**
  Stellt weitere Informationen bereit, die möglicherweise zu berücksichtigen sind, zum Beispiel Überlegungen ihm Hinblick auf Gesetze oder Verweise auf anderen Standards.

Nachfolgend ist ein Beispiel abgebildet, welches zeigt, wie eine unabhängige Überprüfung der Informationssicherheit durchgeführt, bzw. welche Punkte beachtet werden müs-

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

sen. Es handelt sich um die Massnahme 6.1.8. Quelle: Deutsche Übersetzung der ISO/IEC Norm 27002

6.1.8 Unabhängige Überprüfung der Informationssicherheit

- **Massnahme**
  Der Ansatz einer Organisation zur Handhabung und Umsetzung der Informationssicherheit (d.h. Massnahmenziele, Massnahmen, Leitlinien, Prozesse und Verfahren für Informationssicherheit) sollte in regelmässigen Zeitabständen, oder nach wesentlichen Änderungen an der implementierten Sicherheit von unabhängiger Seite überprüft werden.

- **Anleitung zur Umsetzung**
  Die unabhängige Prüfung sollte vom Management veranlasst werden. Solch eine unabhängige Überprüfung ist notwendig, um die ständige Eignung, Angemessenheit und Wirksamkeit des Ansatzes der Organisation für die Handhabung der Informationssicherheit zu gewährleisten. Die Überprüfung sollte auch die Untersuchung von Möglichkeiten zur Verbesserung und Untersuchungen des Bedarfs für Änderungen am generellen Ansatz für Sicherheit, einschliesslich der Leitlinie und der Massnahmenziele beinhalten.

  Eine derartige Überprüfung sollte durch Personen ausgeführt werden, die unabhängig von dem zu überprüfenden Bereich sind, z. B. die interne Revision, interne Auditoren, eine unabhängige Führungskraft oder eine externe Organisation, die auf solche Prüfungen spezialisiert ist. Personen, die diese Überprüfungen durchführen, sollten die erforderlichen Fähigkeiten und Erfahrungen besitzen.

  Die Ergebnisse der unabhängigen Überprüfung sollten aufgezeichnet und dem Management berichtet werden, dass die Überprüfung veranlasst hat. Diese Aufzeichnungen sollten aktuell gehalten werden.

  Falls die unabhängige Überprüfung ergibt, dass der Ansatz und die Umsetzung der Organisation für die Handhabung von Informationssicherheit nicht angemessen sind oder nicht konform mit der Ausrichtung der Informationssicherheit, wie sie in der Informationssicherheitsleitlinie festgelegt ist, sollte das Management Korrekturen des Vorgehens in Betracht ziehen.

- **Weitere Informationen**
  Der Bereich, den Manager regelmässig überprüfen sollten, darf auch von unabhängiger Seite überprüft werden. Überprüfungsmethoden können Interviews des Managements, die Kontrolle von Aufzeichnungen oder die Durchsicht von Sicherheitsleitlinien sein. ISO 19011:2002, Leitfaden für Audits von Qualitätsmanagement- und/oder Umweltmanagementsystemen, kann ebenfalls eine hilfreiche Anleitung zur Durchführung einer unabhängigen Überprüfung, einschliesslich der Erstellung und Umsetzung eines Überprüfungsprogramms liefern.

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

5 ISO/IEC 27005

Die ISO/IEC 27005 „Information Security Risk Management“ bietet Richtlinien, Tabellen und Beispiele zum IT-Risikomanagement, besonders in Bezug auf den Zertifizierungsstandard ISO 27001 für Informationssicherheit. Die neue ISO 27005 ersetzt die Richtlinien TR 13335-3:1998 sowie TR 13335-4:2000 als Zusammenführung und Erweiterung dieser Reports.

