Rochusstraße 16
50129 Bergheim
Mobil 0177 8072315
Fon (02238) 303318
heike.stumm@stumm-it-sicherheit.de
stumm-it-sicherheit.de

ISMS flow

Ziel:

ISMS flow soll Organisationen mit geringer Personalkapazität für Informationssicherheit ermöglichen, dennoch ein standardkonformes Informations-Sicherheits-Management-System (ISMS) einzuführen. Die beauftragte Person wird durch den Einführungsprozess geführt und erhält Unterstützung durch Musterlösungen, die den BSI Standard 200 (IT-Grundschutz-Methodik) mit der Vorgehensweise Standard-Absicherung erfüllen. Bei Einhaltung der formalen Voraussetzungen ist das ISMS daher nach ISO 27001 **auf Basis von IT-Grundschutz zertifizierbar**, wenn die Anforderungen angemessen umgesetzt wurden.

Es ist eine Terminplanung beigefügt, die eine Einführung des ISMS innerhalb eines halben Jahres vorsieht, dafür wird ein personeller Aufwand von einem Tag pro Woche für die beauftragte Person erwartet (26 Personentage). Der Einführungszeitraum kann natürlich bei entsprechender zeitlicher Verfügbarkeit der beauftragten Person verkürzt oder verlängert werden.

Vorgehen:

Kern des ISMS flow ist ein Workflow-Dokument, das mit der Benennung der beauftragten Person beginnt und diese dann durch den Einführungsprozess führt. Dabei werden zunächst **5 grundlegende Schritte** durchgeführt:

- Benennung der beauftragten Person
- Übernahme des IT-Grundschutz als Standard für das eigene ISMS
- Gestaltung des Informations-Sicherheits-Prozesses als Grundlage für das ISMS
- Definition des Schutzbedarfes
- Beginn der Erfassung des IT-Verbundes (Scope)

Nach diesen Schritten wird dann die **Sicherheitskonzeption** der für den IT-Verbund erforderlichen Themen (Bausteine des IT-Grundschutz) ebenfalls schrittweise erarbeitet. Die Reihenfolge der Themen kann frei nach aktuell anstehenden Projekten angepasst werden.

Die Bearbeitung der einzelnen Schritte wird durch einen **Terminplan** gesteuert. Als Vorschlag sind in diesem Terminplan bereits Aufwandsschätzungen enthalten, die auf eine personelle Verfügbarkeit der beauftragten Person von einem Tag pro Woche veranschlagt sind.

Inhalte:

Die gesamte Vorgehensweise wird durch Musterdokumente, die auf den eigenen IT-Verbund angepasst werden sollen, unterstützt. Im Wesentlichen handelt es sich dabei um:

- **Musteraufträge**:
  Mit diesen werden die einzelnen Aufgaben, die sich im Rahmen der einzelnen Schritte ergeben Organisationseinheiten oder Personen zugewiesen. Dadurch wird die Zuweisung der Aufgabe im Rahmen des ISMS rechtsverbindlich dokumentiert und eine Basis für die Überprüfung der Umsetzung geschaffen. Auch eine Terminkontrolle erfolgt hierdurch. Die Überwachung der Aufgabenumsetzung ist im Terminplan bereits angelegt, es müssen noch die korrekten Termine eingetragen werden.
- **Regelungen**:
  In den Regelungen werden die Anforderungen des IT-Grundschutz themenbezogen zusammengefasst. Es handelt sich dabei um eine Umsortierung der IT-Grundschutz-Bausteine, in der Regel in der Unterscheidung zwischen Planungs- und Betriebsanforderungen. Durch die Freigabe der Regelungen akzeptiert die Organisation den IT-Grundschutz als den anzuwendenden Standard.
- **Mustergliederung Planungsvorgaben:**
  Die Planungsanforderungen des IT-Grundschutz geben vor, welche Planungen je Thema durchzuführen und zu dokumentieren sind. Die Mustergliederungen stellen die erforderlichen Bestandteile zusammen und dienen dadurch als Checkliste für zukünftige Planungen.
- **Mustergliederung Ergänzende Betriebsregelungen:**
  Die Anforderungen für den Betrieb werden in den Regelungen unverändert zum Standard übernommen. Sie müssen aber für den eigenen IT-Verbund angepasst werden. Dies kann durch eine Konkretisierung erfolgen, durch die Verwendung einer mindestens gleichwertigen Alternativmaßnahme oder durch einen (vorübergehenden) Verzicht der Umsetzung bei gleichzeitiger Übernahme des Risikos durch das Management der Organisation. Diese Anpassungen müssen dokumentiert und begründet werden. Dazu dienen die Mustergliederungen, bei denen entsprechende Anpassungen für jede einzelne Betriebsanforderung erfasst werden können.
- **Muster-Richtlinien und -Konzepte:**
  Natürlich haben wir auch unsere Erfahrung bei der Einführung von Informationssicherheit in ISMS flow eingebracht und stellen Best Practise Lösungen für Themenkomplexe bereit, bei denen sich dies anbietet, also zum Beispiel dem Berechtigungs-Management oder der Erstellung eines Kryptokonzeptes.
- **Musterformulare:**
  Werden aus dem IT-Grundschutz heraus bestimmte Workflows oder zu erfassende Inhalte vorgegeben, haben wir soweit möglich dafür Umsetzungsformulare entworfen. Eine papierbezogene Verwendung ist möglich, es empfiehlt sich aber natürlich eine Umwandlung in IT-gestützte Workflows.

Die Gestaltung von baulichen Sicherheitsmaßnahmen anhand einer Musterlösung verursacht häufig unnötige Ausgaben, da durch die Fixierung auf das Muster kostengünstigere Alternativen übersehen werden. Daher haben wir auf ein bauliches Musterkonzept verzichtet.

ISMS flow

Voraussetzungen:

ISMS flow ist bewusst so gestaltet, dass **keine besonderen technischen Voraussetzungen** erforderlich sind. Es werden ausschließlich Standardprodukte aus der Bürokommunikation benötigt (Microsoft Word, Excel, Acrobat Reader).

Weitergehende Unterstützung:

ISMS flow ist so gestaltet, dass es ohne weitergehende Unterstützung verwendet werden kann. Dennoch zeigt unsere Erfahrung, dass in vielen Organisationen eine Unterstützung bei der Vorbereitung oder Einführung gewünscht wird, um den eigenen „Lesebedarf" zu reduzieren. Daher bieten wir entsprechende unterstützende Workshops an:

- **ISMS facts:**
  Halbtägiger Workshop zur Entscheidungshilfe, ob ein ISMS erforderlich ist und wenn ja, ob der ISMS flow das geeignete Produkt ist.
- **ISMS navigator:**
  3-tägige Workshop-Reihe zur Unterstützung bei der eigenständigen Einführung des ISMS mit ISMS flow.
  An den einzelnen Tagen werden die Methodik vermittelt, gemeinsam die Grundlagen des Informations-Sicherheits-Prozesses erarbeitet und die typischen Aufwandsschwerpunkte bei der Konzeption näher betrachtet.
  ISMS navigator wird als **individuelle Inhouse-Lösung**, oder als offener Workshop angeboten.
- **ISMS pilot:**
  Wir führen das **ISMS** zum Pauschalpreis für Ihre Organisation auf Basis des ISMS flow **ein**.