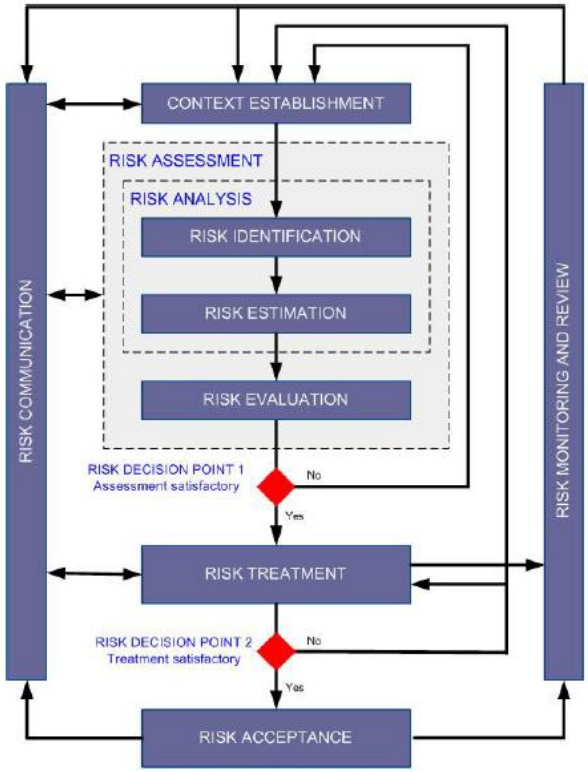
5.1 Struktur des Standards

Der Standard enthält die Beschreibung des Informationssicherheitsrisikomanagement-Prozesses und der Massnahmen. Der Aufbau ist in folgende Kapitel unterteilt:

- Einrichtung eines Risikomanagements
- Risiko-Einschätzung
- Risiko-Behandlung
- Risiko-Akzeptanz
- Risiko-Kommunikation
- Risiko-Überwachung und –Kontrolle

Der Anhang des Standards enthält weitergehende Informationen: Definition von Ziel- und Rahmenbedingungen, Identifizierung und Bewertung von Werten, Bedrohungen und Verwundbarkeiten.

5.2 Ablauf nach ISO 27005



Bildquelle: ISO/IEC 27005

Zuerst wird der Rahmen definiert (Context Establishment). Anschliessend kann eine Risikobewertung durchgeführt werden (Risk Assessment). Wenn diese ausreichende Informationen geliefert hat, um die notwendigen Massnahmen zur Reduktion der Risiken auf ein akzeptables Niveau zu bringen, ist dieser Schritt abgeschlossen. Genügen die

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

Informationen nicht, muss eine andere Sicht der bewertung auf alle oder einzelne Bereich durchgeführt werden (Zum Beispiel durch andere Kriterien zur Bewertung der Risiken, veränderte Akzeptanzkriterien, usw.) = Risk Desicion Point 1.

Die Wirksamkeit der Risikobehandlung hängt von den Ergebnissen der Risikobewertung ab. Es ist dabei möglich, dass die Wirksamkeit der getroffenen Massnahmen nicht sofort auf das geforderte, akzeptable Niveau der Restrisiken führt. Daher muss erneut eine andere Sicht der Risikobewertung durchgeführt werden = Risk Decision Point 2.

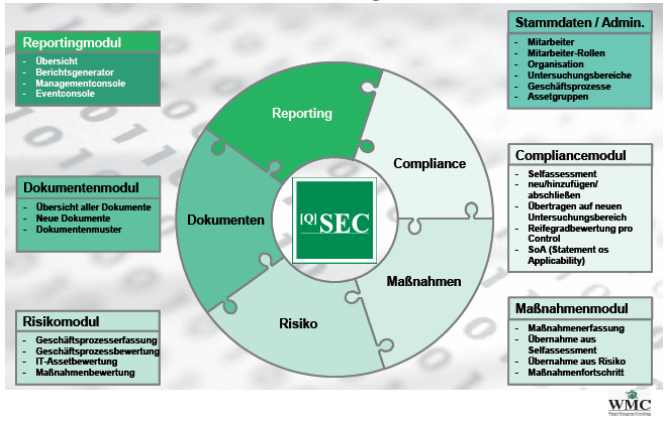
Durch den gesamten Prozess ist es wichtig, dass das Management die Risiken kenn und Restrisiken klar akzeptiert. Dies ist insbesondere dann wichtig, wenn Kontrollen, zum Beispiel aus finanziellen Gründen, weggelassen werden.

6 Dokumentation und Umsetzung mit |Q|SEC

Eine grosse Herausforderung stellt die Dokumentation dar. Ständig kommen neue Informationen dazu, die Prozesse ändern und Risiken verlagern sich. Es ist wichtig, dass das Management ständig einen Überblick über den Stand der Arbeiten hat und entsprechende (Korrektur-) Massnahmen einleiten kann. Auf dem Markt gibt es einige Programme, die hier Unterstützung bieten. Oft sind diese aber auf ein Teilgebiet beschränkt (z.B. Risiko-Erkennung und –Steuerung) oder waren ursprünglich für einen anderen Einsatzzweck gedacht und nun an ISO 27001 angepasst. Grössere Firmen haben zudem in der Regel mit grossem Aufwand eine eigene Lösung geschaffen. Die Pflege bedarf aber eines grossen Aufwands.

Abhilfe schafft die |Q| SEC Suite der Firma WMC. Sie umfasst alle Teilbereiche des Sicherheitsmanagements, von der konsequenten Weiterentwicklung des betrieblichen Informationssicherheitskonzeptes bis hin zum aktiven Management der gesamten Sicherheitsarchitektur. Auf einfachste Weise können die Geschäftsprozesse und Untersuchungsbereiche erfasst werden. Anschliessend können die Kritikalitäten dieser Prozesse bewertet werden. Ein umfassender Fragenkatalog hilft bei der korrekten Erfassung und Bewertung. Kontrollpunkte werden anschliessend sauber ausgegeben. Somit verfügt die Geschäftsleitung über ein umfassendes und einfach zu steuerndes Reporting-System.

Die |Q|SEC Suite umfasst die folgenden Module:



goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

Folgende Abbildung zeigt, wie beispielsweise die Risiko-management-Übersicht aussieht:

Risiko Management - Übersicht

Assetgruppen	
Erfasste Assetgruppen:	39
Assetgruppen mit hoher Kritikalität:	36
Davon mit hohem Assetgruppenwert:	0
Davon mit hohem Gesamt-Risikowert:	9
Davon noch nicht detailliert bewertet:	0

Maßnahmen	
Erfasste Maßnahmen:	16
Kosteneffektiv:	3
Wegen Risiko-Akzeptanz nicht durchzuführen:	1
Noch nicht risikobewertet:	13

Weitere Informationen zu den hohen Risikowerten und den entsprechend erfassten Massnahmen können mit einem Klick aufgerufen werden:

Relevante Bedrohungen

Status	Einzel-Risikowert	Bedrohungs-Szenario	Maßname vorhanden	Maßnahme anlegen
☐	8	B: Eindringen in IT-Systeme S: Unangemessene oder nachlässige Verwendung von Zutrittskontrollmechanismen	ja	
☐	8	B: Mißbrauch von Administrator Rechten S: Fehlende Rollentrennung	nein	
☐	8	B: Mangelhafte/Fehlerhafte Erbringung von Dienstleistungen S: Fehlende Kontrollmechanismen für Dienstleistungen	nein	

[Q]SEC – die Vorteile auf einen Blick:

- Systematische, ganzheitliche und kontinuierliche Umsetzung der Sicherheitsziele und deren Management nach dem Plan-Do-Check-Act-Verfahren (PDCA) durch die Integration der Module
- Nachhaltige Reduzierung der internen und externen Aufwendungen bei der Einführung und dem Betrieb des ISMS durch methodische, umfangreiche Unterstützungsfunktionen von [Q]SEC nach Best Practice inkl. vieler Musterdokumente
- Möglichkeit der tagesaktuellen Dokumentation und des einfachen Reportings des Sicherheitsstatus erhöht das Vertrauen und die Zufriedenheit der Geschäftspartner (Kunden, Lieferanten, Kooperationspartner, Aktionäre)
- Gezielter und optimierter Einsatz der Sicherheitsinvestitionen durch Transparenz der wesentlichen Erfordernisse aus dem Risiko-, und Massnahmenmanagement
- Rentabilitätssteigerung durch Ausfallreduzierung und schnelleren Wiederanlauf nach Sicherheitsvorfällen

Als offizieller Partner der WMC kann Ihnen die GO OUT Production GmbH umfassende Unterstützung im Aufbau des ISMS mit der [Q]SEC Suite bieten.

7 Zertifizierung

Bei der Zertifizierung nach ISO 27001 versuchen sich die Auditoren in die Lage des Unternehmens zu versetzen und selber die Risikostellen zu identifizieren. Anschliessend werden diese mit denjenigen des Unternehmens verglichen. Sind alle vorhanden? Sind weitere erkannt worden? Werden entsprechende Massnahmen abgeleitet? Erst danach werden die entsprechenden Massnahmen genauer angeschaut. Dabei geht es weniger um die technischen Details, sondern um die korrekte Erkennung und das Einleiten von Massnahmen. Diese Schritte müssen zwingend dokumentiert werden. Protokolle der Managementsitzungen und internen Audits bilden einen weiteren Kontrollpunkt der Auditoren. Sind auch hier Risiken und passende Massnahmen enthalten sowie Umsetzungen durchgeführt? Falls dies regelmässig und vollständig stattfindet, steht einer erfolgreichen Zertifizierung nach ISO 27001 nichts mehr im Wege.

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21